Applicable Algebra in Engineering, Communication and Computing (2023) 34:629–648
https://doi.org/10.1007/s00200-021-00519-2

ORIGINAL PAPER

AG codes from $\mathbb{F}_{q^7}$-rational points of the GK maximal curve

Stefano Lia[1] · **Marco Timpanella**[2]

Received: 26 February 2021 / Revised: 15 June 2021 / Accepted: 30 June 2021 /
Published online: 4 September 2021

Abstract
In Beelen and Montanucci (Finite Fields Appl 52:10–29, 2018) and Giulietti and Korchmáros (Math Ann 343:229–245, 2009), Weierstrass semigroups at points of the Giulietti–Korchmáros curve $\mathcal{X}$ were investigated and the sets of minimal generators were determined for all points in $\mathcal{X}(\mathbb{F}_{q^2})$ and $\mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$. This paper completes their work by settling the remaining cases, that is, for points in $\mathcal{X}(\overline{\mathbb{F}}_q)\setminus\mathcal{X}(\mathbb{F}_{q^6})$. As an application to AG codes, we determine the dimensions and the lengths of duals of one-point codes from a point in $\mathcal{X}(\mathbb{F}_{q^7})\setminus\mathcal{X}(\mathbb{F}_q)$ and we give a bound on the Feng–Rao minimum distance d_{ORD}. For $q = 3$ we provide a table that also reports the exact values of d_{ORD}. As a further application we construct quantum codes from $\mathbb{F}_{q^7}$-rational points of the GK-curve.

Keywords Algebraic curves · AG codes · AG quantum codes · Weierstrass semigroups

1 Introduction

Algebraic geometric methods have largely been used for the construction of error-correcting linear codes from algebraic curves. The essential idea going back to Goppa's work (see [10] and [11]) is that a linear code can be obtained from an algebraic curve $\mathcal{X}$ defined over a finite field $\mathbb{F}_q$ by evaluating certain rational functions whose poles are prescribed by a given $\mathbb{F}_q$-rational divisor G at some $\mathbb{F}_q$-rational divisor D whose support is disjoint from that of G. These codes are

✉ Marco Timpanella
marco.timpanella@unicampania.it

Stefano Lia
stefano.lia@unibas.it

[1] Department of Mathematics, Computer Science and Economics, University of the Basilicata, Potenza, Italy

[2] Department of Mathematics and Physics, University of Campania "Luigi Vanvitelli", Caserta, Italy

called functional (or evaluation) codes. The dual of such a code can also be obtained by using Goppa's idea, taking residues of differential forms rather than rational functions. They are called differential AG codes. Actually, any linear code is an AG code; see [19].

AG codes are proven to have good performances provided that $\mathcal{X}$, G and D are carefully chosen in an appropriate way. In particular, AG codes with better parameters can arise from curves which have many $\mathbb{F}_q$-rational points, especially from maximal curves which are curves defined over $\mathbb{F}_q$ with q square whose number of $\mathbb{F}_q$-rational points $\mathcal{X}(\mathbb{F}_q)$ attains the Hasse-Weil upper bound, namely $|\mathcal{X}(\mathbb{F}_q)| = q + 1 + 2\mathfrak{g}\sqrt{q}$, where $\mathfrak{g}$ is the genus of $\mathcal{X}$; for AG codes from maximal curves see for instance [6, 13, 17, 18]. Regarding the choice of the two divisors D and G, the latter is typically taken to be a multiple mP of a single point P of degree one. Such codes are known as one-point codes, and have been extensively investigated; see for instance [5, 8, 15, 21, 24].

An important ingredient for the construction of one-point AG codes is the Weierstrass semigroup $H(P)$ of $\mathcal{X}$ at P, whose elements are the non-negative integers k for which there exists a rational function on $\mathcal{X}$ having pole divisor kP. Indeed, the knowledge of this semigroup allows to obtain useful information on the parameters of functional and differential codes. Although the structure of $H(P)$ is not always the same for every point P of $\mathcal{X}$, it is known that this holds true for all but a finite number of points $P \in \mathcal{X}$. A point for which the Weierstrass semigroup is not the typical one is a called a Weierstrass point. If $G(P) := \mathbb{N}\backslash H(P)$ denotes the set of gaps at P, it is well known that the size of $G(P)$ equals the genus $\mathfrak{g}$ of $\mathcal{X}$ for every $P \in \mathcal{X}$; see [22, Theorem 1.6.8].

Several papers have been dedicated to the construction of AG codes from the GK curves; see [1, 2, 4, 7]. The GK-curves are $\mathbb{F}_{q^6}$-maximal curves due to Giulietti and Korchmáros, which provided the first family of maximal curves that are not subcovers of the Hermitian curve [9]. The Weierstrass semigroup is known at any $\mathbb{F}_{q^2}$-rational point of the GK curve $\mathcal{X}$, see [9], as well as at any point in $\mathcal{X}(\mathbb{F}_{q^6})\backslash\mathcal{X}(\mathbb{F}_{q^2})$, see [3]. In the latter paper, see Result 7, the authors also deal with Weierstrass semigroups at points in $\mathcal{X}(\overline{\mathbb{F}}_q)\backslash\mathcal{X}(\mathbb{F}_{q^6})$, showing that the Weierstrass points of the GK curve are exactly its $\mathbb{F}_{q^6}$-rational points. However the problem of determining the generators of a Weierstrass semigroup $H(P)$ with $P \in \mathcal{X}(\overline{\mathbb{F}}_q)\backslash\mathcal{X}(\mathbb{F}_{q^6})$ has remained open. In the present paper we solve this problem. Therefore the Weierstrass semigroups at the points of the GK curve are completely determined.

Let $S = S_1 \cup S_2$, with

$$\begin{aligned} S_1 &= \{q^3 + i(q^3 - q) + j(q^4 - q^3 - q^2) \mid i = 0, \dots, q-1, \quad j = 0, \dots, q-1\}, \\ S_2 &= \{q^3 - 1 + i(q^3 - q) + j(q^4 - q^2 - 1) \mid i = 0, \dots, q-1, \quad j = 0, \dots, q-2\}. \end{aligned}$$

Then, our main result is the following theorem.

Theorem 1 *Let $\mathcal{X}$ be the GK curve over $\mathbb{F}_q$ and let $P \in \mathcal{X}(\bar{\mathbb{F}}_q)\backslash\mathcal{X}(\mathbb{F}_{q^6})$. Then if $q > 2$, S is a minimal set of generators for the Weierstrass semigroup $H(P)$. For $q = 2$, the minimal set of generators for $H(P)$ is* $\{7, 8, 12, 13, 18\}$.

This theorem together with the already quoted previous results provide a complete description of the Weierstrass semigroups at any point of the *GK*-curve.

Theorem 2 *Let $\mathcal{X}$ be the GK curve over $\mathbb{F}_q$ and P be a point of $\mathcal{X}$. Then one of the following occurs, where $e(H(P))$ denotes the number of generators of $H(P)$.*

- $P \in \mathcal{X}(\mathbb{F}_{q^2})$, $H(P) = \langle q^3 - q^2 + q, q^3, q^3 + 1\rangle$ *and* $e(H(P)) = 3$;
- $P \in \mathcal{X}(\mathbb{F}_{q^6})\backslash\mathcal{X}(\mathbb{F}_{q^2})$, $H(P) = \langle q^3 - q + 1, q^3 + 1, q^3 + i(q^4 - q^3 - q^2 + q - 1) : i = 0, \dots, q - 1\rangle$ *and* $e(H(P)) = q + 2$;
- $q > 2$, $P \in \mathcal{X}(\bar{\mathbb{F}}_q)\backslash\mathcal{X}(\mathbb{F}_{q^6})$, $H(P) = \langle S\rangle$ *and* $e(H(P)) = 2q^2 - q$;
- $q = 2$, $P \in \mathcal{X}(\bar{\mathbb{F}}_q)\backslash\mathcal{X}(\mathbb{F}_{q^6})$, $H(P) = \langle 7, 8, 12, 13, 18\rangle$ *and* $e(H(P)) = 5$,

The above results are then applied to the construction of AG codes and quantum codes from an $\mathbb{F}_{q^7}$-rational point of the GK curve. More in detail, Sect. 4 is devoted to the construction of dual codes of one-point AG codes. We investigate their parameters and we provide explicit tables in the case $q = 3$. In Sect. 5, by applying the CSS construction to the codes constructed in Sect. 4, we exhibit families of quantum codes. Also in this case, explicit tables are provided.

2 Background on numerical semigroups and on the GK-curve

2.1 Numerical semigroups

A subset H of $\mathbb{N}_0$ containing 0, which is closed under sums and which has finite complement is called a numerical semigroup. The main reference for the theory of numerical semigroups is [20]. Associated to H there are several invariants, parameters and subsets, the most important being the genus $g(H)$ and the gapset $G(H) = \mathbb{N}_0\backslash H$. The genus is the cardinality of the gapset, which, by definition, is finite.

For a nonempty subset $A = \{a_1, \dots, a_n\}$ of $\mathbb{N}_0$, $\langle A\rangle$ denotes the smallest subset of $\mathbb{N}_0$ containing A, 0 and closed under addition; clearly $\langle A\rangle = \mathbb{N}_0 a_1 + \cdots + \mathbb{N}_0 a_n$. For a numerical semigroup H, the minimal system of generators $\{h_1, \dots, h_e\}$ is the smallest subset of H such that $H = \langle h_1, \dots, h_e\rangle$, and its cardinality $e(H)$ is called the embedding dimension of H.

Definition 1 For a numerical semigroup H and $n \in H\backslash\{0\}$, the Apéry set of n is

$$Ap(H, n) := \{x \in H \mid x - n \notin H\}.$$

A strong connection between the Apéry set and the genus is given by the following result.

Result 3 [20, Lemma 2.4, Proposition 2.12] *Let H be a numerical semigroup and n a nonzero element of H. Then $|Ap(H, n)| = n$ and*

$$g(H) = \frac{1}{n} \sum_{x \in Ap(H,n)} x - \frac{n-1}{2}. \tag{1}$$

2.2 Weierstrass semigroups and AG codes

For a curve $\mathcal{X}$, we adopt the usual notation and terminology. In particular, $\mathbb{F}_q(\mathcal{X})$ and $\mathcal{X}(\mathbb{F}_q)$ denote the field of $\mathbb{F}_q$-rational functions on $\mathcal{X}$ and the set of $\mathbb{F}_q$-rational points of $\mathcal{X}$, respectively, and $\mathrm{Div}(\mathcal{X})$ denotes the set of divisors of $\mathcal{X}$, where a divisor $D \in \mathrm{Div}(\mathcal{X})$ is a formal sum $n_1P_1 + \cdots + n_rP_r$, with $P_i \in \mathcal{X}$, $n_i \in \mathbb{Z}$ and $P_i \neq P_j$ if $i \neq j$. The support $\mathrm{Supp}\,(D)$ of the divisor D is the set of points P_i such that $n_i \neq 0$, while $\deg(D) = \sum_i n_i$ is the degree of D. The divisor D is $\mathbb{F}_q$-rational if $n_i \neq 0$ implies $P_i \in \mathcal{X}(\mathbb{F}_q)$. For a function $f \in \mathbb{F}_q(\mathcal{X})$, (f), $(f)_0$ and $(f)_\infty$ are the divisor of f, its divisor of zeroes and its divisor of poles, respectively. The Weierstrass semigroup $H(P)$ at $P \in \mathcal{X}$ is

$$H(P) := \{n \in \mathbb{N}_0 \mid \exists f \in \mathbb{F}_q(\mathcal{X}), (f)_\infty = nP\} = \{\rho_0 = 0 < \rho_1 < \rho_2 < \cdots\}.$$

The Riemann-Roch space associated with an $\mathbb{F}_q$-rational divisor D is

$$\mathcal{L}(D) := \{f \in \mathcal{X}(\mathbb{F}_q) \ : \ (f) + D \geq 0\} \cup \{0\}$$

and its vector space dimension over $\mathbb{F}_q$ is $\ell(D)$.

Fix a set of pairwise distinct $\mathbb{F}_q$-rational points $\{P_1, \cdots, P_N\}$, and let $D = P_1 + \cdots + P_N$. Take another divisor G whose support is disjoint from the support of D. The AG code $C(D, G)$ is the (linear) subspace of $\mathbb{F}_q^N$ which is defined as the image of the evaluation map $ev : \mathcal{L}(G) \to \mathbb{F}_q^N$ given by $ev(f) = (f(P_1), f(P_2), \ldots, f(P_N))$. In particular $C(D, G)$ has length N. Moreover, if $N > \deg(G)$ then ev is an embedding and $\ell(G)$ equals the dimension of $C(D, G)$. The minimum distance d of $C(D, G)$, usually depends on the choice of D and G. A lower bound for d is $d^* = N - \deg(G)$, where d^* is called the Goppa designed minimum distance of $C(D, G)$. Furthermore, if $\deg(G) > 2\mathfrak{g} - 2$ then $k = \deg(G) - \mathfrak{g} + 1$ by the Riemann--Roch Theorem; see [12, Theorem 2.65].

The dual code $C^\perp(D, G)$ can be obtained in a similar way from the $\mathbb{F}_q(\mathcal{X})$-vector space $\Omega(\mathcal{X})$ of differential forms over $\mathcal{X}$. With $\omega \in \Omega(\mathcal{X})$, there is associated the divisor (ω) of $\mathcal{X}$, and for an $\mathbb{F}_q$-rational divisor D,

$$\Omega(D) := \{\omega \in \Omega(\mathcal{X}) \ : \ (\omega) \geq D\} \cup \{0\}$$

is a $\mathbb{F}_q$-vector space of rational differential forms over $\mathcal{X}$. Then the code $C^\perp(D, G)$ coincides with the (linear) subspace of $\mathbb{F}_q^N$ which is the image of the vector space $\Omega(G - D)$ under the linear map $res_D : \Omega(G - D) \mapsto \mathbb{F}_q^N$ given by $res_D(\omega) = (res_{P_1}(\omega), \ldots, res_{P_N}(\omega))$, where $res_{P_i}(\omega)$ is the residue of ω at P_i. In particular, $C^\perp(D, G)$ is an AG code with dimension $k^\perp = N - k$ and minimum distance $d^\perp \geq \deg(G) - 2\mathfrak{g} + 2$.

In the case where $G = \alpha P$, $\alpha \in \mathbb{N}_0$, $P \in \mathcal{X}(\mathbb{F}_q)$, the AG code $C(D, G)$ is referred to as one-point AG code. For a Weierstrass semigroup $H(P) = \{\rho_0 = 0 < \rho_1 < \rho_2 < \cdots\}$ and an integer $\ell \geq 0$, the Feng–Rao function is

$$\nu_\ell := |\{(i,j) \in \mathbb{N}_0^2 \ : \ \rho_i + \rho_j = \rho_{\ell+1}\}|.$$

Consider

$$C_\ell(P) = C^\perp(P_1 + P_2 + \cdots + P_N, \rho_\ell P),$$

with $P, P_1, \ldots, P_N$ pairwise distint points in $\mathcal{X}(\mathbb{F}_q)$. The number

$$d_{ORD}(C_\ell(P)) := \min\{\nu_m \ : \ m \geq \ell\}$$

is a lower bound for the minimum distance $d(C_\ell(P))$ of the code $C_\ell(P)$ which is called the order bound or the Feng–Rao designed minimum distance of $C_\ell(P)$; see [12, Theorem 4.13].

For the following result see [12, Theorem 5.24].

Result 4 $d_{ORD}(C_\ell(P)) \geq \ell + 1 - \mathfrak{g}$. *Equality holds if* $\ell \geq 2c - \mathfrak{g} - 1$ *with* $c = \max\{m \in \mathbb{Z} \ : \ m - 1 \notin H(P)\}$.

2.3 The GK curve

Let q be a prime power and $\mathbb{K} = \bar{\mathbb{F}}_q$. The Giulietti-Korchmáros (GK) curve $\mathcal{X}$ is the first example of a $\mathbb{F}_{q^6}$-maximal curve which is covered by the Hermitian curve over $\mathbb{F}_{q^6}$ only for $q = 2$; see [9]. The GK curve $\mathcal{X}$ is a non-singular curve, viewed as curve of $PG(3, \mathbb{K})$, defined by the affine equations

$$\begin{cases} Y^{q+1} = X^q + X, \\ Z^{q^2-q+1} = Y^{q^2} - Y. \end{cases} \tag{2}$$

It has genus $\mathfrak{g}(\mathcal{X}) = \frac{1}{2}(q^5 - 2q^3 + q^2)$ and as many as $q^8 - q^6 + q^5 + 1$ $\mathbb{F}_{q^6}$-rational points. From Eq. (2), the GK curve is a Galois extension (in fact a Kummer extension) of the Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ given by the affine equation $Y^{q+1} = X^q + X$. The automorphism group $\mathrm{Aut}(\mathcal{X})$ of $\mathcal{X}$ is also defined over $\mathbb{F}_{q^6}$. It has order $q^3(q^3+1)(q^2-1)(q^2-q+1)$ and contains a normal subgroup isomorphic to $SU(3, q)$.

The set of $\mathbb{F}_{q^6}$-rational points of $\mathcal{X}$ splits into two orbits $\mathcal{O}_1 = \mathcal{X}(\mathbb{F}_{q^2})$ and $\mathcal{O}_2 = \mathcal{X}(\mathbb{F}_{q^6}) \backslash \mathcal{X}(\mathbb{F}_{q^2})$ under the action of $\mathrm{Aut}(\mathcal{X})$. The orbit $\mathcal{O}_1$ is non-tame and has size $q^3 + 1$, whereas $\mathcal{O}_2$ is tame of size $q^3(q^3+1)(q^2-1)$. Furthermore, these are the only short orbits of $\mathrm{Aut}(\mathcal{X})$, and $\mathrm{Aut}(\mathcal{X})$ acts on $\mathcal{O}_1$ as PGU $(3, q)$ in its doubly transitive permutation representation; see [9, Theorem 7]. As it is known, the structure of Weierstrass semigroups is invariant under the action of automorphism groups; see [22, Lemma 3.5.2].

In Sect. 4 we will construct AG codes from $\mathbb{F}_{q^7}$-rational points of the GK curve. In order to compute the number of those points the following results will be useful.

Result 5 [16, Propositions 1 and 2] *Let $\mathcal{X}$ be a curve defined over $\mathbb{F}_q$. Then the following holds.*

1. *if $\mathcal{X}$ is $\mathbb{F}_q$-maximal and n is odd, then $\mathcal{X}$ is $\mathbb{F}_{q^n}$-maximal;*
2. if $\mathcal{X}$ is $\mathbb{F}_{q^{2n}}$-maximal, then $|\mathcal{X}(\mathbb{F}_{q^n})| = q^n + 1$.

As the Hermitian curve $\mathcal{H}_q$ is $\mathbb{F}_{q^2}$-maximal, the following corollary of Result 5 holds.

Result 6 *If d is odd, the number of $\mathbb{F}_{q^d}$-rational points of the Hermitian curve $\mathcal{H}_q$ is $q^d + 1$.*

Proposition 1 $|\mathcal{X}(\mathbb{F}_{q^7})| = q^7 + 1$.

Proof Observe that $(q^7 - 1, q^2 - q + 1) = (q^7 - 1 - (q^5 + q^4 - q^2 - q)(q^2 - q + 1), q^2 - q + 1)$ $= (q - 1, q^2 - q + 1) = 1$, and hence $q^2 - q + 1$ and $q^7 - 1$ are coprime. Therefore, the equation $X^{q^2-q+1} = c$, with $c \in \mathbb{F}_{q^7}$, has exactly one solution. This shows that the number of $\mathbb{F}_{q^7}$-rational points of $\mathcal{X}$ equals the number of $\mathbb{F}_{q^7}$-rational points of the Hermitian curve $\mathcal{H}_q$. Therefore the claim follows by Result 6. □

In [3] the Weierstrass semigroup $H(P)$ for $P \in \mathcal{X}(\overline{\mathbb{F}}_q)\backslash\mathcal{X}(\mathbb{F}_{q^6})$ was studied. In particular, the authors showed that $H(P)$ is the same for every $P \in \mathcal{X}(\overline{\mathbb{F}}_q)\backslash\mathcal{X}(\mathbb{F}_{q^6})$, and computed explicitly the set of gaps $G(P) = \mathbb{N}_0\backslash H(P)$.

Result 7 [3, Theorem 4.10] *Let P be a point of $\mathcal{X}$ with $P \in \mathcal{X}(\overline{\mathbb{F}}_q)\backslash\mathcal{X}(\mathbb{F}_{q^6})$. Then the set of gaps at P is*

$$\begin{aligned} G(P) = \{ & iq^3 + kq + m(q^2+1) + \sum_{s=1}^{q-2}(n_s(s+1)q^2) \\ & + j + 1 \mid i,j,k,m,\dots,n_{q-2} \geq 0, \\ & j \leq q-1, \text{ and } i + j + k + mq + \sum_{s=1}^{q-2}(n_s((s+1)q - s)) \leq q^2 - 2\}. \end{aligned} \tag{3}$$

Each element of $G(P)$ admits a unique representation as in (3), i.e. each element of $G(P)$ is uniquely identified by the tuple of coefficients $(i,j,k,m,n_1,\dots,n_{q-2})$. Furthermore the set $G(P)$ is the disjoint union of the sets G_1, G_2, G_3, where

- *G_1 is the subset of $G(P)$ corresponding to the coefficients $(i,0,k,m,0,\dots,0)$. Moreover, from (3), $0 \leq m \leq q-1$;*
- *G_2 is the subset of $G(P)$ corresponding to the coefficients $(i,j,k,m,0,\dots,0)$ such that $1 \leq j \leq q-1$, $k \leq q-1$ and $j + m \leq q-1$;*
- *G_3 is the subset of $G(P)$ corresponding to the coefficients $(i,j,k,0,\dots,n_s,\dots,0)$ such that $1 \leq s \leq q-2$, $n_s = 1$ and $i + k + (s+1)q \geq q^2 - 1$.*

Result 8 [3, Observation 4.4] *For a point* $P \in \mathcal{X}(\overline{\mathbb{F}}_q)\backslash\mathcal{X}(\mathbb{F}_{q^6})$, $\max\{m \in \mathbb{Z} \ : \ m-1 \ m-1 \notin H(P)\} = 2\mathfrak{g} - q^2 + 2$.

3 Proof of Theorem 1

For $q = 2$ the claim is already known; see [3, Example 4.12]. Therefore, assume $q > 2$ and let T denote the semigroup generated by S. To show $T = H(P)$ it is enough to prove that $T \subset H(P)$ and that T and $H(P)$ have the same genus. For this purpose, some properties of the following subsets of T are useful.

$$\begin{aligned}
Ap_1 :=&\{a(q^3-1)+i(q^3-q)+j(q^4-q^3-q^2) \mid a=2,\dots,q-1,\\
&\quad i=0,\dots,q-1, \quad j=0,\dots,a-2\};\\
Ap_{2,1} :=&\{q^3+i(q^3-q)+j(q^4-q^3-q^2) \mid\\
&\quad i=0,\dots,q-1, \quad j=0,\dots,q-1\};\\
Ap_{2,2} :=&\{(q^3-1)+i(q^3-q)+j(q^4-q^2-1) \mid\\
&\quad i=0,\dots,q-1, \quad j=0,\dots,q-2\};\\
Ap_2 :=&(Ap_{2,1}\backslash\{q^3\}) \cup Ap_{2,2};\\
Ap_3 :=&\{q^3+q^3-1+i(q^3-q)+j(q^4-q^3-q^2) \mid\\
&\quad i,j=0,\dots,q-1, \quad j\neq 0\}\\
Ap_4 :=&\{q^3+a(q^3-1)+i(q^3-q)+j(q^4-q^3-q^2) \mid\\
&\quad i=0,\dots,q-1,\\
&\quad j=2,\dots,q-1, \quad a=2,\dots,j\};\\
A :=&Ap_1 \cup Ap_2 \cup Ap_3 \cup Ap_4 \cup \{0\}.
\end{aligned}$$

Proposition 2 *The sets* Ap_1, $Ap_{2,1}$, $Ap_{2,2}$, Ap_3, *and* Ap_4 *are pairwise disjoint.*

Proof Let $x_{a,i,j}$ denote the element of Ap_1 corresponding to the choices of the parameters a, i, j, that is

$$x = a(q^3-1)+i(q^3-q)+j(q^4-q^3-q^2).$$

We use an analogous notation for the elements of $Ap_{2,1}$, $Ap_{2,2}$, Ap_3 and Ap_4.

- $Ap_1 \cap Ap_{2,1}$ is empty since no element of Ap_1 is divisible by q. The same argument also shows that $Ap_{2,1} \cap Ap_{2,2}$, $Ap_{2,1} \cap Ap_3$ and $Ap_{2,1} \cap Ap_4$ are empty.
- Let $x_{a,i,j} \in Ap_1$ and $x_{\bar{i},\bar{j}} \in Ap_{2,2}$. If $x_{a,i,j} = x_{\bar{i},\bar{j}}$ then

$$\begin{aligned} &a(q^3-1)+i(q^3-q)+j(q^4-q^3-q^2)\\ &\quad=(q^3-1)+\bar{i}(q^3-q)+\bar{j}(q^4-q^2-1). \end{aligned} \tag{4}$$

Reducing Eq. (4) modulo q we obtain $a=\bar{j}+1$. Substituting $a=\bar{j}+1$ in (4) and dividing by q it is readily seen (again reducing modulo q) that $i=\bar{i}$. Thus Eq. (4) now reads

$$j(q^2-q-1)=\bar{j}(q^2-q-1),$$

whence $j=\bar{j}$, a contradiction since $j\le a-2=\bar{j}-1$.

– Let $x_{a,i,j}\in Ap_1$ and $x_{\bar{i},\bar{j}}\in Ap_3$. If $x_{a,i,j}=x_{\bar{i},\bar{j}}$ then

$$\begin{aligned} &a(q^3-1)+i(q^3-q)+j(q^4-q^3-q^2)\\ &\quad=2q^3-1+\bar{i}(q^3-q)+\bar{j}(q^4-q^3-q^2), \end{aligned}$$

that modulo q yields $a=1$, a contradiction with $a\ge 2$.

– Let $x_{a,i,j}\in Ap_1$ and $x_{\bar{a},\bar{i},\bar{j}}\in Ap_4$. If $x_{a,i,j}=x_{\bar{a},\bar{i},\bar{j}}$ then

$$\begin{aligned} &a(q^3-1)+i(q^3-q)+j(q^4-q^3-q^2)\\ &\quad=q^3+\bar{a}(q^3-1)+\bar{i}(q^3-q)+\bar{j}(q^4-q^3-q^2), \end{aligned}$$

that modulo q yields $a=\bar{a}$. Therefore

$$i(q^3-q)+j(q^4-q^3-q^2)=q^3+\bar{i}(q^3-q)+\bar{j}(q^4-q^3-q^2),$$

whence $i=\bar{i}$ follows. Thus

$$j(q^4-q^3-q^2)=q^3+\bar{j}(q^4-q^3-q^2),$$

whence $j\ge\bar{j}$, a contradiction with $j\le a-2=\bar{a}-2\le\bar{j}-2$.

– $Ap_{2,2}\cap Ap_3$ is empty since for every element x of Ap_3, $x-(q^3-1)$ is divisible by q, whereas this fails for any element of $Ap_{2,2}$.

– Let $x_{i,j}\in Ap_{2,2}$ and $x_{\bar{a},\bar{i},\bar{j}}\in Ap_4$. If $x_{i,j}=\bar{x}_{\bar{a},\bar{i},\bar{j}}$ then

$$\begin{aligned} &(q^3-1)+i(q^3-q)+j(q^4-q^2-1)\\ &\quad=q^3+\bar{a}(q^3-1)+\bar{i}(q^3-q)+\bar{j}(q^4-q^3-q^2), \end{aligned} \tag{5}$$

whence reducing modulo q yields $j=\bar{a}-1$. Now Equation (6) reads

$$i(q^2-1)+j(q^3-q^2-q)-q^2=\bar{i}(q^2-1)+\bar{j}(q^3-q^2-q), \tag{6}$$

and hence $i=\bar{i}$. Therefore

$$j(q^3-q^2-q)=q^2+\bar{j}(q^3-q^2-q)$$

and $j\ge\bar{j}$, a contradiction with $j=\bar{a}-1\le\bar{j}-1$.

– $Ap_3\cap Ap_4$ is empty since for every element x of Ap_3, $x+1$ is divisible by q, but this fails for any element of Ap_4.

□

Proposition 3 *The cardinalities of the sets Ap_1, Ap_2, Ap_3, Ap_4 are as follows*

(i) $|Ap_1| = |Ap_4| = q(q-1)(q-2)/2$;
(ii) $|Ap_2| = q^2 + q(q-1) - 1$;
(iii) $|Ap_3| = q(q-1)$;
(iv) $|A| = q^3$.

Proof From the definition of Ap_1, $Ap_{2,1}$, $Ap_{2,2}$ Ap_3, and Ap_4, a straightforward computation shows that different choices of the parameters lead to different elements in the corresponding set.

We provide here the proof for the case Ap_1. Analogous computations can be applied to the other cases. Let $x, y \in Ap_1$, so

$$x = a(q^3-1) + i(q^3-q) + j(q^4-q^3-q^2)$$

and

$$y = \bar{a}(q^3-1) + \bar{i}(q^3-q) + \bar{j}(q^4-q^3-q^2),$$

with $a, \bar{a} \in \{2, \dots, q-1\}$, $i, \bar{i} \in \{0, \dots, q-1\}$, and $j \in \{0, \dots, a-2\}$, $\bar{j} \in \{0, \dots, \bar{a}-2\}$. Assume that $x = y$ holds. Then $a \equiv \bar{a} \pmod{q}$, and since $a, \bar{a} \in \{2, \dots, q-1\}$, we obtain $a = \bar{a}$. Therefore

$$i(q^3-q) + j(q^4-q^3-q^2) = \bar{i}(q^3-q) + \bar{j}(q^4-q^3-q^2),$$

whence

$$i(q^2-1) + j(q^3-q^2-q) = \bar{i}(q^2-1) + \bar{j}(q^3-q^2-q).$$

By applying the same argument as above, we obtain $i = \bar{i}$. Finally, this implies $j = \bar{j}$, and so the claim follows. □

Proposition 4 *If $x \in A$ then $x - q^3 \notin H(P)$.*

Proof For each element x in A, we exhibit a representation of $x - q^3$ as in (3). The claim trivially holds for $x = 0$. Moreover,

(a) if $x \in Ap_1$ then

$$\begin{aligned} x - q^3 &= a(q^3-1) + i(q^3-q) + j(q^4-q^3-q^2) - q^3 \\ &= (a + i + jq - j - 2)q^3 + (q - j - 1)q^2 + (q - i - 1)q + q - a - 1 + 1, \end{aligned}$$

where $a \in \{2, \dots, q-1\}$, $i \in \{0, \dots, q-1\}$ and $j \in \{0, \dots, a-2\}$. Therefore

$$\begin{cases} a+i+jq-j-2 \geq 0 \\ q-j-1 \geq 0 \\ q-i-1 \geq 0 \\ 0 \leq q-a-1 \leq q-1 \\ (a+i+jq-j-2)+q(q-j-1)-(q-j-2)+(q-i-1)+ \\ +(q-a-1)=q^2-2. \end{cases}$$

Therefore $x-q^3 \notin H(P)$ by (3).

(b) if $x \in Ap_{2,1} \setminus \{q^3\}$ then

$$\begin{aligned} x-q^3 =& i(q^3-q)+j(q^4-q^3-q^2) \\ =& (i+jq-j-1)q^3+(q-j-1)(q^2+1)+(q-i-1)q+j+1; \end{aligned} \tag{7}$$

where $i \in \{0,\dots,q-1\}$ and $j \in \{0,\dots,q-1\}$. Since $x \neq q^3$, $(i,j) \neq (0,0)$ and

$$\begin{cases} i+jq-j-1 \geq 0 \\ q-j-1 \geq 0 \\ q-i-1 \geq 0 \\ 0 \leq j \leq q-1 \\ i+jq-j-1+q(q-j-1)+(q-i-1)+j=q^2-2. \end{cases}$$

Therefore $x-q^3 \notin H(P)$ by (3).

(c) if $x \in Ap_{2,2}$ then

$$\begin{aligned} x-q^3 =& i(q^3-q)+j(q^4-q^2-1)-1 \\ =& (i+jq-1)q^3+(q-j-2)(q^2+1)+(2q-i-1)q+1; \end{aligned} \tag{8}$$

where $i \in \{0,\dots,q-1\}$ and $j \in \{0,\dots,q-2\}$. Now if $(i,j)=(0,0)$ then $x=q^3-1$ and hence $x-q^3 \notin H(P)$. Therefore $(i,j) \neq (0,0)$ is assumed. Then

$$\begin{cases} i+jq-1 \geq 0 \\ q-j-2 \geq 0 \\ 2q-i-1 \geq 0 \\ i+jq-1+q(q-j-2)+(2q-i-1)=q^2-2. \end{cases}$$

Therefore $x-q^3 \notin H(P)$ by (3).

(d) if $x \in Ap_3$ then

$$\begin{aligned} x-q^3 &= q^3-1+i(q^3-q)+j(q^4-q^3-q^2) \\ &= (i+jq-j)q^3+(q-j-1)(q^2+1)+(q-i-1)q+j-1+1; \end{aligned}$$

where $i \in \{0,\dots,q-1\}$ and $j \in \{1,\dots,q-1\}$. Therefore

$$\begin{cases} i+jq-j \geq 0 \\ q-j-1 \geq 0 \\ q-i-1 \geq 0 \\ 0 \leq j-1 \leq q-1 \\ i+jq-j+q(q-j-1)+(q-i-1)+j-1 = q^2-2. \end{cases}$$

Therefore $x - q^3 \notin H(P)$ by (3).

(e) if $x \in Ap_4$ then

$$\begin{aligned} x - q^3 &= a(q^3-1) + i(q^3-q) + j(q^4-q^3-q^2) \\ &= (i+jq-j+a-1)q^3 \\ &\quad + (q-j-1)(q^2+1) + (q-i-1)q + j - a + 1; \end{aligned}$$

where $i \in \{0, \ldots, q-1\}$, $j \in \{2, \ldots, q-1\}$ and $a \in \{2, \ldots, j\}$. Therefore

$$\begin{cases} i+jq-j+a-1 \geq 0 \\ q-j-1 \geq 0 \\ q-i-1 \geq 0 \\ 0 \leq j-a \leq q-1 \\ i+jq-j+a-1+q(q-j-1)+(q-i-1)+j-a = q^2-2. \end{cases}$$

Therefore $x - q^3 \notin H(P)$ by (3).

□

We use Proposition 4 to prove the following lemma.

Lemma 1 *The semigroup T is contained in $H(P)$.*

Proof Since $T = \langle S \rangle$, it suffices to show that $S = S_1 \cup S_2 \subseteq H(P)$. We carry out the computation for the case $x \in S_1 = Ap_{2,1}$. Analogous computation can be done for the other elements in $S_2 = Ap_{2,2}$. Take $x \in S_1$. Then

$$x = q^3 + i(q^3-q) + j(q^4-q^3-q^2),$$

for some $0 \leq i \leq q-1$ and $0 \leq j \leq q-1$. It may be observed that

$$x = (i+jq-j)q^3 + (q-j-1)(q^2+1) + (q-i-1)q + j + 1.$$

We assume on the contrary $x \in G(P)$. Taking into account Result 7 we distinguish three cases according to either $x \in G_1$, or $x \in G_2$, or $x \in G_3$.

– Case $x \in G_1$. There exist non-negative integers $\bar{m}, \bar{i}, \bar{k}$ such that $\bar{i} + \bar{k} + \bar{m}q \leq q^2 - 2$ and

$$\begin{aligned}&(i+jq-j)q^3+(q-j-1)(q^2+1)+(q-i-1)q+j+1\\&\quad=\bar{i}q^3+\bar{m}(q^2+1)+\bar{k}q+1.\end{aligned}\tag{9}$$

Equation (9) modulo q yields

$$\bar{m}\equiv -1 \pmod{q},$$

whence $\bar{m}=q-1$. Hence

$$(i+jq-j)q^3+(q-j-1)q^2+(q-i-1)q=\bar{i}q^3+\bar{m}q^2+\bar{k}q,$$

and, dividing by q,

$$(i+jq-j)q^2+(q-j-1)q+q-i-1=\bar{i}q^2+(q-1)q+\bar{k},$$

that is

$$(i+jq-j)q^2-jq+q-i-1=\bar{i}q^2+\bar{k}.\tag{10}$$

Equation (10) modulo q now yields

$$\bar{k}\equiv -i-1 \pmod{q}.$$

Moreover $\bar{i}+\bar{k}+\bar{m}q\le q^2-2$, gives $\bar{k}+\bar{i}\le q-2$ and hence $\bar{k}=q-i-1$.

Substituting in Eq. (10) we obtain

$$(i+jq-j)q^2-jq=\bar{i}q^2.$$

Again dividing by q and reducing shows $j\equiv 0 \pmod{q}$, whence $j=0$. Therefore $\bar{i}=i$, and a contradiction arises from $\bar{k}+\bar{i}\le q-2$.

– Case $x\in G_2$. There exist non-negative integers $\bar{m},\bar{i},\bar{k}$ and $\bar{j}$ such that

$$\begin{cases}1\le\bar{j}\le q-1,\\ \bar{k}\le q-1,\\ \bar{j}+\bar{m}\le q-1,\\ \bar{i}+\bar{k}+\bar{j}+\bar{m}q\le q^2-2\end{cases}$$

and

$$\begin{aligned}&(i+jq-j)q^3+(q-j-1)(q^2+1)+(q-i-1)q+j+1\\&\quad=\bar{i}q^3+\bar{m}(q^2+1)+\bar{k}q+\bar{j}+1.\end{aligned}\tag{11}$$

Then, reducing modulo q, Eq. (11) yields $\bar{j}+\bar{m}\equiv -1 \pmod{q}$. As $\bar{j}+\bar{m}\le q-1$, we have $\bar{j}+\bar{m}=q-1$ and (11) reads

$$\begin{aligned}&(i+jq-j)q^3+(q-j-1)(q^2+1)+(q-i-1)q+j+1\\&\quad=\bar{i}q^3+\bar{m}q^2+\bar{k}q+\bar{m}+\bar{j}+1,\end{aligned}$$

that is

$$(i+jq-j)q^2+(q-j-1)q+q-i-1=\bar{i}q^2+\bar{m}q+\bar{k}. \tag{12}$$

Again, $\bar{k}\le q-1$ and Eq. (12) modulo q imply $\bar{k}=q-i-1$. Thus

$$(i+jq-j)q+(q-j-1)=\bar{i}q+\bar{m}, \tag{13}$$

whence $\bar{m}=q-j-1$ and $\bar{j}=j$. Finally, $\bar{i}=i+jq-j$ and

$$\begin{aligned}\bar{i}+\bar{k}+\bar{j}+\bar{m}q&=i+jq-j+q-i-1\\&\quad+j+(q-j-1)q=q^2-1>q^2-2,\end{aligned}$$

a contradiction.

– Case $x\in G_3$. There exist non-negative integers $s,\bar{i},\bar{k}$ and $\bar{j}$ such that

$$\begin{cases}1\le s\le q-2,\\ \bar{j},\bar{k}\le q-1,\\ \bar{i}+\bar{k}+(s+1)q\ge q^2-1,\\ \bar{i}+\bar{j}+\bar{k}+(s+1)q-s\le q^2-2\end{cases}$$

and

$$\begin{aligned}&(i+jq-j)q^3+(q-j-1)(q^2+1)+(q-i-1)q+j+1\\&\quad=\bar{i}q^3+(s+1)q^2+\bar{k}q+\bar{j}+1.\end{aligned} \tag{14}$$

Note that in particular $\bar{j}<s$ must hold. On the other hand, Eq. (14) modulo q yields $\bar{j}=q-1>s$, a contradiction.

□

Proposition 5 $A=Ap(H(P),q^3)=Ap(T,q^3)$.

Proof It is readily seen that each element of A is a linear combination of elements of S. Therefore $A\subset T$ and by Propositions 3 and 4 we get $A=Ap(H(P),q^3)$. Moreover, from Lemma 1 we have $T\subseteq H(P)$ so each gap of $H(P)$ is also a gap T, whence the claim follows. □

Now Result 3 and Proposition 5 show that T and $H(P)$ have the same genus. Furthermore, since T is contained in $H(P)$, $T=\langle S\rangle=H(P)$. Finally, since $S=Ap_2\cup\{q^3\}$, Proposition 3 yields $|S|=e(H(P))=2q^2-q$. This ends the proof of Theorem 1.

4 AG codes from $\mathbb{F}_{q^7}$-rational points of the GK curve

In this section we construct a family of AG codes from $\mathbb{F}_{q^7}$-rational points of the GK curve. For $q=3$ the parameters of the codes obtained are reported in the table below.

We keep our notation in Sect. 2.2. In particular, for a point $P \in \mathcal{X}(\mathbb{F}_{q^7}) \backslash \mathcal{X}(\mathbb{F}_q)$, $H(P) = \{0 = \rho_1 < \rho_2 < ...\}$ denotes the Weierstrass semigroup at P and $C_\ell(P)$ stands for the dual code $C_\ell(P) = C^\perp(D, \rho_\ell P)$, where

$$D = \sum_{Q \in \mathcal{X}(\mathbb{F}_{q^7}) \backslash \{P\}} Q$$

is a divisor supported at all $\mathbb{F}_{q^7}$-rational points of $\mathcal{X}$ but P. From the Feng–Rao lower bound on the minimum distance of $C_\ell(P)$, we have that $C_\ell(P)$ is an $[n, k, d]_{q^7}$ linear code, with $n = q^7$, $k = n - \ell$ and

$$d \geq \max\{d_{ORD}(C_\ell(P)), d^*\}, \tag{15}$$

where $d^* = \deg(G) - 2\mathfrak{g} + 2$ denotes the designed minimum distance of $C_\ell(P)$. We remark that the Feng–Rao lower bound can be computed only in terms of the Weierstrass semigroup $H(P)$, that we explicitly described in Theorem 1.

As a consequence of Results 4 and 8 the following result follows.

Proposition 6 *For every* $\ell \geq 3\mathfrak{g} - 2q^2 + 3$, $d_{ORD}(C_\ell(P)) = \ell + 1 - \mathfrak{g}$.

Remark 1 Proposition 6 also shows that if $\ell \geq 3\mathfrak{g} - 2q^2 + 3$, then $d_{ORD}(C_\ell(P)) = d^*$. Indeed, let $\ell = 3\mathfrak{g} - 2q^2 + 3 + r$ for some $r \geq 0$. Then $\ell = \mathfrak{g} + 1 + (2\mathfrak{g} - 2q^2 + 2 + r) \geq \mathfrak{g} + 1$. Since $\rho_{\mathfrak{g}+1} = 2\mathfrak{g}$ and Result 8 yields that $2\mathfrak{g} - q^2 + 1$ is the largest gap in $H(P)$, we have

$$\rho_\ell = 2\mathfrak{g} + (2\mathfrak{g} - 2q^2 + r + 2) = 4\mathfrak{g} - 2q^2 + r + 2.$$

Hence Proposition 6 yields

$$d_{ORD}(C_\ell(P)) = \ell + 1 - \mathfrak{g} = 2\mathfrak{g} - 2q^2 + 4 + r = \rho_\ell - 2\mathfrak{g} + 2 = d^*.$$

In the remaining cases $\ell < 3\mathfrak{g} - 2q^2 + 3$ and the Feng–Rao minimum distance may provide an improvement on the designed minimum distance d^*.

For $q = 3$ the parameters of the codes $C_\ell(P)$ are reported in the table below. These codes have length $n = 2187$, whereas their dimension k and their Feng–Rao minimum distance d_{ORD} varies. We limit ourselves to the cases where $d_{ORD}(C_\ell(P)) > d^*$ and by Remark 1 this can only happen when $\ell < 3\mathfrak{g} - 2q^2 + 3$. As the table shows, the Feng–Rao minimum distance is strictly greater than the designed minimum distance d^*, for all those cases apart from a small number of exceptions.

n	k	ρ_ℓ	d_{ORD}	k	ρ_ℓ	d_{ORD}	k	ρ_ℓ	d_{ORD}
2187	2185	26	2	2184	27	2	2183	50	2
2187	2182	51	2	2181	52	2	2180	53	2
2187	2179	54	2	2178	72	2	2177	74	2
2187	2176	75	2	2175	76	2	2174	77	2
2187	2173	78	2	2172	79	2	2171	80	2

n	k	ρ_ℓ	d_{ORD}	k	ρ_ℓ	d_{ORD}	k	ρ_ℓ	d_{ORD}
2187	2170	81	2	2169	96	2	2168	97	2
2187	2167	98	2	2166	99	2	2165	100	2
2187	2164	101	2	2163	102	2	2162	103	2
2187	2161	104	2	2160	105	2	2159	106	2
2187	2158	107	2	2157	108	2	2156	117	2
2187	2155	120	2	2154	121	2	2153	122	2
2187	2152	123	2	2151	124	2	2150	125	2
2187	2149	126	2	2148	127	2	2147	128	2
2187	2146	129	2	2145	130	2	2144	131	2
2187	2143	132	2	2142	133	2	2141	134	2
2187	2140	135	2	2139	141	2	2138	143	2
2187	2137	144	2	2136	145	2	2135	146	2
2187	2134	147	2	2133	148	2	2132	149	2
2187	2131	150	2	2130	151	2	2129	152	2
2187	2128	153	2	2127	154	2	2126	155	2
2187	2125	156	2	2124	157	2	2123	158	2

n	k	ρ_ℓ	d_{ORD}	k	ρ_ℓ	d_{ORD}	k	ρ_ℓ	d_{ORD}
2187	2122	159	2	2121	160	2	2120	161	2
2187	2119	162	2	2118	165	6	2117	167	8
2187	2116	168	8	2115	169	8	2114	170	8
2187	2113	171	8	2112	172	8	2111	173	8
2187	2110	174	8	2109	175	8	2108	176	8
2187	2107	177	8	2106	178	8	2105	179	8
2187	2104	180	8	2103	181	8	2102	182	8
2187	2101	183	8	2100	184	8	2099	185	8
2187	2098	186	8	2097	187	8	2096	188	8
2187	2095	189	8	2094	191	11	2093	192	14
2187	2092	193	19	2091	194	19	2090	195	19
2187	2089	196	19	2088	197	19	2087	198	19
2187	2086	199	19	2085	200	19	2084	201	19
2187	2083	202	19	2082	203	19	2081	204	19
2187	2080	205	19	2079	206	19	2078	207	19
2187	2077	208	19	2076	209	19	2075	210	19
2187	2074	211	19	2073	212	19	2072	213	19
2187	2071	214	19	2068	217	28	2067	218	34
2187	2066	219	38	2065	220	43	2064	221	43
2187	2063	222	43	2062	223	43	2061	224	43
2187	2060	225	43	2059	226	43	2058	227	43
2187	2057	228	43	2056	229	43	2055	230	43
2187	2054	231	43	2053	232	43	2052	233	43

n	k	ρ_ℓ	d_{ORD}	k	ρ_ℓ	d_{ORD}	k	ρ_ℓ	d_{ORD}
2187	2051	234	43	2050	235	43	2049	236	43
2187	2048	237	43	2047	238	43	2041	244	54

n	k	ρ_ℓ	d_{ORD}	k	ρ_ℓ	d_{ORD}	k	ρ_ℓ	d_{ORD}
2187	2040	245	59	2039	246	62	2038	247	65
2187	2037	248	65	2036	249	65	2035	250	65
2187	2034	251	65	2033	252	65	2032	253	65
2187	2031	254	65	2030	255	65	2029	256	65
2187	2028	257	65	2027	258	65	2026	259	65
2187	2025	260	65	2023	262	67	2014	271	80
2187	2013	272	84	2012	273	86	2011	274	90
2187	2010	275	92	2009	276	92	2008	277	92
2187	2007	278	92	2006	279	92	2005	280	92

We point out that many other linear codes can be obtained from the above table by using the following propagation rules; see [23, Exercise 7].

Result 9 *If an* $[n, k, d]_q$ *linear code exists, then:*

(i) *for every non-negative integer* $s < d$, *an* $[n, k, d-s]_q$ *linear code exists;*
(ii) *for every non-negative integer* $s < k$, *an* $[n, k-s, d]_q$ *linear code exists;*
(iii) *for every non-negative integer* $s < k$, *an* $[n-s, k-s, d]_q$ *linear code exists;*
(iv) *for every non-negative integer* $s < \min\{n-k-1, d\}$, *an* $[n-s, k, d-s]_q$ *linear code exists.*

5 Quantum codes from $\mathbb{F}_{q^7}$-rational points of the GK curve

It is known that quantum codes can be constructed from (classical) linear codes by using the so-called CSS construction; see [14, Lemma 2.5]. Our aim is to show how the CSS-construction applies to one-point AG codes on the GK curve.

As before q is a prime power. Let $\mathbb{H} = (\mathbb{C}^q)^{\otimes n} = \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$ be a q^n-dimensional Hilbert space. Then the q-ary quantum code C of length n and dimension k are the q^k-dimensional Hilbert subspace of $\mathbb{H}$. Such quantum codes are denoted by $[[n, k, d]]_q$, where d is the minimum distance. As in the ordinary case, C can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors. Moreover, the quantum version of the Singleton bound states that for a $[[n, k, d]]_q$-quantum code, $2d + k \leq 2 + n$ holds. Again, by analogy with the ordinary case, the quantum Singleton defect and the relative quantum Singleton defect are defined to be $\delta_Q := n - k - 2d + 2$ and $\Delta_Q := \frac{\delta_Q}{n}$, respectively. We recall [14, Lemma 2.5].

Lemma 2 (CSS construction) *Let C_1 and C_2 be linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively, and assume that $C_1 \subset C_2$. Then there exists a $[[n, k_2 - k_1, d]]_q$-quantum code with*

$$d = \min\{w(c) \mid c \in (C_2 \backslash C_1) \cup (C_1^{\perp} \backslash C_2^{\perp})\}.$$

We apply the CSS construction to the dual codes $C_\ell(P)$ constructed in Sect. 4. We keep the same notation as in Sect. 4. For two non-gaps $\rho_\ell, \rho_{\ell+s} \in H(P)$, with $s \geq 1$, let $C_1 = C_{\ell+s}(P)$ and $C_2 = C_\ell(P)$ be the codes constructed in Sect. 4. Then $C_1 \subset C_2$. Also, if k_i denotes the dimension of C_i, then

$$k_2 = q^7 - h_\ell \quad \text{and} \quad k_1 = q^7 - h_{\ell+s} = q^7 - h_\ell - s,$$

where h_i is the number of those non-gaps at P that do not exceed i. The CSS construction now provides a $[[n, s, d]]_{q^7}$-quantum code with $n = q^7$ and

$$d = \min\{w(c) \mid c \in (C_\ell \backslash C_{\ell+s}) \cup (C(D, \rho_{\ell+s}P) \backslash C(D, \rho_\ell P))\}.$$

It may be noted that

$$d \geq \min\{d_{ORD}(C_\ell), d_1\}, \tag{16}$$

where d_1 is the minimum distance of $C(D, \rho_{\ell+s}P)$.

Theorem 10 *For every $\ell \in [3\mathfrak{g} - 2q^2 + 3, q^7 - \mathfrak{g}]$ and $s \in [1, q^7 - 2\ell]$ there exists a $[[q^7, s, d]]_{q^7}$-quantum code with $d \geq \ell + 1 - \mathfrak{g}$.*

Proof Since $\ell \geq 3\mathfrak{g} - 2q^2 + 3$, Proposition 6 applies and $d_{ORD}(C_\ell) = \ell + 1 - \mathfrak{g}$. Also, $\rho_{\ell+s} = \mathfrak{g} - 1 + \ell + s$, whence $d_1 \geq q^7 - \deg(\rho_{l+s}P) = q^7 - \rho_{\ell+s} \geq q^7 - \ell - s - \mathfrak{g} + 1$. Since $s \leq q^7 - 2\ell$, then $d_{ORD}(C_\ell) \leq d_1$ and the claim follows from (16). □

For $\ell \in [3\mathfrak{g} - 2q^2 + 3, q^7 - \mathfrak{g}]$ and $s = q^7 - 2\ell$, Theorem 10 proves the existence of $[[q^7, s, d]]_{q^7}$-quantum codes whose relative quantum Singleton defect Δ_Q is upper bounded as follows,

$$\Delta_Q = \frac{q^7 - s - 2d + 2}{q^7} = \frac{2\ell - 2d + 2}{q^7} \leq \frac{2\mathfrak{g}}{q^7} = \frac{q^5 - 2q^3 + q^2}{q^7},$$

and therefore it goes to 0 as q goes to infinity.

For $q = 3$ and ℓ ranging in $\mathfrak{g}, \ldots, 3\mathfrak{g} - 2q^2 + 2$ the following table reports the parameters of quantum codes which are the first non-trivial cases in which Theorem 10 does not apply.

n	s	$d \geq$	s	$d \geq$	s	$d \geq$	s	$d \geq$
2187	1989	1	1987	2	1985	3	1983	4
2187	1981	5	1979	6	1977	7	1975	8
2187	1973	9	1971	10	1969	11	1967	12
2187	1965	13	1963	14	1961	15	1959	16

n	s	$d \geq$	s	$d \geq$	s	$d \geq$	s	$d \geq$
2187	1957	17	1955	18	1953	19	1951	20
2187	1949	21	1947	22	1945	23	1943	24
2187	1941	25	1939	26	1937	27	1935	28
2187	1933	29	1931	30	1929	31	1927	32
2187	1925	33	1923	34	1921	35	1919	36
2187	1917	37	1915	38	1913	39	1911	40
2187	1909	41	1907	42	1905	43	1903	44
2187	1901	45	1899	46	1897	47	1895	48
2187	1893	49	1891	50	1889	51	1887	52
2187	1885	53	1883	54	1881	55	1879	56
2187	1877	57	1875	58	1873	59	1871	60
2187	1869	61	1867	62	1865	63	1863	64
2187	1861	65	1859	66	1857	67	1855	68
2187	1853	69	1851	70	1849	71	1847	72
2187	1845	73	1843	74	1841	75	1839	76
2187	1837	77	1835	78	1833	79	1831	80
2187	1829	81	1827	82	1825	83	1823	84

n	s	$d \geq$	s	$d \geq$	s	$d \geq$	s	$d \geq$
2187	1821	85	1819	86	1817	87	1815	88
2187	1813	89	1811	90	1809	91	1807	92
2187	1805	93	1803	94	1801	95	1799	96
2187	1797	97	1795	98	1793	99	1791	100
2187	1789	101	1787	102	1785	103	1783	104
2187	1781	105	1779	106	1777	107	1775	108
2187	1773	109	1771	110	1769	111	1767	112
2187	1765	113	1763	114	1761	115	1759	116
2187	1757	117	1755	118	1753	119	1751	120
2187	1749	121	1747	122	1745	123	1743	124
2187	1741	125	1739	126	1737	127	1735	128
2187	1733	129	1731	130	1729	131	1727	132
2187	1725	133	1723	134	1721	135	1719	136
2187	1717	137	1715	138	1713	139	1711	140
2187	1709	141	1707	142	1705	143	1703	144
2187	1701	145	1699	146	1697	147	1695	148
2187	1693	149	1691	150	1689	151	1687	152
2187	1685	153	1683	154	1681	155	1679	156
2187	1677	157	1675	158	1673	159	1671	160
2187	1669	161	1667	162	1665	163	1663	164
2187	1661	165	1659	166	1657	167	1655	168
2187	1653	169	1651	170	1649	171	1647	172

n	s	$d \geq$	s	$d \geq$	s	$d \geq$	s	$d \geq$
2187	1645	173	1643	174	1641	175	1639	176
2187	1637	177	1635	178	1633	179	1631	180
2187	1629	181	1627	182	1625	183		

We end this section with the construction of a second family of quantum codes arising from the GK curve. Our construction is based on a generalization of Lemma 2 given in [14, Theorem 3.1].

Lemma 3 (General t-point construction) *Let $\mathcal{Y}$ be an absolutely irreducible non-singular curve over $\mathbb{F}_q$ of genus $\mathfrak{g}$ containing $n+t$ distinct $\mathbb{F}_q$-rational points for some $n, t > 0$. For every $i = 1, \ldots, t$, let a_i, b_i be positive integers such that $a_i \leq b_i$ and that*

$$2\mathfrak{g} - 2 < \sum_{i=1}^{t} a_i < \sum_{i=1}^{t} b_i < n.$$

Then there exists a $[[n, k, d]]_q$-quantum code with $k = \sum_{i=1}^{t} b_i - \sum_{i=1}^{t} a_i$ and $d \geq \min\{n - \sum_{i=1}^{t} b_i, \sum_{i=1}^{t} a_i - (2\mathfrak{g} - 2)\}$.

Lemma 3 applied to the set of $\mathbb{F}_{q^7}$-rational points of the GK curve gives the following result.

Proposition 7 *Let $a, b \in \mathbb{N}_0$ such that*

$$q^5 - 2q^3 + q^2 - 2 < a < b < q^7.$$

Then there exists a quantum code with parameters $[[q^7, b-a, d]]_{q^7}$, where

$$d \geq \min\{q^7 - b,\ a - (q^5 - 2q^3 + q^2 - 2)\}.$$

Acknowledgements The research of S. Lia and M. Timpanella was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The second author was supported by the project "VALERE: VAnviteLli pEr la RicErca" of the University of Campania "Luigi Vanvitelli".

Funding Open access funding provided by Università degli Studi della Campania Luigi Vanvitelli within the CRUI-CARE Agreement.

References

1. Bartoli, D., Bonini, M.: Minimum weight codewords in dual Algebraic-Geometric codes from the Giulietti–Korchmáros curve. Des. Codes Cryptogr. **87**, 1433–1455 (2019). https://doi.org/10.1007/s10623-018-0541-y
2. Bartoli, D., Montanucci, M., Zini, G.: Multi point AG codes on the GK maximal curve. Des. Codes Cryptogr. **86**, 161–177 (2018)
3. Beelen, P., Montanucci, M.: Weierstrass semigroups on the Giulietti–Korchmáros curve. Finite Fields Appl. **52**, 10–29 (2018)
4. Castellanos, A.S., Tizziotti, G.C.: Two-point AG codes on the GK maximal curves. IEEE Trans. Inf. Theory **62**, 681–686 (2016)
5. Duursma, I., Kirov, R.: An Extension of the Order Bound for AG Codes. Lecture Notes in Computer Science, vol. 5527. Springer, Berlin (2009)
6. Eid, A., Hasson, H., Ksir, A., Peachey, J.: Suzuki-invariant codes from the Suzuki curve. Des. Codes Cryptogr. **81**, 413–425 (2016)
7. Fanali, S., Giulietti, M.: One-point AG codes on the GK maximal curves. IEEE Trans. Inf. Theory **56**, 202–210 (2010)
8. Geil, O., Munuera, C., Ruano, D., Torres, F.: On the order bounds for one-point AG codes. Adv. Math. Commun. **5**, 489–504 (2011)
9. Giulietti, M., Korchmáros, G.: A new family of maximal curves over a finite field. Math. Ann. **343**, 229–245 (2009)
10. Goppa, V.D.: Codes on algebraic curves. Dokl. Akad. NAUK SSSR **259**, 1289–1290 (1981)
11. Goppa, V.D.: Algebraic-geometric codes. Izv. Akad. NAUK SSSR **46**, 75–91 (1982)
12. Høholdt, T., van Lint, J.H., Pellikaan, R.: Algebraic geometry codes. In: Pless, V.S., Huffman, W.C., Brualdi, R.A. (eds.) Handbook of Coding Theory, vol. 1, pp. 871–961. Elsevier, Amsterdam (1998)
13. Korchmáros, G., Nagy, G.P., Timpanella, M.: Codes and gap sequences of Hermitian curves. IEEE Trans. Inf. Theory (2019)
14. La Guardia, G.G., Pereira, F.R.F.: Good and asymptotically good quantum codes derived from algebraic geometry codes. Quantum Inf. Process. **16**(6), Article ID 165, 12 pages (2017)
15. Matthews, G., Michel, T.W.: One-point codes using places of higher degree. IEEE Trans. Inf. Theory **51**, 1590–1593 (2005)
16. McGuire, G., Yılmaz, E.S.: Divisibility of L-polynomials for a family of Artin–Schreier curves. J. Pure Appl. Algebra **223**, 3341–3358 (2019)
17. Montanucci, M., Pallozzi, V.L.: AG codes from the second generalization of the GK maximal curve. Discrete Math. **343**, 111810 (2020)
18. Montanucci, M., Timpanella, M., Zini, G.: AG codes and AG quantum codes from cyclic extensions of the Suzuki and Ree curves. J. Geom. **109**, 23 (2018)
19. Pellikaan, R., Shen, B.Z., van Wee, G.J.M.: Which linear codes are algebraic-geometry. IEEE Trans. Inf. Theory **37**, 583–602 (1991)
20. Rosales, J.C., García-Sánchez, P.A.: Numerical Semigroups, Developments in Mathematics, vol. 20. Springer, New York (2009)
21. Sakata, S.: Fast erasure-and-error decoding of any one-point AG codes up to the Feng–Rao bound. Bull. Univ. Electro-Commun. **9**, 39–57 (1996)
22. Stichtenoth, H.: Algebraic Function Fields and Codes. Springer
23. Tsfasman, M.A., Vladut, S.G.: Algebraic-Geometric Codes. Kluwer, Amsterdam (1991)
24. Xing, C., Chen, H.: Improvements on parameters of one-point AG codes from Hermitian curves. IEEE Trans. Inf. Theory **48**, 535–537 (2002)