Condensed Matter Physics 2008, Vol. 11, No 2(54), pp. 383–396

CONDENSED MATTER PHYSICS

# Quantum codes from algebraic curves with automorphisms

T.Shaska

[1] 367 Science and Engineering Building, Department of Mathematics and Statistics, Oakland University, Rochester, MI, 48309

[2] University of Maria Curie Sklodovska, Lublin, Poland

Received January 31, 2008

Let $\mathcal{X}$ be an algebraic curve of genus $g \geqslant 2$ defined over a field $\mathbb{F}_q$ of characteristic $p > 0$. From $\mathcal{X}$, under certain conditions, we can construct an algebraic geometry code $C$. If the code $C$ is self-orthogonal under the symplectic product then we can construct a quantum code $Q$, called a QAG-code. In this paper we study the construction of such codes from curves with automorphisms and the relation between the automorphism group of the curve $\mathcal{X}$ and the codes $C$ and $Q$.

**Key words:** *algebraic curves, algebraic-geometry codes, quantum algebraic codes*

**PACS:** *03.67.Dd*

## 1. Introduction

In recent years there is an increased interest on the use of algebraic geometry in the theory of quantum cryptography and quantum coding. In this survey we study the way of constructing quantum codes from algebraic geometry codes (AG-codes). We call such codes quantum algebraic geometry codes (QAG-codes). Furthermore, we discuss the relation between the automorphism group of the algebraic curve, the automorphism group of the AG-code, and the automorphism group of the corresponding quantum code.

Throughout this paper $\mathcal{X}$ denotes a genus $g$ irreducible, algebraic curve defined over a finite field $\mathbb{F}_q$. Under certain conditions, starting with $\mathcal{X}$ one can construct an algebraic geometry code which we denote by $C_\mathcal{X}$. If $C_\mathcal{X}$ is self-orthogonal then from $C_\mathcal{X}$ we can construct a quantum code $Q_\mathcal{X}$, which will be called a QAG-code. The goal of this paper is to explore when the above constructions are possible. There are several papers in this area and a few algorithms, some of which have been implemented on some computer algebra systems. To our surprise the current versions of such algorithms have many weaknesses and their capabilities are quite limited. Also, their implementations are very inefficient when the size of the field increases. Our goal is to study how one can broaden the scope of these algorithms and improve their implementations. Such implementations will be discussed in detail in a subsequent paper.

In classical coding theory AG-codes with a large group of automorphisms have good error-correcting properties. Under certain conditions the automorphism group of the curve is embedded in the automorphism group of the corresponding code. Hence, AG-codes which come from algebraic curves with a large group of automorphisms are of special interest. Very little is known how the automorphism group of the quantum code $Q_\mathcal{X}$ relates to the automorphism group of $\mathcal{X}$ and $C_\mathcal{X}$. The second goal of this paper is to study the relation among such groups. Furthermore, we discuss this problem from the computational viewpoint. The existing algorithms for computing the automorphism group of curves and codes have some limitations.

It is interesting to note that our method of constructing QAG-codes is based on the existence of an automorphism of the curve $\mathcal{X}$. We focus on the algebraic curves with cyclic automorphism group, but other curves may be used as well. Hence, curves with non-trivial automorphism groups are of interest in this construction. In the last section we give a complete table of groups which occur as automorphism groups of curves of genus 3 and 4 over a field of characteristic 2. This paper is organized as follows:

In section 2 we give a brief description of the main definitions of algebraic geometry codes and stabilizer codes. This prepares for the construction of quantum codes when an algebraic curve $\mathcal{X}$ defined over a finite field $\mathbb{F}_q$ is given. Given a linear code $C$ in a vector space $V$, using the properties of stabilizer codes we can construct a quantum code if $C$ is self-dual under some symplectic form.

In section 3 we study the construction of quantum algebraic codes based on the existence of the rational points on the curve $\mathcal{X}$ and the existence of an involution $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathcal{X})$. We use this method to construct QAG-codes from hyperelliptic and non-hyperelliptic curves as well. In section 4 we illustrate this construction for hyperelliptic curves. We are able to easily construct many QAG-codes over small size fields and give an algorithm how this can be done in general.

In the last section we study the automorphism group of quantum codes. We compare the automorphism group $\mathrm{Aut}(\mathcal{X})$ of the curve $\mathcal{X}$ with the automorphism group of the corresponding quantum AG-code.

**Notation:** Throughout the paper $\mathbb{F}_q$ denotes a finite field of $q$ elements where $q$ is a prime power. The notation $[n, k, d]$ denotes a classical code of length $n$, dimension $k$, and minimum distance $d$. $[[n, k, d]]$ will denote a quantum code. A cyclic group of order $n$ is denoted by $C_n$. In general, given a genus $g \geqslant 2$ algebraic curve $\mathcal{X}$ defined over $\mathbb{F}$, the automorphism group of $\mathcal{X}$ is denoted by $\mathrm{Aut}(\mathcal{X})$ and is defined to be the group of automorphisms of $\mathcal{X}$ defined over the algebraic closure of $\mathbb{F}$. The group of automorphisms defined over $\mathbb{F}$ is denoted by $\mathrm{Aut}_{\mathbb{F}}(\mathcal{X})$.

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

## 2. Algebraic geometry codes and stabilizer codes

There are many ways of constructing quantum codes from the existing algebraic geometry codes. In this section we give a brief description of algebraic geometry codes, stabilizer codes, and quantum algebraic codes.

Let $\mathcal{X}$ be an algebraic curve defined over a finite field $\mathbb{F}_q$ with characteristic $p > 0$. By $\mathbb{F} = \mathbb{F}_q(\mathcal{X})$ we will denote the function field of $\mathcal{X}$.

### 2.1. Algebraic geometry codes

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

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

Define the following linear **evaluation map**

$$\varphi : \ \mathcal{L}(G) \to \mathbb{F}_q^n , \qquad f \mapsto (f(P_1), \dots, f(P_n)). \tag{1}$$

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

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

The parameter $d_{\mathrm{des}}$ is called the **designed distance** of the Goppa code. 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

$$\begin{aligned} k &= \dim G \geqslant \deg G + 1 - g, \\ d &\geqslant n - \deg G. \end{aligned}$$

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 $C_{\mathcal{L}}(D,G)$.

Let $D = P_1 + \cdots + P_n$ be a divisor, where the $P_i$'s are places of degree one of an algebraic function field $F/\mathbb{F}_q$, Furthermore, let $G$ be a divisor with $supp(G) \cap supp(D) = \emptyset$. Then we define the code $C_\Omega(D,G)$ by

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

The following result is well known:

**Lemma 1.** *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* $\eta$ *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. $C_{\mathcal{L}}(D,G)^\perp = a \cdot C_{\mathcal{L}}(D,H)$.

One common construction is the so-called one point code. We define as admissible a class of curves which have some additional conditions on their divisors.

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

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

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

Next we define

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

Let $\mathcal{X}/F_q$ be an admissible curve over $F_q$ of genus $g$ where $l > k$. Assume that $m \geqslant l$. 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 $\mathcal{X}$. The one point code of level $m$ is the code

$$\mathcal{L}(D, mP_\infty).$$

With the above notation we have the following:

**Lemma 2.** *Let $\mathcal{X}/F_q$ be an admissible curve over $F_q$ of genus $g$ where $l > k$. Assume that $m \geqslant l$. 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*

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

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

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

*Proof.* See [18] for details. □

Next we give a brief introduction to the way of constructing quantum codes from algebraic geometry codes.

### 2.2. Stabilizer codes

Stabilizer codes are helpful devices that make possible the construction of quantum codes from classical codes. Let $V$ denote the qubit state space and $G_n$ the Pauli group on $n$ qubits. Let $H \leqslant G_n$ and denote by $V_H$ the subspace of $V$ fixed by $H$;

$$V_H := \{v \in V \mid gv = v, \forall g \in G_n\}.$$

The proof of the following lemma is elementary.

**Lemma 3.** *$V_H$ is non-trivial if and only if $H$ is Abelian and $-I \notin H$.*

From now on we will assume that $H$ is Abelian and $-I \notin H$. The subspace $V_H$ is called the **stabilizer code** $C(H)$ of $H$. For a proof of the following see [2].

**Proposition 1.** *Let $\{E_i\}$ be a set of operators in $G_n$ such that $E_j^\dagger E_k \notin N(H) \setminus H$ for all $j$ and $k$, where $E^\dagger$ denotes the adjoint of $E$. Then $\{E_j\}$ is a correctable set of errors for the code $C(H)$.*

**Corollary 1.** *Let $H$ be an Abelian subgroup of $G_n$. If a state $|\psi\rangle$ is in the $+1$ eigenspace of a set of generators $\{g_1, \dots, g_l\}$ of $H$, it is an eigenstate of all elements in $H$.*

Since we have seen that it suffices to look at a set of generators, we can represent a stabilizer code in an easier way. A **generator matrix** $\mathcal{G}$ of a stabilizer code is an $l \times 2n$-matrix $\mathcal{G}(X|Z)$ where the first $n$ components represent the $X$ errors, the second $n$ components represent the $Z$ errors. This matrix defines a $[[n,\, k,\, d]]$ quantum error correcting code with $k = n - l$.

The **weight** $wt$ of an operator $U_1 \otimes \dots \otimes U_n$ is the number of elements $U_i$ that are not equal to the identity.

Let $E \in G_n$ be an error operator. Then:

1. If $E \in H$ then $E$ is a codeword.
2. If $E \in G_n \backslash N(H)$ the error is detectable and can be corrected.
3. If $E \in N(H) \backslash H$ the error cannot be detected and therefore is not correctable.

The above allows us to introduce the distance of a stabilizer code. The **distance** $d$ of a quantum stabilizer code $C$ is the minimum weight of all normalizer elements that are not in the stabilizer.

$$d = \min \{wt(x) \mid x \in N(H) \backslash H\}.$$

Let $x = (x_1, \dots, x_{2n}),\ y = (y_1, \dots, y_{2n}) \in F_q^{2n}$. We call $\langle x, y\rangle_s$ the **standard symplectic inner product**,

$$\langle x, y\rangle_s = \sum_{i=1}^n x_i y_{n+i} - x_{n+i} y_i\,.$$

The stabilizer code of the normalizer $N(H)$ is equal to the dual code $C^{\perp_s}$ with respect to the symplectic inner product $\langle\, ,\, \rangle_s$. We obtain that

$$d = \min \left\{ wt(x) \mid x \in C^{\perp_s} \backslash C \right\}.$$

The next proposition gives a way of constructing quantum codes from classical codes; see [2] for details.

**Proposition 2.** *Let $C \subset F_q^{2n}$ be a $(n+k)$-dimensional subspace such that $C^{\perp_s} \subset C$. Then, there exists a quantum code $Q \subset \mathcal{H}^{\otimes n}$ of dimension $q^k$ and minimum distance $d := \dim C \setminus C^{\perp_s}$.*

Hence, in order to construct quantum AG-codes we need to construct AG-codes which are self-orthogonal.

## 3. Quantum algebraic geometry codes from algebraic curves with automorphisms

We continue with the notation of the previous session; $\mathcal{X}$ is a genus $g$ curve defined over a finite field $\mathbb{F}_q$ and $F$ is its function field. The following lemma is cited from [11, Prop. VII.1.2]. It permits to construct differentials with special properties that help to construct a self-orthogonal code.

**Lemma 4.** *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 $i = 1, \dots, n$. Then the differential $\eta := x \cdot \frac{dy}{y}$ satisfies $v_{P_i}(\eta) = -1$ and $\operatorname{res}_{P_i}(\eta) = 1$ for $i = 1, \dots, n$.*

First, we show under which circumstances a quantum stabilizer code can be obtained from an algebraic geometric construction.

**Theorem 1.** *Let $\mathcal{X}$ be a genus $g$ irreducible algebraic curve defined over $\mathbb{F}_q$ and $P_1, \dots, P_n$ degree one rational points on $\mathcal{X}$. Let $\sigma \in Aut_{\mathbb{F}}(\mathcal{X})$ be an involution such that $\sigma P_i \neq P_j$, $\forall\, i, j = 1, \dots, n$. Further assume that we have a divisor $G$ such that $\sigma G = G$, $v_{P_i}(G) = v_{\sigma P_i}(G) = 0$ for all $i$. Then, there exists a quantum code $Q_{\mathcal{X}} = [[n, k, d]]$ such that*

$$k = \dim G - \dim\left(G - P_1 - \cdots P_n - \sigma(P_1) - \cdots \sigma(P_n)\right) - n, \quad d \geqslant n - \left\lfloor \frac{deg\ G}{2} \right\rfloor.$$

*Proof.* Let $\mathbb{F} = F_q(\mathcal{X})$ be the function field of $\mathcal{X}$. Let $P_1, \dots, P_n$ be pairwise distinct places of degree one such that $\sigma P_i \neq P_j$, $\forall\, i, j = 1, \dots, n$. Then, by a strong approximation theorem there is a differential $\eta$ such that

$$\begin{cases} v_{P_i}(\eta) = v_{\sigma P_i}(\eta) = -1, \\ res_{P_i}(\eta) = 1, \\ res_{\sigma P_i}(\eta) = -1. \end{cases} \tag{2}$$

Further assume that we have a divisor $G$ such that $\sigma G = G$, $v_{P_i}(G) = v_{\sigma P_i}(G) = 0$ for all $i$. Define

$$C(G) = \{(f(P_1), \dots, f(P_n), f(\sigma P_1), \dots, f(\sigma P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^{2n}.$$

Let

$$H = (P_1 + \cdots + P_n + \sigma P_1 + \cdots + \sigma P_n) - G + (\eta),$$

where $\eta$ is as in equation (2). Then, we have $C(G)^{\perp_s} = C(H)$.

Let us assume that $H \leqslant G$. Then, $\mathcal{L}(H) \subset \mathcal{L}(G)$. Hence, $C(D, G)^{\perp_s} \subset C(D, G)$. We have $k = \dim C(D, G) - n$ which implies the result.

Let $f \in \mathcal{L}(G)$ such that wt $(f(P_1), \dots, f(\sigma(P_n)) = \delta \neq 0$. Hence, there exists a set of coordinates $f(P_1), \dots, f(P_{i-\delta})$ which are all zero. Thus, we have $f \in \mathcal{L}\left(G - \sum_{j=1}^{n-\delta}(P_{i,j} + \sigma P_{i,j})\right)$. The dimension of this space is $> 0$, which implies the result.

□

Next, we should like to construct quantum codes starting from algebraic curves which have nontrivial automorphisms. The most common class of curves are obviously the hyperelliptic curves. However, we start in a more general setting. Our first class of curves are the curves that have a cyclic group embedded in the automorphism group of the curve. The hyperelliptic curves will be studied more in detail in the next section.

### 3.1. Codes on the cyclic covers of the projective line

Let $k$ be a field of characteristic $p > 0$ and $F_0 = k(x)$ a function field of the projective line $\mathbb{P}^1(k)$. We consider a degree $r$ cyclic extension $F := k(x, y)$, where

$$y^r = f(x) = \prod_{i=1}^{s}(x - \alpha_i)^{d_i}, \quad 0 < d_i < m$$

for some fixed $m \in \mathbb{Z}^+$. The only places of $F_0$ that ramify are the places that correspond to the points $x = \alpha_i$. We denote such places by $Q_1, \dots, Q_s$ and by $\mathcal{B} := \{Q_1, \dots, Q\}$ the set of these places. The ramification indexes are $e(Q_i) = \frac{r}{(r,d_i)}$.

Let $\mathcal{X}$ denote the algebraic curve with affine equation

$$y^r = f(x)$$

defined over $k$, and let $G := \text{Aut}\ (\mathcal{X})$ be the automorphism group. Then, there is a cyclic group $C_r = Gal(F/F_0)$ of order $r$ such that $C_r \hookrightarrow \text{Aut}\ (\mathcal{X})$. Fix a generator $\sigma \in C_r$.

**Lemma 5.** *Let $\tau \in Aut\ (\mathcal{X})$ such that $\tau \notin C_r$, $s$ be the number of ramified places of the extension $F/F_0$, and $d = \deg f(x)$. Then, the equation of the curve is given by*

$$y^r = f(x^\delta)$$

*for some $\delta | d$. Moreover, $f(x^\delta)$ is a monic polynomial with constant coefficient 1.*

*Proof.* It can be easily obtained from [1, Lemma 2.3] or from the results in [13], [6] that the defining equation of $F$ is

$$y^2 = \sum_{i=0}^{d/\delta} a_i x^{\delta \cdot i}.$$

Since $\mathcal{X}$ is a smooth algebraic curve, the discriminant of the right hand side should be non-zero. Hence, all $d_i = 1$, $i = 1, \dots, s$. Hence, $s = d$. The rest follows. $\square$

Let $\mathcal{X}$ be an algebraic curve defined over a field $\mathbb{F}_q$ of characteristic $p > 0$ given by an equation

$$y^r = f(x^\delta),$$

where $d = \deg f(x)$. Let $C_r \hookrightarrow \text{Aut}\ (\mathcal{X})$ such that $C_r = \langle \sigma \rangle$. The corresponding cover $\psi := \mathcal{X} \to \mathcal{X}^\sigma$ has $d$ branch points. Let $\mathcal{B}$ be the branch set. For a given rational point $P \in \mathcal{X}$ we define $\mathcal{O}rb_\alpha(P) = \{\sigma(P) \in X\}$. If $\psi(P) \notin \mathcal{B}$ then $|\mathcal{O}rb_\sigma(P)| = r$.

Let $P_1, \dots, P_n$ be rational points on $\mathcal{X}$ such that $\psi(P_i) \notin \mathcal{B}$ for all $i = 1, \dots, n$. Define the divisor

$$D = \sum_{i=1}^n \left( P_i + \sigma(P_i) + \cdots + \sigma^{r-1}(P_i) \right) = \sum_{i=1}^n \mathcal{O}rb(P_i) \,.$$

Then $\deg D = rn$. For some $P \in \mathcal{X}$ such that $\psi(P) \in \mathcal{B}$ we define $G = mP$ for some integer $m$. Then $\sigma(G) = G$. We can take infinity to be one of the branch points in $\mathcal{B}$. In that case the point $P$ is the fiber is denoted by $P_\infty$. It is common in coding theory to take $G$ to be $mP_\infty$.

We define an algebraic geometry code as previously $C_\mathcal{X} = \mathcal{L}(G, D)$. The proof of the following theorem is similar to that of Theorem 1.

**Theorem 2.** *Let $\mathcal{X}$ be an algebraic curve defined over a field $\mathbb{F}_q$ of characteristic $p > 0$ such that $C_r = \langle \sigma \rangle \hookrightarrow Aut\ (\mathcal{X})$. Let $P_1, \dots, P_n$ be rational points on $\mathcal{X}$ such that $|\mathcal{O}rb_\sigma(P_i)| = r$ and $\mathcal{O}rb_\sigma(P_i) \cap \mathcal{O}rb_\sigma(P_j) = \emptyset$ for all $i, j$. Further assume that we have a divisor $G$ such that $\sigma G = G$, $v_{P_i}(G) = v_{\sigma P_i}(G) = 0$ for all $i$. Then, there exists a quantum code $Q_\mathcal{X} = [[nr, k, d]]$ such that*

$$k = \dim G - \dim(G - D) - n\, r, \quad d \geqslant n\, r - \left\lfloor \frac{deg\ G}{2} \right\rfloor .$$

**Example 1.** Let $\mathcal{X}$ be the curve

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

defined over $\mathbb{F}_q$. For characteristic $p > 7$, Aut $(\mathcal{X})$ is a group of order 96 with Gap identity $(96, 64)$. Denote the set of affine rational points of $\mathcal{X}$ over $\mathbb{F}_q$ by $\{P_1, \dots, P_n\}$. Let $C = C_\mathcal{L}(D, G)$, where $n + 1$ is the number of rational points of $\mathcal{X}$ and

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

The permutation automorphism group PAut $(C)$ is as follows:

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

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

For a proof of the above statement see [15].

Let $\mathcal{X}$ be defined over $F_4$. 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 $\alpha$ is a primitive element of $F_4$. 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. The automorphism group $\Gamma$Aut $(C)$ has Gap identity $(1944, 3876)$. Next we construct a quantum code from this curve. One can check that this code is self-orthogonal with respect to the inner product. Hence, there is a quantum code $Q$ which has parameters $[[4, 4]]$. Its automorphism group is of the order 31104 and is a degree 2 extension of $\Gamma$Aut $(C)$.

□

It is obvious from the above theorem that to construct quantum codes from algebraic geometry codes we have to start with algebraic curves having many rational points. Hence, we have to look at classes of curves which are normally used to construct AG-codes. Thus, Hermitian curves, hyperelliptic curves, and more generally $C_{ab}$ curves, seem to be good candidate curves. From the above construction, we also need to have algebraic curves with at least one involution. Hence, we want curves with automorphisms and with many rational points. An obvious class of curves which assures the existence of an involution are of course the hyperelliptic curves. They will be the focus of the next section. However, we should mention that there are many other classes of curves that have an involution. Many questions remain unanswered about the choice of the involution. Does the choice of the involution determine any of the parameters of the code? Does the size of the automorphism group of the curve have any effect on the corresponding algebraic geometry code or the corresponding quantum code. Very little is known in this field. In the next section we will see how the hyperelliptic involution can be used to construct quantum algebraic geometry codes. However, other involutions can be used as well.

## 4. Hyperelliptic quantum codes

The goal of this section is to construct quantum stabilizer codes starting with AG-codes which come from hyperelliptic curves. We focus on odd characteristic. Let $K := \mathbb{F}_{p^m}$ be a finite field of characteristic $p > 2$, and $\mathcal{X}_g$ a genus $g$ hyperelliptic curve given by the equation $y^2 = f(x)$. Let $F := K(x, y)$ be the function field and $\sigma$ denotes the hyperelliptic involution of $\mathcal{X}_g$. Then $F$ has a set of rational places which are not fixed by the hyperelliptic involution. Choose a set of distinct places in $F$ such that

$$SP = \{P_1, \dots, P_n, \sigma(P_1), \dots, \sigma(P_n)\},$$

such that $\pi(P_i) = \alpha_i$, where $\pi$ is the hyperelliptic projection.

Let $P_\infty$ denote the place at infinity and $D, G \in$ Jac $(\mathcal{X}_g)$ be as follows:

$$D := \sum_{i=1}^{n} P_i \; + \; \sum_{i=1}^{n} \sigma(P_i) \quad \text{and} \qquad G := (n + g - 1 - r)P_\infty,$$

where $0 \leqslant r \leqslant n-g$. Then $D$ has degree $2n$. By the Riemann's theorem there exists $\eta \in F$ such that

$$\eta = \frac{1}{y \prod_{i=1}^{n}(x-\alpha_i)} \mathrm{d}x \,.$$

Hence, $(\eta) = (2n+2g-2)P_\infty - D$. We denote

$$W := (\eta) = (2n+2g-2)P_\infty - D, \text{ and } \quad H := D - G + W.$$

Then $W$ is a canonical divisor. and the residues of $\eta$ at the places $P_1, \ldots, P_n$, $\sigma(P_1), \ldots, \sigma(P_n)$ satisfy

$$a_i := \mathrm{res}_{P_i}(\eta) = -\mathrm{res}_{\sigma(P_i)}(\eta) \,.$$

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

Now we can construct a Goppa codes $C(D,G)$ and $C(D,H)$. The weighted symplectic inner product is defined as below

$$\langle x, y\rangle_s^a = \sum_{i=0}^{C} 4na_i\left(x_i y_{n+i} - x_{n+i} y_i\right)$$

for all $x, y \in C$ and all $a_i \neq 0$.

**Lemma 6.** *Let $C(D,G)$ and $C(D,H)$ be as above. Then*

$$C(D,G)^{\perp_s} = C(D,H) \cdot \mathrm{diag}(a_1, \ldots, a_n, 1, \ldots, 1).$$

*Moreover, $C(D,G) \subseteq C(D,G)^{\perp_s^a}$ with respect to the symplectic inner product $\langle\ ,\ \rangle_s^a$.*

*Proof.* Since $G = (n+g-1-r)P_\infty$ then we replace $(\eta)$ to get $H = (n+g-1+r)P_\infty \geqslant G$. Hence, $\mathcal{L}(G) \subset \mathcal{L}(H)$ and $C(D,G) \subset C(D,H)$. From the above lemma we have that $C(D,G)^{\langle a,s\rangle_s^a} = C(D,H)$.

□

We transform $C(D,G)$ to a self-orthogonal code $C'(D,G)$ with respect to the standard symplectic inner product by multiplying each component $x_i$ of every codeword by the corresponding $a_i$, for $1 \leqslant i \leqslant n$.

Then, we have the following:

**Proposition 3.** *$C'(D,G)$ is a stabilizer code with parameters $[[n,\, k,\, d]]$, where $k = g+r-1$ and $d \geqslant \frac{n-k}{2}$.*

*Proof.* We can construct a stabilizer code since $C'(D,G)$ is self-orthogonal; see Theorem 1. The new code has the same parameters with $C'(D,G)$. So it is left to compute $k$ and $d$. From the Riemman-Roth theorem we have that

$$k = \dim H - \dim(H-D) - n = (n+g-1+r) - n = g+r-1,$$

since $\dim(H-D) = 0$. For $d$ we have $d \geqslant n - \lfloor \frac{\deg H}{2} \rfloor \geqslant \frac{n-k}{2}$.

□

We summarize in the following theorem.

**Theorem 3.** *Let $\mathcal{X}$ be a genus $g$ irreducible hyperelliptic curve defined over $\mathbb{F}_q$ and $P_1, \ldots, P_n$ be degree one rational points on $\mathcal{X}$. Let $\sigma \in Aut_{\,\mathbb{F}}(\mathcal{X})$ be an involution such that $\sigma P_i \neq P_j$, $\forall\, i,j = 1, \ldots, n$. Further assume that we have a divisor $G$ such that $\sigma G = G$, $v_{P_i}(G) = v_{\sigma P_i}(G) = 0$ for all $i$. Then, there exists a quantum code $Q_{\mathcal{X}} = [[n,k,d]]$ such that*

$$k = \dim G - \dim\left(G - P_1 - \cdots P_n - \sigma(P_1) - \cdots \sigma(P_n)\right) - n, \quad d \geqslant n - \left\lfloor \frac{deg\ G}{2} \right\rfloor.$$

In the next section we study the relation between the automorphism groups of the curve $\mathcal{X}_g$, and the codes $C_{\mathcal{X}}$ and $Q_{\mathcal{X}}$.

### 4.1. Explicit construction of quantum AG-codes

Next we describe an algorithm which would create a hyperelliptic quantum code.

**Algorithm 1.** Hyperelliptic quantum codes

*Input:* A genus $g$ hyperelliptic curve over a finite field $\mathbb{F}_q$.
*Output:* A quantum code $Q$

i) *Find all rational places of degree 1 of $\mathcal{X}_g$ which are not fixed by the hyperelliptic involution, say $S = \{P_1, \dots, P_n, \sigma(P_1), \dots, \sigma(P_n)\}$.*

ii) *Let*

$$D := \sum_{P \in S} (P + \sigma(P))\,, \qquad G := (n + g - 1 - r)P_\infty\,, \qquad (\eta) := -D + (2n + 2g - 2)P_\infty\,.$$

iii) *Create a list $A = [a_1, \dots, a_n]$, where $a_i := res_{P_i}(\eta) = -res_{\sigma(P_i)}(\eta)$.*

iv) *Construct the AG code $C = \mathcal{L}(D, G)$ and let the generator matrix of $C$ be $\mathcal{G}$.*

v) Transform $C$ to a self-orthogonal symplectic code $Q$ by multiplying each coordinate $x_i$ by $a_i$,

$$(\dots, x_i, \dots) \to (\dots, a_i x_i, \dots).$$

vi) Return $Q$.

## 5. Automorphism groups

In this section we give a brief survey of automorphism groups of curves over finite fields, automorphism groups of codes, and automorphism groups of quantum codes.

### 5.1. Automorphism groups of curves

It has been known since Hurwitz (1892) that a Riemann surface of genus $g > 1$ has at most $84(g-1)$ automorphisms. This estimate is optimal; there are Riemann surfaces of arbitrarily high genus with $84(g-1)$ automorphisms (Hurwitz' bound in characteristic 0), the Klein curve most notable of them. The Hurwitz estimate is not valid in prime characteristic. Roquette (1970) found that the estimate

$$|G| \leqslant 84(g-1),$$

on the order of the automorphism group $G$, holds under the additional assumption $p > g+1$, with one exception: the function field $F = K(x, y)$ with $y^p - y = x^2$ has genus $g = \frac{1}{2}(p-1)$ and $8g(g+1)(2g+1)$ automorphisms.

Stichtenoth (1973) gives a general estimate for the number of automorphisms of a smooth projective curve in characteristic $p > 0$. He proves the inequality

$$|G| < 16 \cdot g^4,$$

but also with one series of exceptions: the function field $F = K(x, y)$ with $y^{p^n} + y = x^{p^{n+1}}$ has genus $g = \frac{1}{2}p^n(p^n - 1)$ and $|G| = p^{3n}(p^{3n} + 1)(p^{2n} - 1)$ automorphisms, so $|G|$ is in this case slightly larger than $16g^4$.

Let $X$ denote a smooth, genus $g$ algebraic curve defined over $k$, char $k = p > 0$. A theorem of Blichfeld on invariants (in char 0) of subgroups of $PGL_3(k)$ implies that the genus $g$ curve lifts to characteristic 0 for $p > 2g+1$; see [**?**, pg. 236-254]. Hence, for large enough $p$ (i.e., $p > 2g+1$), methods described in [**?**] can be used to determine such groups. Thus, to determine the list of groups that occur as automorphism groups of genus $g$ curves we have to classify the groups that occur for all primes $p \leqslant 2g+1$.

### 5.1.1. Automorphisms groups over finite fields of characteristic 2

Let $C$ be a hyperelliptic curve of genus $g$ over an algebraically closed field K of characteristic 2. We use an Artin-Schreier generation $y^2 + y = g(x)$ such that $g(x) \in K(x)$. We can find a rational function $h(x) \in K(x)$ such that the rational function $g(x) + h(x) + h(x)^2$ has no poles of even order. Let $f(x) := g(x) + h(x) + h(x)^2$ and use the normalized form $y^2 + y = f(x)$. Then, $y$ is unique up to transformations of the form $y \longmapsto y + B(x)$, where $B(x)$ is a rational function of $x$.

Let $\Sigma n_a(a)$ be the polar divisor of $f(x)$ on the projective line, $\mathbf{P}^1$. $C$ is ramified at each $a$ and if $P_a$ is the unique point of $C$ over $a$ then the curve $y^2 + y = f(x)$ has the different

$$\mathrm{Diff}(C/\mathbf{P}^1) = \Sigma(n_a + 1)P_a\,,$$

where the $n_a$ are odd ([10], Prop III.7.8)

$$2g - 2 = -2[F : K(x)] + deg(Diff(C/\mathbf{P}^1)) \implies deg(Diff(C/\mathbf{P}^1)) = 2g + 2.$$

Take two hyperelliptic curves, $C : y^2 + y = f(x)$ and $C' : y^2 + y = h(x)$. Then there are finite morphisms $f_1 : C \longmapsto \mathbf{P}^1$, and $f_2 : C' \longmapsto \mathbf{P}^1$ of degree 2, and there exists a unique automorphism $\sigma$ of $\mathbf{P}^1$ such that $f_2 = \sigma \circ f_1$. Any isomorphism between these curves has the form

$$(x, y) \longmapsto (\frac{ax + b}{cx + d}, y + B(x))$$

for some $B(x) \in K(x)$. Hence, these curves are isomorphic if and only if

$$h(x) = f(\frac{ax + b}{cx + d}) + s(x) + s(x)^2$$

for some $s(x) \in K(x)$. The ramification types determine the isomorphism classes of the hyperelliptic curves. The solutions of the equation $\Sigma(n_a + 1) = 2g + 2$ in the unknown odd positive integers give us the following ramification types:

$$\begin{aligned} &(1,1,1,1), (3,1,1), (3,3), (5,1), (7) \quad for\ genus\ 3,\\ &(1,1,1,1,1), (3,1,1,1), (3,3,1), (5,1,1), (5,3), (7,1), (9) \quad for\ genus\ 4. \end{aligned} \tag{3}$$

Therefore, we get the following normal forms for genus 3 and 4 respectively.

$$\begin{aligned} y^2 + y &= \begin{cases} \alpha_1 x + \alpha_2 x^{-1} + \alpha_3 (x-1)^{-1} + \alpha_4 (x-\lambda)^{-1} \\ x^3 + \alpha x + \beta x^{-1} + \gamma (x-1)^{-1} \\ x^3 + \alpha x + \beta x^{-3} + \gamma x^{-1} \\ x^5 + \alpha x^3 + \beta x^{-1} \\ x^7 + \alpha x^5 + \beta x^3 \end{cases} \\ y^2 + y &= \begin{cases} \alpha_1 x + \alpha_2 x^{-1} + \alpha_3 (x-1)^{-1} + \alpha_4 (x-\lambda)^{-1} + \alpha_5 (x-\mu)^{-1} \\ x^3 + \alpha x + \beta_1 x^{-1} + \beta_2 (x-1)^{-1} + \beta_3 (x-\lambda)^{-1} \\ x^3 + \alpha x + \beta x^{-3} + \gamma x^{-1} + \sigma (x-1)^{-1} \\ x^5 + \alpha x^3 + \beta x^{-1} + \gamma (x-1)^{-1} \\ x^5 + \alpha x^3 + \beta x^{-3} + \gamma x^{-1} \\ x^7 + \alpha x^5 + \beta x^3 + \gamma x^{-1} \\ x^9 + \alpha_1 x^7 + \alpha_2 x^5 + \alpha_3 x^3 \end{cases} \end{aligned} \tag{4}$$

These are plane curves given in inhomogeneous form, birational to the given nonsingular curves( i.e. the function fields are isomorphic). We will use the above normal forms to determine $\bar{G}$, the reduced group of automorphisms, namely the quotient of the group of automorphisms, $G$ by $\langle \iota \rangle$ which is contained in the center of $G$. And then we will compute $G$.

**Proposition 4.** *Let $C$ be a genus $g$ hyperelliptic curve defined over an algebraically closed field $K$ of characteristic 2.*

*i) If $g = 3$ then the automorphism group of $C$ is one of the following: $C_2$, $C_4$, $V_4$, $C_2 \times C_2 \times C_2$, $C_6$, $C_{14}$, $D_{12}$.*

*ii) If $g = 4$ then the automorphism group of $C$ is one of the following: $C_2$, $V_4$, $C_4$, $C_2 \times C_2 \times C_2$, $C_6$, $C_{18}$, $D_{20}$.*

*Proof.* See [3] for details. □

Furthermore, the parametric equation of the curve in each case is given by equation in table 1.

**Table 1.** Automorphism groups of hyperelliptic curves of genus 3 and 4 over fields of characteristic 2.

| Curve | Condition | $G$ |
|---|---|---|
| g=3 | | |
| $y^2 + y = \alpha_1 x + \alpha_2 x^{-1}$ $+\alpha_3(x-1)^{-1} + \alpha_4(x-\lambda)^{-1}$ | $\alpha_1 = \alpha_2\lambda^{-1}, \alpha_3 = \alpha_4\lambda^{-1}, \alpha_1 \neq \alpha_3\lambda$ | $V_4$ |
| | $\alpha_1 = \alpha_3\lambda$, $\alpha_2 = \alpha_4\lambda$, $\alpha_1 \neq \alpha_2\lambda^{-1}$ | $V_4$ |
| | $\alpha_1 = \alpha_4$, $\alpha_2 = \alpha_3\lambda^2$, $\alpha_1 \neq \alpha_2\lambda^{-1}$ | $V_4$ |
| | $\alpha_1 = \alpha_2\lambda^{-1}, \alpha_3 = \alpha_4\lambda^{-1}, \alpha_1 = \alpha_3\lambda$ | ${C_2}^3$ |
| $y^2 + y = x^3 + \alpha x$ $+\beta x^{-1} + \gamma(x-1)^{-1}$ | $\alpha \neq 0$, or $\beta \neq \gamma$ | $C_2$ |
| | $\alpha = 0$, and $\beta = \gamma$ | $V_4$ |
| $y^2 + y = x^3 + \alpha x$ $+x^{-3} + \beta x^{-1}$ | none | $C_2$ |
| | $\beta \neq 1, \alpha = \gamma = 0$ | $C_6$ |
| | $\beta = 1, \alpha = \gamma \neq 0$ | $V_4$ |
| | $\beta = 1, \alpha = \gamma\zeta \neq 0$ | $V_4$ |
| | $\beta = 1, \alpha = \gamma\zeta^2 \neq 0$ | $V_4$ |
| | $\beta = 1, \alpha = \gamma = 0$ | $D_{12}$ |
| $y^2 + y = x^5 + \alpha x^3 + \beta x^{-1}$ | none | $C_2$ |
| $y^2 + y = x^7 + \alpha x^5 + \beta x^3$ | $\alpha = \beta = 0$ | $C_{14}$ |
| | $\alpha = 0, \beta \neq 0$ | $C_2$ |
| | $\alpha \neq 0, \beta = c_3 = 0$ | $C_2$ |
| | $\alpha \neq 0, \beta = 0, c_3 \neq 0$ | $C_{14}$ |
| | $\alpha \neq 0, \beta \neq 0, c_3 = 0$ | $C_2$ |
| | $\alpha \neq 0, \beta \neq 0, c_3 \neq 0$ | $C_{14}$ |
| g =4 | | |
| $y^2 + y = \alpha_1 x + \alpha_2 x^{-1} + \alpha_3(x-1)^{-1}$ $+\alpha_4(x-\lambda_1)^{-1} + \alpha_5(x-\lambda_2)^{-1}$ | $\alpha_2 = \alpha_3, \alpha_4 = \alpha_5, \alpha_2 \neq \alpha_4$ | $V_4$ |
| | $\alpha_2 = \alpha_4, \alpha_3 = \alpha_5, \alpha_2 \neq \alpha_3$ | $V_4$ |
| | $\alpha_2 = \alpha_5, \alpha_3 = \alpha_4, \alpha_2 \neq \alpha_3$ | $V_4$ |
| | $\alpha_2 = \alpha_3 = \alpha_4 = \alpha_5$ | ${C_2}^3$ |
| | $\alpha_1 = \alpha_2 = \alpha_3\lambda = \alpha_4\lambda = \alpha_5$ | $D_{20}$ |
| | $\alpha_1 = \alpha_2 = \alpha_3\lambda^{-1} = \alpha_4 = \alpha_5\lambda^{-1}$ | $D_{20}$ |
| | $\cdots$ | $\cdots$ |
| | $\cdots$ | $\cdots$ |
| $y^2 + y = x^3 + \alpha x + \beta_1 x^{-1}$ $+\beta_2(x-1)^{-1} + \beta_3(x-\lambda)^{-1}$ | $\alpha \neq 0$ | $C_2$ |
| | $\alpha = 0, \beta = \gamma\lambda, \gamma = \sigma\lambda, \sigma = \beta\lambda$ | $C_6$ |
| $y^2 + y = x^3 + \alpha x$ $+x^{-3} + \beta x^{-1} + \gamma(x-1)^{-1}$ | none | $C_2$ |
| | $\beta = 1, \alpha = \gamma$ | $V_4$ |
| $y^2 + y = x^5 + \alpha x^3$ $+\beta x^{-1} + \gamma(x-1)^{-1}$ | $\alpha \neq 0, or 1$ | $C_2$ |
| | $\alpha = 0$ | $V_4$ |
| | $\alpha = 1$ | $C_4$ |
| $y^2 + y = x^5 + \alpha x^3 + x^{-3} + \beta x^{-1}$ | none | $C_2$ |
| $y^2 + y = x^7 + \alpha x^5 + \beta x^3 + \gamma x^{-1}$ | none | $C_2$ |
| $y^2 + y = x^9 + \alpha_1 x^7 + \alpha_2 x^5 + \alpha_3 x^3$ | $\alpha_1 \neq 0$ | $C_2$ |
| | $\alpha_1 = 0$ | $C_{18}$ |

Determining complete lists of full automorphism groups for a given genus $g > 3$ is still an open problem with tremendous applications in theoretical mathematics and computer science and electrical engineering. For more details on this problem see [12].

### 5.2. Automorphism groups of codes

The **permutation automorphism group** of the code $C \subseteq \mathbb{F}_q^n$ is the subgroup of $S_n$ (acting on $\mathbb{F}_q^n$ by coordinate permutation) which preserves $C$. We denote this 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 $\gamma$ be a field automorphism of $\mathbb{F}_q$ and $M$ a monomial matrix. Denote by $M_\gamma$ the map $M_\gamma : C \to C$ such that $\forall \mathrm{x} \in \mathrm{C}$ we have $M_\gamma(\mathrm{x}) = \gamma(\mathrm{Mx})$. The set of all maps $M_\gamma$ forms the **automorphism group** of $C$, denoted by $\Gamma$Aut $(C)$. It is well known that

$$\mathrm{PAut}\ (C) \leqslant \mathrm{MAut}\ (C) \leqslant \Gamma\mathrm{Aut}\ (C).$$

Recall that for binary codes PAut $(C)$ = MAut $(C)$ = $\Gamma$Aut $(C)$, which we simply denote by Aut $(C)$. If the code $C$ is defined over a prime field then MAut $(C)$ = $\Gamma$Aut $(C)$. Two codes $C$ and $C'$ are called **permutation equivalent**, **monomially equivalent**, or **equivalent** if there is an element $\sigma$ in the respective automorphism group such that $\sigma(C) = C'$. In classical coding theory these automorphism groups of codes play an important role in classifying codes. There is a weight preserving linear transformation between $[n, k]$ codes $C$ and $C'$ over $\mathbb{F}_q$ if and only if $C$and $C'$ are monomially equivalent. Furthermore, the linear transformation agrees with the associated monomial transformation on every codeword in $C$; see [4, Thm. 7.9.4].

If $\mathcal{X}$ is a genus $g \geqslant 2$ algebraic curve defined over $\mathbb{F}_q$ then Aut $(\mathcal{X})$ is the group of automorphisms of $\mathcal{X}$ over the algebraic closure of $\mathbb{F}_q$. There have been published many papers studying the relation between the automorphism group of the algebraic curve $\mathcal{X}$ and the automorphism groups as defined above of the corresponding AG-code $C_\mathcal{X}$; see [15] among others. Let us assume that $C_\mathcal{X}$ is a self-orthogonal code such that we can construct a quantum code $Q_\mathcal{X}$ as in the previous section. If $Q$ is a symplectic quantum code, then the group of equivalences of the code is the complex Clifford group.

### 5.3. Some computational remarks on the automorphism groups of codes

In this section we want to make a few remarks concerning the efficiency of computing the automorphism group of a given code. There are several open questions related to automorphism groups of algebraic curves, AG-codes, and naturally quantum codes. We suggest some problems and point some inefficiencies regarding some existing programs.

**Problem 1.** Let $\mathcal{X}$ be a genus $g$ curve defined over a finite field $F_q$. Determine the list of groups that occur as full groups of automorphisms of $\mathcal{X}$ over the algebraic closure of $\mathbb{F}_q$.

**Problem 2.** Let $\mathcal{X}$ be a genus $g$ curve defined over a finite field $F_q$. Design and implement a program that computes the automorphism group of $\mathcal{X}$ over $\mathbb{F}_q$.

Let $C_\mathcal{X}$ and $Q_\mathcal{X}$ be the codes constructed as in sections 2 and 3. In GAP, the package GUAVA which is specifically written for coding theory, creates such codes (with some simple implementations of our algorithms) and computes groups of such codes using an algorithm of Leon [5]. Similar capabilities are also available in Magma. Both MAGMA and GAP come short when it comes to computing the automorphism group of a code over a relatively large size field $\mathbb{F}_q$. Magma only computes automorphism groups of codes over a field $\mathbb{F}_q$ where $q = p$ or $p^2$.

**Problem 3.** Design and implement an algorithm which computes the automorphism groups PAut $(C)$, MAut $(C)$, $\Gamma$Aut $(C)$ of a given code $C$ (including quantum codes) over any field $F_q$.

The existing algorithms in Magma and GAP/GUAVA (both are based on the algorithm of Leon) are slow. It is unclear whether this is because of poor implementations or due to the limitations of the algorithm. Furthermore, it seems that extending such algorithms and implementations to larger size fields should be the next step. We intend to pursue such questions in further work.

## References


1. Antoniadis J., Kontogeorgis A. On cyclic covers of the projective line. Manuscripta Math., 2006, **121**, No. 1, 105–130.
2. Ashikhmin A., Knill E., Nonbinary quantum stabilizer codes, IEEE Transactions on Information Theory, 2001, **47**, No. 7, 3065–3072.
3. Demirbas Y., Automorphism groups of hyperelliptic curves of genus 3 in characteristic 2, Computational aspects of algebraic curves, T. Shaska (Edt), Lect. Notes in Comp., World Scientific, 2005.
4. Huffman W.C., Pless V., Fundamentals of error-correcting codes. Cambridge University Press, Cambridge, 2003.
5. Leon J.S. Computing automorphism groups of error-correcting codes. IEEE Trans. Inform. Theory, 1982, **28**, No. 3, 496–511.
6. Gutierrez J., Shaska T. Hyperelliptic curves with extra involutions, LMS J. of Comput. Math., 20005, **8**, 102–115.
7. The Magma Computational Algebra System for Algebra, Number Theory and Geometry, v2.11-5, Sydney, 2004.
8. Matsumoto R., Improvement of the Ashikhmin-Litsyn-Tsfasman Bound for Quantum Codes, IEEE Transactions on Information Theory, 2002, **48**, No. 7, 2122–2124.
9. Nebe G., Rains E.M., Sloane N.J.A. Self-Dual Codes and Invariant Theory. Springer, 2006.
10. Stichtenoth H. Self-dual Goppa Codes, Journal of Pure and Applied Algebra, 1988, **55**, 199-211.
11. Stichtenoth H. Algebraic Function Fields and Codes. Springer-Verlag, Berlin, 1993.
12. Shaska T. Some open problems in computational algebraic geometry, Alb. Jour. Math., 2007, **1**, No. 3, (to appear).
13. Shaska T. Determining the automorphism group of hyperelliptic curves, Proc. of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM Press, p. 248–254, 2003.
14. Shaska T., Shor C. Codes over $F_{p^2}$ and $F_p \times F_p$, lattices, and theta functions, Advances in Coding Theory and Cryptology, 2007, **2**, 70–80.
15. Shaska T., Wang Q. On the automorphism groups of some AG-codes based on $C_{ab}$ curves, Serdica Journal of Computing, (to appear).
16. Shaska T., Wijesiri S. Codes over rings of size four, Hermitian lattices, and corresponding theta functions, Proc. Amer. Math. Soc., to appear.
17. Xing C. Hyperelliptic function fields and codes, Journal of Pure and Applied Algebra, 1991, **74**, 109–118.
18. Wesemeyer S. On the automorphism group of various Goppa codes, IEEE Trans. Inform. Theory, 1998, **44**, 630–643.

# Квантові коди за алгебраїчними кривими з автоморфізмами

Т.Шаска

[1] Факультет математики та статистики, Університет Окленду, Рочестер, США

[2] Університет Марії Кюрі-Склодовської, Люблін, Польща

Отримано 31 січня 2008 р.

Нехай $\chi$ – алгебраїчна крива типу $g \geqslant 2$, що визначена над полем $F_q$ характеристики $p$. При деяких умовах на $\chi$ ми можемо будувати алгебраїчно-геометричний код $C$. Якщо код $C$ є само-ортогональним відповідно до симплектичного добутку, то будується квантовий код $Q$, який будемо називати QAC кодом. В статті вивчаються конструкції таких кодів за кривими з автоморфізнами і зв'язки між групами автоморфізмів кривої $\chi$ та кодів $C$ та $Q$.

**Ключові слова:** *алгебраїчні криві, алгебраїчно-геометричні коди, квантові алгебраїчні коди*

**PACS:** *03.67.Dd*