QUANTUM CODES FROM SUPERELLIPTIC CURVES

A. Elezi

Department of Mathematics and Statistics,
American University,
Email: aelezi@american.edu

T. Shaska

367 Science and Engineering Building,
Department of Mathematics and Statistics,
Oakland University,
Email: shaska@oakland.edu

Abstract. Let $\mathcal{X}$ be an algebraic curve of genus $g \geq 2$ 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.

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.

Let $\mathcal{X}$ denote 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 $C_{\mathcal{X}}$ (or its dual) is self-orthogonal under an appropriate symplectic form, then from $C_{\mathcal{X}}$ we can construct a quantum code $Q_{\mathcal{X}}$, which will be called a QAG-code; see [2, 32] among other sources. 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 interesting. Very little is known how the automorphism group of the quantum code $Q_{\mathcal{X}}$ relates to the automorphism group of $\mathcal{X}$ and $C_{\mathcal{X}}$.

In this paper we explain

(a) how to construct quantum codes from algebraic geometry codes (quantum algebraic geometry codes), and

(b) the relations between the automorphism group of the algebraic curve, the automorphism group of the AG-code, and the automorphism group of the corresponding quantum code.

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 interesting 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. For more details on automorphism groups of curves, their Weierstrass points and other aspects of superelliptic curves see [4–48].

Notation: Throughout this 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 of the same parameters. A cyclic group of order n is denoted by C_n. In general, given a genus $g \geq 2$ algebraic curve $\mathcal{X}$ defined over $\mathbb{F}$, the automorphism group of $\mathcal{X}$ is denoted by 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 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 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 $\forall \mathrm{x} \in \mathrm{C}$ we have $M_\gamma(\mathrm{x}) = \gamma(\mathrm{Mx})$. The set of all maps M_γ forms the automorphism group of C, denoted by ΓAut (C).

2. Linear Codes, Algebraic Geometry Codes and Quantum Stabilizer Codes

2.1. **Linear Codes.**
A linear code C of length n and dimension k over a finite field $\mathbb{F}_q$ is a k-dimensional subspace of $V = \mathbb{F}_q^n$. A k-bit codeword of C is encoded into an n-bit word of V to protect the information and recover errors during transmission. The Hamming distance d of the linear code C is the minimum of the weights of the vectors in C. Here the weight of a vector is the number of nonzero coordinates. Such a linear code is denoted by $[n, k, d]$. It detects up to $d - 1$ errors and corrects up to $\frac{d-1}{2}$ errors.

2.2. **Algebraic geometry codes.**
Let $\mathcal{X}$ be a genus g algebraic curve defined over a finite field $\mathbb{F}_q$ with characteristic $p > 0$ and $\mathbb{F} = \mathbb{F}_q(\mathcal{X})$ its function field. Let $P_1, \ldots, P_n$ be places of degree one, $D = P_1 + \cdots + P_n$ and G a divisor with $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$. The following two algebraic geometry codes have been introduced by Goppa:

Type A) $C_{\mathcal{L}}(D, G) := \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n$. To compute its parameters consider the following **evaluation map**

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

Since $P_1, \ldots, P_n$ are places of degree one and $\text{supp}(G) \cap \text{supp}(D) = \emptyset$, φ is a well-defined map with kernel is $\mathcal{L}(G - D)$. Clearly

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

a linear $[n, k, d]$ code with parameters

$$k = \dim G - \dim(G - D), \quad d \geq n - \deg G.$$

One can easily see that

(1) If we assume $\deg G < n = \deg D$ then $\deg(G - D) < 0$ hence $\dim(G - D) = 0$. It follows that $\varphi : \mathcal{L}(G) \to C_{\mathcal{L}}(D, G)$ is injective and $C_{\mathcal{L}}(D, G)$ is an $[n, k, d]$ code with

$$k = \dim G \geq \deg G + 1 - g \quad \text{and} \quad d \geq n - \deg G.$$

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

(4) Let $\text{Aut}_{D,G}(\mathcal{X}) := \{\sigma \in \text{Aut}(\mathcal{X}) | \sigma(D) = D \text{ and } \sigma(G) = G\}$. This group acts on $C_{\mathcal{L}}(D, G)$ via

$$\sigma(f(P_1) \ldots f(P_n)) = (f(\sigma(P_1)) \ldots f(\sigma(P_n))).$$

If $n > 2g + 2$, then this action is faithful.

Type B) The second algebraic geometry code $C_\Omega(D, G)$ is defined by

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

The following result is well known:

Lemma 1. *If D and G are as above then:*

(1) $C_{\mathcal{L}}(D, G)^\perp = C_\Omega(D, G)$ *under the standard pairing in $\mathbb{F}_q^n$.*
(2) *Let η be any differential with $v_{P_i}(\eta) = -1$ for $i = 1, \ldots, n$. (Notice that by the approximation theorem such differentials exist.) Let $H = D - G + (\eta)$. Then $C_\Omega(D, G) = a \cdot C_{\mathcal{L}}(D, H)$ where $a = (\text{res}_{P_1}(\eta), \ldots, \text{res}_{P_n}(\eta))$.*
(3) $C_{\mathcal{L}}(D, G)^\perp = a \cdot C_{\mathcal{L}}(D, H)$.

2.3. One point codes and their automorphism groups. Let D be a divisor as above, $P \notin \text{sup}(D)$, and m an integer. The **one point codes of level** m are defined to be algebraic geometry codes of the form

$$C_{\mathcal{L}}(D, mP)$$

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

Lemma 2. *Let $\mathcal{X}/F_q$ be an admissible curve over F_q of genus g where $l > k$. Assume that $m \geq l$. 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 [51] for details   □

2.4. Quantum codes, stabilizer codes and connection with classical codes.

Let $q = p^m$ be a prime power and V_q a q-dimensional complex vector space. **A q-ary quantum code of length n and dimension k** is a k-dimensional subspace Q of $V := V_q^{\otimes n}$. V_q is the quantum counterpart of $\mathbb{F}_q$. Its elements are called **quantum states**. A codeword of k quantum states in Q is encoded into a word of n quantum states in V for protection and error correction.

A *general quantum error* of a q-ary quantum system is a linear transformation of the space V_q. Let $e_1, e_2, \ldots, e_{q^2}$ be a basis for the space of quantum errors of such a system, where e_1 is the identity linear transformation. *A quantum error of an n q-ary system* is a linear transformation of V. A basis for the space of general quantum errors is formed by $E := \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n$ with $\sigma_i \in \{e_1, e_2, \ldots, e_{q^2}\}$. Define the *weight* of such E as

$$wt(W) = |\{\sigma_i \neq e_1\}|.$$

Recall that if a code can correct a set of errors then it can correct their linear span.

For a quantum code Q, we let P be the projection $P : V \to Q$. It can be shown that a quantum error E is *detectable* iff

$$PEP = c_E P$$

for some scalar c_E. *The minimum distance* of a quantum code Q is the largest integer d such that every error of weight $d - 1$ can be detected by Q.

Stabilizer codes are a general class of quantum codes that can be constructed from classical codes. We review briefly this construction here, see [1] for more details.

First, we construct a special error basis. Let T, R be $p \times p$ matrices defined by $T_{i,j} = \delta_{i,j-1 \ (mod \ p)}$ and $R_{ij} = \omega^i \delta_{i,j}$ where ω is a p-th root of unity. For $a \in F_q$, let $(a_1, \ldots, a_m)$ be the coordinates of a in some fixed basis of F_q as an F_p-vector space. Define

$$T_a := T^{a_1} \otimes \cdots \otimes T^{a_m}, \ R_a := R^{a_1} \otimes \cdots \otimes R^{a_m}.$$

Finally, for $a = (a^1, a^2, \ldots, a^n) \in F_q^n$ and $b = (b^1, b^2, \ldots, b^n) \in F_q^n$, let

$$E_{a,b} := T_{a^1} R_{b^1} \otimes \cdots \otimes T_{a^n} R_{b^n}.$$

It is shown in [1] that $E_{a,b}$ form a basis for quantum errors of an n q-ary system.

Let S be an abelian subgroup of $\Omega = \{\omega^i E_{a,b}, i = 0, 1, \ldots, p-1; a, b \in F_q^n\}$ and μ an S linear character that satisfies $\mu(\omega I) = \omega$. The eigenspace $Q_{S,\mu}$ of S associated with μ, i.e.

$$Q_{S,\mu} := \{v \in V \ : \ E(v) = \mu(E)v, \forall E \in S\},$$

is called *a quantum stabilizer code*. If the order of S is p^{r+1}, then the dimension of $Q_{S,\mu}$ is p^{mn-r}.

Quantum stabilizer codes constructed above are related to classical codes in F_q^{2n}. First some preliminaries. Let tr: $F_q \to F_p$ the trace map. Elements of F_q^{2n} will be denoted by $v = (a, b)$ where $a = (a_1, a_2, \ldots, a_n), b = (b_a, b_2, \ldots, b_n) \in F_q^n$. The (symplectic) weight of such an element is

$$wt(v) = |\{i \; : \; (a_i, b_i) \neq (0, 0)\}|.$$

For $x = (x_1, \ldots, x_n); y = (y_1, \ldots, y_n)$ we let

$$\langle x, y \rangle := x_1 y_1 + \cdots + x_n y_n$$

be the standard pairing in F_q^n. Define two symplectic products on F_q^{2n} as follows:

$$\langle (a, b), (a', b') \rangle_s := \langle a, b' \rangle - \langle a', b \rangle$$

and

$$tr_s((a, b), (a', b')) := tr(\langle a, b' \rangle - \langle a', b \rangle).$$

The quantum stabilizer code $Q_{S,\mu}$ yields a classical code $C := \{(a, b) \; : \; E_{a,b} \in S\} \subset F_q^{2n}$. It is an F_p-linear code of length $2n$ and size p^r. The commutativity of S implies that the code C is self-orthogonal relative to the symplectic product tr_s, i.e. $C \subset C^{\perp_s}$ where $C^{\perp_s}$ be the dual of the code C. The minimum distance of the quantum stabilizer code $Q_{S,\mu}$ is related to the classical minimum distance of $C^{\perp_s} \backslash C$. In fact, if $S^{\perp_s}$ denotes the centralizer of S, it is shown in [1] that an error E is detectable by $Q_{S,\mu}$ iff $E \in S^{\perp_s} \backslash S$. It follows that the minimum distance of $Q_{S,\mu}$ is the $\min\{wt(v) \; v \in C^{\perp_s} \backslash C\}$. It is clear that this process is reversible, i.e. a tr_s self-orthogonal code C in F_q^{2n} with p^r codewords determines a quantum stabilizer code Q of dimension p^{mn-r}.

Remark: We note that if C is an F_q-linear code then the duals of C relative to the two symplectic forms are the same (this not true, however, for general F_p-linear codes.) From now on, we will be interested only in F_q-linear codes and the symplectic form $\langle (a, b), (a', b') \rangle_s$. The dual of a linear code C relative to this symplectic form will be denoted by $C^{\perp_s}$.

The following proposition will be used in constructing AG-quantum stabilizers codes from AG-classical self-orthogonal codes.

Proposition 1. *Let $C \subset F_q^{2n}$ be a $(n + k)$-dimensional F_q-subspace such that such that $C^{\perp_s} \subset C$ (i.e. $C^{\perp_s}$ is self orthogonal). Then, there exist a quantum code $Q \subset V$ of dimension q^k and minimum distance $d = \min \{wt(x) \mid x \in C \backslash C^{\perp_s}\}$.*

Proof. The F_q-code $C^{\perp_s}$ is self-orthogonal and has dimension $n - k$, so it has p^r codewords with $r = m(n - k)$. From the above construction we get a quantum stabilizer code of dimension $p^{mn-r} = p^{mn-m(n-k)} = p^{mk} = q^k$.

$\square$

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

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 [50, Prop. VII.1.2]. It allows for the construction of 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 $\eta := x \cdot \frac{dy}{y}$ satisfies $v_{P_i}(\eta) = -1$ and $\mathrm{res}_{P_i}(\eta) = 1$ for $i = 1, \ldots, n$.*

A quantum stabilizer code can be obtained from an algebraic geometric construction related to curves with an involution.

Theorem 1. *Let $\mathcal{X}$ be a genus g irreducible algebraic curve defined over $\mathbb{F}_q$ and $P_1, \ldots, P_n$ degree one rational points on $\mathcal{X}$. Let $\sigma \in Aut_{\mathbb{F}}(\mathcal{X})$ be an involution such that $\sigma P_i \neq P_j$, $\forall i, j = 1, \ldots, n$. 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*

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

Proof. Let Let $D = P_1 + \cdots + P_n + \sigma P_1 + \cdots + \sigma P_n$. By the strong approximation theorem, there is a differential η such that

$$ (2) \qquad \begin{cases} v_{P_i}(\eta) = v_{\sigma P_i}(\eta) = -1, \\ \mathrm{res}_{P_i}(\eta) = 1, \\ \mathrm{res}_{\sigma P_i}(\eta) = 1. \end{cases} $$

It follows that $H := D - G + (\eta) \leq G$. Consider the algebraic geometry code

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

One can easily see that

$$ (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n}) \in C_{\mathcal{L}}(D, G) \Leftrightarrow (x_{n+1}, \ldots, x_{2n}, x_1, \ldots, x_n) \in C_{\mathcal{L}}(D, G), $$

which implies that $C_{\mathcal{L}}(D, G)^{\perp_s} = C_{\mathcal{L}}(D, H)$.

Notice that $\mathcal{L}(H) \subset \mathcal{L}(G)$ since $H \leq G$. It follows that $C(D, G)^{\perp_s} = C(D, H) \subset C(D, G)$. Now apply the last proposition with $k = \dim C(D, G) - n$.

To show the inequality of the distance, let $f \in \mathcal{L}(G)$ such that

$$ \mathrm{wt} \ (f(P_1), \ldots, f(\sigma(P_n)) = \delta \neq 0. $$

Hence, there exists a set of $n - \delta$ pairs $(f(P_{i_j}), f(\sigma P_{i_j})), j = 1, 2, \ldots, n - \delta$ which are all zero. Thus, we have $f \in \mathcal{L}\left(G - \sum_{j=1}^{n-\delta}(P_{i_j} + \sigma P_{i_j})\right)$. Hence

$$ \dim \mathcal{L}\left(G - \sum_{j=1}^{n-\delta}(P_{i_j} + \sigma P_{i_j})\right) > 0, $$

which implies the result.

$\square$

From this theorem we see that curves with an involution and many rational points are useful in generating quantum codes. These are also the typical curves used in constructing AG-codes. Clearly hyperelliptic curves have an involution but there are others. It is however unknown how the choice of the involution affects the parameters of the code - this remains an open question.

Curves which have a cyclic group embedded in their automorphism group may also be used to produce quantum stabilizer codes. We deal with them in the next section.

3.1. **Quantum codes from superelliptic curves.** A genus $g \geq 2$ superelliptic curve of level n is given by an equation of the form $y^n = f(x)$ for some degree $d > 4$ polynomial $f(x)$ and $n \geq 2$. Let us assume that

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

Then, $\sum_{i=1}^{s} d_i = d$. We call this the **standard form** of the superelliptic curve. Superelliptic curves of level n are studied in detail in [16]. They are interesting from the point of view of this article because they have extra automorphisms and we can determine their automorphism groups and their equations; see [24, 25]

Let k be an algebraic closed field of characteristic $p \geq 0$. Let $F_0 = k(x)$ be the function field of the projective line $\mathbb{P}^1(k)$ and $F := k(x, y)$. If $d := \sum_{i=1}^{s} d_i \equiv 0$ mod n then the place at infinity does not ramify at the above extension. The only places at F_0 that are ramified are the places P_i that correspond to the points $x = \alpha_i$ and the corresponding ramification indices are given by

$$e_i = \frac{n}{(n, d_i)}.$$

Moreover if $(n, d_i) = 1$ then the places P_i are ramified completely and the Riemann-Hurwitz formula implies that the function field F has genus

$$g = \frac{(n-1)(s-2)}{2}.$$

Notice that the condition $g \geq 2$ is equivalent to $s \geq 2\frac{n+1}{n-1}$. In particular, $s > 2$.

For the proof of the following Lemmas see [16].

Lemma 4. *Let $G = Aut(F)$. Suppose that a cyclic extension F/F_0 of the rational function field F_0 is ramified completely at s places and $n := |Gal(F/F_0)|$. If $2n < s$ then $Gal(F/F_0) \lhd G$.*

Lemma 5. *Suppose that τ is an extra automorphism of F, and let s be the number of ramified places at the extension F/F_0 and let d be the degree of the defining polynomial. Then $\delta|s, \delta|d$ and the defining equation of F can be written as*

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

where $a_0 = 1$.

We will say that the superelliptic curve is in **normal form** if and only if it is given by an equation:

$$y^n = x^s + \sum_{i=1}^{\frac{d}{\delta}} a_i x^{\delta \cdot i} + 1.$$

Parametrizing superelliptic curves that admit an extra automorphism of order δ, is the set of coefficients $\{a_{s/\delta-1}, \cdots, a_1\}$ of a normal form up to a change of coordinate in x. The condition $\tau(x) = \zeta x$, implies that $\bar{\tau}$ fixes the places $0, \infty$. Moreover we can change the defining equation by a morphism $\gamma \in PGL(2,k)$ of the form $\gamma : x \to mx$ or $\gamma : x \to \frac{m}{x}$ so that the new equation is again in normal form. Substituting $a_0 = (-1)^{d/s} \prod_{i=1}^{d/s} \beta_i^s$ we have

$$(-1)^{s/\delta} \prod_{i=1}^{s/\delta} \gamma(\beta_i)^{\delta} = 1$$

and this gives $m^s = (-1)^{s/\delta}$. Then, x is determined up to a coordinate change by the subgroup $D_{s/\delta}$ generated by

$$\tau_1 : x \to \epsilon x, \ \tau_2 : x \to \frac{1}{x}$$

where ϵ is a primitive s/δ-root of one, see [16] for details.

The action of $D_{s/\delta}$ on the parameter space $k(a_1, \ldots, a_{s/\delta})$ is given by

$$\tau_1 : a_i \to \epsilon^{\delta i} a_i, \ for \ i = 1, \ldots s/\delta$$
$$\tau_2 : a_i \to a_{d/\delta-i}, \ for \ i = 1, \ldots [s/\delta]$$

Notice that if $s/\delta = 1$ then the above actions are trivial, therefore the normal form determines the equivalence class. If $s/\delta = 2$ then

$$\tau_1(a_1) = -a_1, \tau_1(a_2) = a_2, \tau_2 = 1$$

and the action is not dihedral but cyclic on the first vector.

Lemma 6. *Let $r := s/\delta > 2$ The elements*

$$\mathfrak{s}_i := a_1^{r-i} a_1 + a_{r-1}^{r-i} a_{r-i}, \ for \ i = 1, \ldots, r$$

are invariants under the action of the group $D_{s/\delta}$ defined as above.

See [16] for details. The elements $\mathfrak{s}_i$ are called the **dihedral invariants** or $\mathfrak{s}$-**invariants** of $D_{s/\delta}$. Two superelliptic curves are isomorphic if and only if they have the same $\mathfrak{s}$-invariants.

Let $\mathcal{X}$ be a genus g superelliptic curve of level $r > 2$ and σ the automorphism of order r of $\mathcal{X}$. The corresponding projection $\psi_\sigma : \mathcal{X} \to \mathbb{P}^1$ has d branch points. Let $\mathcal{B}$ be the branch set. For a given rational point $P \in \mathcal{X}$ we define $\mathcal{O}rb_\sigma(P) = \{\sigma(P) \in X\}$. If $\psi(P) \notin \mathcal{B}$ then $|\mathcal{O}rb_\sigma(P)| = r$.

Let $P_1, \ldots, P_n$ rational points on $\mathcal{X}$ such that $\psi(P_i) \notin \mathcal{B}$ for all $i = 1, \ldots, n$ and let

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

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 in the fiber is denoted by P_∞. It is common in coding theory to take G to be mP_∞.

Again we work with $C_\mathcal{X} = C_\mathcal{L}(G, D)$. The proof of the following theorem should go through like in Thm. 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 $P_1, \ldots, P_n$ 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*

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

As in the case of curves with involutions, it is unclear how the cyclic group or the automorphism group of the curve affects the parameters of the quantum code. This remains an open question.

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 $\{P_1, \ldots, P_n\}$. Let $C = C_\mathcal{L}(D, G)$, where $n + 1$ is the number of rational points of $\mathcal{X}$ and

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

The permutation automorphism group PAut (C) is as follows:
  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 $(C) \cong Aut_{D, mP_\infty}(\mathcal{X})$.

For a proof of the above statements see [32].

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 α is a primitive element of F_4. The permutation automorphism group is isomorphic to the group with GAP identity $[24, 12]$. In this case

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

This code is clearly an MDS code. The automorphism group $\Gamma Aut\,(C)$ has Gap identity $(1944, 3876)$. 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 has order 31104 and is a degree 2 extension of $\Gamma Aut\,(C)$.
□

In the next section we 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 $\mathcal{X}_g$ a genus g hyperelliptic curve given by the equation $y^2 = f(x)$, $F := K(x, y)$

its function field and σ 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

$$\{P_1, \ldots, P_n, \sigma(P_1), \ldots, \sigma(P_n)\},$$

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

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

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

where $0 \leq r \leq n - g$. 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

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

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

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

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

Now we can construct algebraic geometry codes $C_{\mathcal{L}}(D, G)$ and $C_{\mathcal{L}}(D, H)$. The weighted symplectic inner product is defined as below

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

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

Lemma 7. *Let $C_{\mathcal{L}}(D, G)$ and $C_{\mathcal{L}}(D, H)$ be as above. Then*

$$C_{\mathcal{L}}(D, G)^{\perp_s} = C_{\mathcal{L}}(D, H) \cdot \text{diag}(a_1, \ldots, a_n, 1, \ldots, 1)$$

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

We transform $C_{\mathcal{L}}(D, G)$ to a code $C'_{\mathcal{L}}(D, G)$ which has the same parameters as $C_{\mathcal{L}}(G, D)$ and is self-orthogonal with respect to the standard symplectic inner product by multiplying each component x_i of every codeword by the corresponding a_i, for $1 \leq i \leq n$.

Then, we have the following:

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

4.1. **Explicit construction of quantum AG-codes.** Here is 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 hyper-elliptic involution, say $S = \{P_1, \ldots, P_n, \sigma(P_1), \ldots, \sigma(P_n)\}$.*

ii) *Let*

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

iii) *Create a list $A = [a_1, \ldots, a_n]$, 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, to be $\mathcal{G}$.*

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

$$(\ldots, x_i, \ldots) \to (\ldots, a_i x_i, \ldots)$$

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

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

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 $p > 2g + 1$. Hence, for large enough p (i.e., $p > 2g + 1$) methods described in [24] 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 $p \leq 2g + 1$.

5.1.1. *Automorphism groups of superelliptic curves.* The automorphism groups of superelliptic curves for every characteristic $p \neq 2$ were determined in [25]. For genus 3 and 4 the following theorem are simply an application of Sanjeewa's results.

Lemma 8. *Let $\mathcal{X}_g$ be a genus 3 superelliptic curve defined over a field of characteristic p. Then the automorphism groups of $\mathcal{X}_g$ are as follows.*

i): $p = 0$: $(2, 1), (4, 2), (3, 1), (4, 1), (8, 2), (8, 3), (7, 1), (21, 1), (14, 2), (6, 2),$ $(12, 2), (9, 1), (8, 1), (8, 5), (16, 11), (16, 10), (32, 9), (30, 2), (42, 3), (12, 4),$ $(16, 7), (24, 5), (18, 3), (16, 8), (48, 33), (48, 48).$

ii): $p = 3$: $(2, 1), (4, 2), (3, 1), (4, 1), (8, 2), (8, 3), (7, 1), (14, 2), (6, 2), (8, 1),$ $(8, 5), (16, 11), (16, 10), (32, 9), (30, 2), (16, 7), (16, 8), (6, 2).$

iii): $p = 5$: $(2, 1), (4, 2), (3, 1), (4, 1), (8, 2), (8, 3), (7, 1), (21, 1), (14, 2),$ $(6, 2), (12, 2), (9, 1), (8, 1), (8, 5), (16, 11), (16, 10), (32, 9), (42, 3), (12, 4),$ $(16, 7), (24, 5), (18, 3), (16, 8), (48, 33), (48, 48).$

iv): $p = 7$: $(2, 1), (4, 2), (3, 1), (4, 1), (8, 2), (8, 3), (7, 1), (21, 1), (6, 2), (12, 2),$ $(9, 1), (8, 1), (8, 5), (16, 11), (16, 10), (32, 9), (30, 2), (42, 3), (12, 4), (16, 7),$ $(24, 5), (18, 3), (16, 8), (48, 33), (48, 48).$

v): $p > 7$: $(2, 1), (4, 2), (3, 1), (4, 1), (8, 2), (8, 3), (7, 1), (21, 1), (14, 2), (6, 2),$ $(12, 2), (9, 1), (8, 1), (8, 5), (16, 11), (16, 10), (32, 9), (30, 2), (42, 3), (12, 4),$ $(16, 7), (24, 5), (18, 3), (16, 8), (48, 33), (48, 48).$

We obtain the following groups as automorphism groups of a genus 4 cyclic curve defined over algebraically closed field of characteristic 0,3,5,7 and bigger than 7. We listed GAP group ID of those groups in following theorem.

Lemma 9. *Let $\mathcal{X}_g$ be a genus 4 superelliptic curve defined over a field of characteristic p. Then the automorphism groups of $\mathcal{X}_g$ are as follows.*

i): $p = 0$: $(2, 1), (4, 2), (3, 1), (6, 2), (9, 2), (5, 1), (10, 2), (20, 1), (9, 1), (27, 4),$ $(18, 2), (15, 1), (4, 1), (20, 4), (18, 3), (8, 3), (40, 8), (12, 5), (36, 12), (54, 4),$ $(16, 7), (20, 5), (32, 19), (24, 10), (8, 4), (60, 9), (36, 11), (24, 3), (72, 42).$

ii): $p = 3$: $(2, 1), (4, 2), (3, 1), (6, 2), (5, 1), (10, 2), (20, 1), (9, 1), (18, 2),$ $(15, 1), (4, 1), (20, 4), (8, 3), (40, 8), (12, 5), (16, 7), (20, 5), (32, 19), (24, 10),$ $(8, 4), (9, 2), (18, 5).$

iii): $p = 5$: $(2, 1), (4, 2), (3, 1), (6, 2), (9, 2), (5, 1), (10, 2), (20, 1), (9, 1),$ $(27, 4), (18, 2), (4, 1), (18, 3), (8, 3), (12, 5), (36, 12), (54, 4), (16, 7), (20, 5),$ $(32, 19), (24, 10), (8, 4), (60, 9), (36, 11), (24, 3), (72, 42), (10, 2), (18, 5).$

iv): $p = 7$: $(2, 1), (4, 2), (3, 1), (6, 2), (9, 2), (5, 1), (10, 2), (20, 1), (9, 1),$ $(27, 4), (18, 2), (15, 1), (4, 1), (20, 4), (18, 3), (8, 3), (40, 8), (12, 5), (36, 12),$ $(54, 4), (16, 7), (20, 5), (32, 19), (24, 10), (8, 4), (60, 9), (36, 11), (24, 3),$ $(72, 42).$

v): $p > 7$: $(2, 1), (4, 2), (3, 1), (6, 2), (9, 2), (5, 1), (10, 2), (20, 1), (9, 1),$ $(27, 4), (18, 2), (15, 1), (4, 1), (20, 4), (18, 3), (8, 3), (40, 8), (12, 5), (36, 12),$ $(54, 4), (16, 7), (20, 5), (32, 19), (24, 10), (8, 4), (60, 9), (36, 11), (24, 3),$ $(72, 42).$

Remark 1. Note that these lists contain all groups and not just the full automorphism groups.

5.1.2. *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

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

where the n_a are odd ([49], 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 σ 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:

(3)
$$(1, 1, 1, 1), (3, 1, 1), (3, 3), (5, 1), (7) \quad for\ genus\ 3$$
$$(1, 1, 1, 1, 1), (3, 1, 1, 1), (3, 3, 1), (5, 1, 1), (5, 3), (7, 1), (9) \quad for\ genus\ 4$$

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

(4)
$$y^2 + y = \begin{cases} \alpha_1 x + \alpha_2 x^{-1} + \alpha_3(x - 1)^{-1} + \alpha_4(x - \lambda)^{-1} \\ x^3 + \alpha x + \beta x^{-1} + \gamma(x - 1)^{-1} \\ x^3 + \alpha x + \beta x^{-3} + \gamma x^{-1} \\ x^5 + \alpha x^3 + \beta x^{-1} \\ x^7 + \alpha x^5 + \beta x^3 \end{cases}$$

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

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 3. *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.

$\square$

Furthermore, the parametric equation of the curve in each case is given by equation in Table 1. Determining complete lists of full automorphism groups for a given genus $g > 3$ is still an open problem with many applications in theoretical mathematics, computer science, and electrical engineering.

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 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 $\forall \mathrm{x} \in \mathrm{C}$ we have $M_\gamma(\mathrm{x}) = \gamma(M\mathrm{x})$. The set of all maps M_γ forms the **automorphism group** of C, denoted by ΓAut (C). It is well known that

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

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 σ 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 [?HP, Thm. 7.9.4].

If $\mathcal{X}$ is a genus $g \geq 2$ algebraic curve defined over $\mathbb{F}_q$ then Aut $(\mathcal{X})$ the group of automorphisms of $\mathcal{X}$ over the algebraic closure of $\mathbb{F}_q$. There have been 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 [32] 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.

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}

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

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

In this section we want to make a few remarks on 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 on 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 $\mathbb{F}_q$. 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. Similar capabilities are available also 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), ΓAut (C) of a given code C (including quantum codes) over any field $\mathbb{F}_q$.

REFERENCES

[1] Alexei Ashikhmin and Emanuel Knill, *Nonbinary quantum stabilizer codes*, IEEE Trans. Inform. Theory **47** (2001), no. 7, 3065–3072.

[2] Annika Niehage, *Quantum Goppa Codes over Hyperelliptic Curves*, arXiv:quant-ph/0501074.

[3] Yasin Demirbas, *Hyperelliptic curves of genus 3 and 4 in characteristic 2*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 145–162.

[4] T. Shaska and F. Thompson, *Bielliptic curves of genus 3 in the hyperelliptic moduli*, Appl. Algebra Engrg. Comm. Comput. **(to appear)**. arXiv:1305.4501 [math.AG]

[5] T. Shaska, *Some remarks on the hyperelliptic moduli of genus 3*, Comm. Algebra **(to appear)**. arXiv:1209.1237 [math.AG]

[6] Tanush Shaska and Engjell Hasimaj (eds.), *Algebraic aspects of digital communications*, NATO Science for Peace and Security Series D: Information and Communication Security, vol. 24, IOS Press, Amsterdam, 2009. Papers from the Conference "New Challenges in Digital Communications" held at the University of Vlora, Vlora, April 27–May 9, 2008.

[7] T. Shaska, W. C. Huffman, D. Joyner, and V. Ustimenko (eds.), *Advances in coding theory and cryptography*, Series on Coding Theory and Cryptology, vol. 3, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2007. Papers from the Conference on Coding Theory and Cryptography held in Vlora, May 26–27, 2007 and from the Conference on Applications of Computer Algebra held at Oakland University, Rochester, MI, July 19–22, 2007.

[8] T. Shaska and C. Shor, *Weierstrass points of genus 3 hyperelliptic curves with extra automorphisms*.

[9] _____ , *q-Weierstrass points of hyperelliptic curves*.

[10] _____ , *Weierstrass points of superelliptic curves and their dihedral invariants*.

[11] Tanush Shaska (ed.), *Computational aspects of algebraic curves*, Lecture Notes Series on Computing, vol. 13, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005. Papers from the conference held at the University of Idaho, Moscow, ID, May 26–28, 2005.

[12] Helmut Voelklein and Tanush Shaska (eds.), *Progress in Galois theory*, Developments in Mathematics, vol. 12, Springer, New York, 2005.

[13] T. Shaska, *Computational algebraic geometry*, J. Symbolic Comput. **57** (2013), 1–2.

[14] T. Shaska and L. Beshaj, *The arithmetic of genus two curves*, Information security, coding theory and related combinatorics, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 29, IOS, Amsterdam, 2011, pp. 59–98.

[15] A. Elezi and T. Shaska, *Quantum codes from superelliptic curves*, Albanian J. Math. **5** (2011), no. 4, 175–191.

[16] Lubjana Beshaj, Valmira Hoxha, and Tony Shaska, *On superelliptic curves of level n and their quotients, I*, Albanian J. Math. **5** (2011), no. 3, 115–137.

[17] T. Shaska, C. Shor, and S. Wijesiri, *Codes over rings of size p^2 and lattices over imaginary quadratic fields*, Finite Fields Appl. **16** (2010), no. 2, 75–87.

[18] T. Shaska and G. S. Wijesiri, *Theta functions and algebraic curves with automorphisms*, Algebraic aspects of digital communications, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 24, IOS, Amsterdam, 2009, pp. 193–237.

[19] Kay Magaard, Tanush Shaska, and Helmut Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Forum Math. **21** (2009), no. 3, 547–566.

[20] T. Shaska and V. Ustimenko, *On the homogeneous algebraic graphs of large girth and their applications*, Linear Algebra Appl. **430** (2009), no. 7, 1826–1837.

[21] Tanush Shaska and V. Ustimenko, *On some applications of graphs to cryptography and turbocoding*, Albanian J. Math. **2** (2008), no. 3, 249–255.

[22] T. Shaska and M. Qarri, *Algebraic aspects of digital communications*, Albanian J. Math. **2** (2008), no. 3, 141–144.

[23] N. Pjero, M. Ramasaço, and T. Shaska, *Degree even coverings of elliptic curves by genus 2 curves*, Albanian J. Math. **2** (2008), no. 3, 241–248.

[24] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213.

[25] ———, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213.

[26] T. Shaska, G. S. Wijesiri, S. Wolf, and L. Woodland, *Degree 4 coverings of elliptic curves by genus 2 curves*, Albanian J. Math. **2** (2008), no. 4, 307–318.

[27] T. Shaska and G. S. Wijesiri, *Codes over rings of size four, Hermitian lattices, and corresponding theta functions*, Proc. Amer. Math. Soc. **136** (2008), no. 3, 849–857.

[28] T. Shaska and C. Shor, *Codes over $\mathbf{F}_{p^2}$ and $\mathbf{F}_p \times \mathbf{F}_p$, lattices, and theta functions*, Advances in coding theory and cryptography, Ser. Coding Theory Cryptol., vol. 3, World Sci. Publ., Hackensack, NJ, 2007, pp. 70–80.

[29] Tanush Shaska, *Some open problems in computational algebraic geometry*, Albanian J. Math. **1** (2007), no. 4, 297–319.

[30] E. Previato, T. Shaska, and G. S. Wijesiri, *Thetanulls of cyclic curves of small genus*, Albanian J. Math. **1** (2007), no. 4, 253–270.

[31] A. Elezi and T. Shaska, *Special issue on algebra and computational algebraic geometry*, Albanian J. Math. **1** (2007), no. 4, 175–177.

[32] Tanush Shaska and Quanlong Wang, *On the automorphism groups of some AG-codes based on $C_{a,b}$ curves*, Serdica J. Comput. **1** (2007), no. 2, 193–206.

[33] David Sevilla and Tanush Shaska, *Hyperelliptic curves with reduced automorphism group A_5*, Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 1-2, 3–20.

[34] T. Shaska, *Subvarieties of the hyperelliptic moduli determined by group actions*, Serdica Math. J. **32** (2006), no. 4, 355–374.

[35] A. Bialostocki and T. Shaska, *Galois groups of prime degree polynomials with nonreal roots*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 243–255.

[36] T. Shaska, *Genus two curves covering elliptic curves: a computational approach*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 206–231.

[37] Jaime Gutierrez, D. Sevilla, and T. Shaska, *Hyperelliptic curves of genus 3 with prescribed automorphism group*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 109–123.

[38] Vishwanath Krishnamoorthy, Tanush Shaska, and Helmut Völklein, *Invariants of binary forms*, Progress in Galois theory, Dev. Math., vol. 12, Springer, New York, 2005, pp. 101–122.

[39] J. Gutierrez and T. Shaska, *Hyperelliptic curves with extra involutions*, LMS J. Comput. Math. **8** (2005), 102–115.

[40] Tanush Shaska and Jennifer L. Thompson, *On the generic curve of genus 3*, Affine algebraic geometry, Contemp. Math., vol. 369, Amer. Math. Soc., Providence, RI, 2005, pp. 233–243.

[41] Tanush Shaska, *Some special families of hyperelliptic curves*, J. Algebra Appl. **3** (2004), no. 1, 75–89.

[42] Tanush Shaska and Helmut Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), Springer, Berlin, 2004, pp. 703–723.

[43] T. Shaska, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280.

[44] _____ , *Computational aspects of hyperelliptic curves*, Computer mathematics, Lecture Notes Ser. Comput., vol. 10, World Sci. Publ., River Edge, NJ, 2003, pp. 248–257.

[45] Tanush Shaska, *Determining the automorphism group of a hyperelliptic curve*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2003, pp. 248–254 (electronic).

[46] Tony Shaska, *Genus 2 curves with $(3,3)$-split Jacobian and large automorphism group*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 205–218.

[47] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, *The locus of curves with prescribed automorphism group*, Sūrikaisekikenkyūsho Kōkyūroku **1267** (2002), 112–141. Communications in arithmetic fundamental groups (Kyoto, 1999/2001).

[48] T. Shaska, *Curves of genus 2 with (N,N) decomposable Jacobians*, J. Symbolic Comput. **31** (2001), no. 5, 603–617.

[49] Henning Stichtenoth, *Self-dual Goppa codes*, J. Pure Appl. Algebra **55** (1988), no. 1-2, 199–211.

[50] _____ , *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

[51] Stephan Wesemeyer, *On the automorphism group of various Goppa codes*, IEEE Trans. Inform. Theory **44** (1998), no. 2, 630–643.