Correspondence

On Semigroups Generated by Two Consecutive Integers and Improved Hermitian Codes

Maria Bras-Amorós and Michael E. O'Sullivan, *Member, IEEE*

***Abstract*—Analysis of the Berlekamp–Massey–Sakata algorithm for decoding one-point codes leads to two methods for improving code rate. One method, due to Feng and Rao, removes parity checks that may be recovered by their majority voting algorithm. The second method is to design the code to correct only those error vectors of a given weight that are also geometrically generic. In this work, formulae are given for the redundancies of Hermitian codes optimized with respect to these criteria as well as the formula for the order bound on the minimum distance. The results proceed from an analysis of numerical semigroups generated by two consecutive integers.**

***Index Terms*—Feng–Rao improved code, Hermitian curve, numerical semigroup.**

I. Introduction

Numerical semigroups have proven to be very useful in the study of one-point algebraic-geometry codes. On one hand, the arithmetic of the numerical semigroup associated to the one-point yields a good bound—called the order bound—on minimum distance [1]–[4]. On the other hand, a close analysis of the numerical semigroup and the decoding algorithm commonly used for one-point codes shows that significant improvements in rate may be achieved while maintaining a given error correction capability [5]. In this article, we discuss the order bound and improvements to the rate for codes constructed from Hermitian curves.

Let us briefly recall the definition of one-point algebraic geometry codes and state the notation we will use. Suppose $\mathbb{F}$ is a finite field, $F/\mathbb{F}$ a function field and P a rational point of $F/\mathbb{F}$. For $m \in \mathbb{N}_0$ let $\mathcal{L}(mP)$ be the vector space of functions in F having poles only at P and of order at most m. Let v_P be the valuation of F associated with P and let $\Lambda = \{-v_P(f) : f \in \bigcup_m \mathcal{L}(mP)\}$. Λ is a *numerical semigroup*. That is, a subset of $\mathbb{N}_0$, closed under summation, containing 0 and with finite complement in $\mathbb{N}_0$. It is called the *Weierstrass semigroup* associated to P. Let $P_1, \ldots, P_n$ be pairwise distinct rational points of $F/\mathbb{F}$ which are different from P and let φ be the map $\bigcup_m \mathcal{L}(mP) \rightarrow \mathbb{F}^n$ such that $f \mapsto (f(P_1), \ldots, f(P_n))$. Suppose that $\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 < \cdots\}$. The ith one-point algebraic-geometry code associated with P and $P_1, \ldots, P_n$ is $[\varphi(\mathcal{L}(\lambda_i P))]^\perp$. Naturally, the semigroup which will give us information about the one-point codes on P will be the Weierstrass semigroup associated to P.

The *Hermitian curve* over $\mathbb{F}_{q^2}$, where q is a prime power, is defined by its affine equation $x^{q+1} = y^q + y$. It has a single point P_∞ at infinity and q^3 proper rational points $P_1, \ldots, P_{q^3}$. The ring of functions on the curve with poles only at P_∞ is generated, as a vector space over $\mathbb{F}_q$, by the set $\{x^i y^j : j < q\}$. Moreover, $v_{P_\infty}(x) = -q$ and $v_{P_\infty}(y) = -q - 1$. Thus, the Weierstrass semigroup at P_∞ is generated by q and $q+1$. *Hermitian codes* are the one-point codes defined on the Hermitian curve associated with P_∞ and $P_1, \ldots, P_{q^3}$. For details on the Hermitian curve and Hermitian codes, we refer to [6], [2], [7].

The scope of this work is to analyze some aspects of Hermitian codes based on the Weierstrass semigroup at P_∞. Since the only thing we will be using about the Hermitian codes is that the associated numerical semigroup is generated by two consecutive integers, all the results can be stated more generally for all those one-point codes for which the associated semigroup is generated by two consecutive integers. In Section II, we analyze the enumeration of semigroups generated by two consecutive integers. Then, we mention the known results on the sequence ν_i and the order bound. In Section III, we give formulas for the number of checks of optimal codes correcting all errors of a given weight, whenever the associated numerical semigroup is generated by two consecutive integers. Pellikaan and Torres in [8, p. 2513] stated that this formula was not known for Hermitian codes. In Section IV, we give formulas for the number of checks of optimal codes correcting all *generic* errors of a given weight.

II. On the Enumeration and the ν-Sequence of Semigroups Generated by Two Consecutive Integers

We start this section with a small survey of the nomenclator and notations we will use on numerical semigroups and, more specifically, those numerical semigroups generated by two consecutive integers. Then we will analyze the enumeration of the latter semigroups and give the tools we will use in Sections III and IV.

A. Semigroups Generated by Two Consecutive Integers

By a *numerical semigroup* we mean a subset of $\mathbb{N}_0$, whose complement in $\mathbb{N}_0$ is finite and which contains any sum of its elements. Given a numerical semigroup Λ we denote *gaps* the elements in its complement in $\mathbb{N}_0$. The *genus* g of Λ is the number of gaps while its *conductor* c is equal to the largest gap plus one. The *enumeration* λ of Λ is the unique increasing bijective map $\lambda : \mathbb{N}_0 \longrightarrow \Lambda$. We say λ_i to denote $\lambda(i)$. Notice that if λ_i is larger than or equal to the conductor or, equivalently, $i \geq c - g$, then $\lambda_i = i + g$.

In this work, we just deal with numerical semigroups generated by two consecutive integers. If the consecutive integers are $a, a+1$ then the numerical semigroup consists of any element $ia + j(a+1)$ with $i, j \in \mathbb{N}_0$. By properties of semigroups generated by two integers [2], we know that the genus of this semigroup is $g = \frac{(a-1)a}{2}$ and its conductor is $c = (a-1)a$. Furthermore, the semigroup generated by $a, a+1$ admits two alternative descriptions. The first one is given by the disjoint union

$$0 \sqcup \{a, a+1\} \sqcup \{2a, 2a+1, 2a+2\} \sqcup \cdots \sqcup \{(a-2)a, (a-2)a+1, \ldots, (a-2)a+a-2\} \sqcup \{i : i \geq (a-1)a\}.$$

The second one was proved in [9] and it is given in the next lemma.

Lemma 2.1: The numerical semigroup generated by $a, a+1$ is the set with all nonnegative integers whose remainder when dividing by a is at most the quotient.

Manuscript received September 28, 2006; revised March 29, 2007.

M. Bras-Amorós is with the Departament d'Enginyeria de la Informació i de les Comunicacions, Escola Tècnica Superior d'Enginyeria, Universitat Autònoma de Barcelona, 08193 Bellaterra, Spain (e-mail: maria.bras@gmail.com).

M. E. O'Sullivan is with the Department of Mathematics and Statistics, San Diego State University, San Diego, CA 92182 USA (e-mail: mosulliv@sciences.sdsu.edu).

Communicated by I. Dumer, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2007.899548

B. Enumeration

As one can see from Lemma 2.1, numerical semigroups generated by two consecutive integers are highly related to the set of pairs $\mathcal{P} = \{(x,y) : x, y \in \mathbb{N}_0, y \leq x\}$. In fact, the numerical semigroup generated by $a, a+1$ is the image of the map

$$\begin{aligned} \alpha_a : \mathcal{P} &\to \mathbb{N}_0 \\ (x,y) &\mapsto ax + y. \end{aligned}$$

It turns out that this map is one-to-one whenever $\alpha_a(x,y)$ is strictly less than $a(a+1)$. Indeed, if $l < a(a+1)$ and $(x,y) \in \alpha_a^{-1}(l)$ then x must be less than or equal to a and y must be strictly less than a. So x and y are the quotient and the remainder of the Euclidean division of l by a, which are unique. In particular, α_a is one-to-one whenever $\alpha_a(x,y)$ is less than or equal to the conductor of the semigroup, which is $c = a(a-1)$.

Furthermore, the total order

$$(x,y) < (x',y') \text{ if } \begin{cases} x < x' \\ x = x' \text{ and } y < y' \end{cases}$$

is compatible with the natural order of the semigroup for all those values in the semigroup which are less than $a(a+1)$. That is, for any $l, l' \in \Lambda$ with $l, l' < a(a+1)$, then $l < l'$ if and only if $\alpha_a^{-1}(l) < \alpha_a^{-1}(l')$.

Now, since $\sum_{j=0}^{k} j = \frac{k(k+1)}{2}$, the sequence $a_k = \frac{k(k+1)}{2}$ is increasing and $a_{k+1} - a_k = k+1$. So any integer i in $\mathbb{N}_0$ can be written uniquely as $i = \frac{x(x+1)}{2} + y$ for some $x \in \mathbb{N}_0$ and some $0 \leq y \leq x$. Thus, the map

$$\begin{aligned} \beta : \mathcal{P} &\to \mathbb{N}_0 \\ (x,y) &\mapsto \frac{x(x+1)}{2} + y \end{aligned}$$

is one-to-one everywhere and it is also compatible with the former total order.

As a conclusion, and taking into consideration that the genus and the conductor of the numerical semigroup generated by $a, a+1$ are, respectively, $\frac{(a-1)a}{2}$ and $(a-1)a$, one can see that the map $\lambda : \mathbb{N}_0 \longrightarrow \Lambda$ with

$$\lambda_i = \begin{cases} \alpha o \beta^{-1}(i), & \text{if } i \leq \frac{(a-1)a}{2} \\ i + \frac{(a-1)a}{2}, & otherwise \end{cases}$$

is increasing and one-to-one. Hence, it is exactly the enumeration of the semigroup generated by $a, a+1$.

C. The ν-Sequence and the Order Bound

Given a numerical semigroup Λ with enumeration λ define the sequence ν_i by

$$\nu_i = |\{j \in \mathbb{N}_0 : \lambda_i - \lambda_j \in \Lambda\}|.$$

The sequence ν_i is used to define the *order bound* on the minimum distance of one-point algebraic-geometry codes:

$$\delta_i = \min\{\nu_j : j > i\}.$$

The order bound, also known as Feng–Rao bound, is a lower bound on the minimum distance of the ith one-point code on P. In this case, the numerical semigroup is the Weierstrass semigroup associated to P. Details can be found in [1]–[4].

The Feng–Rao improved codes [5] are defined by means of the sequence ν_i as well. First a set of functions on the curve $\{z_i : i \in \mathbb{N}_0\}$ having only poles at P is considered such that the valuation of z_i at P is $-\lambda_i$. Now, the Feng–Rao code designed to correct t errors has as parity checks the evaluation in certain points of the curve of functions z_i for all i with $\nu_i < 2t+1$.

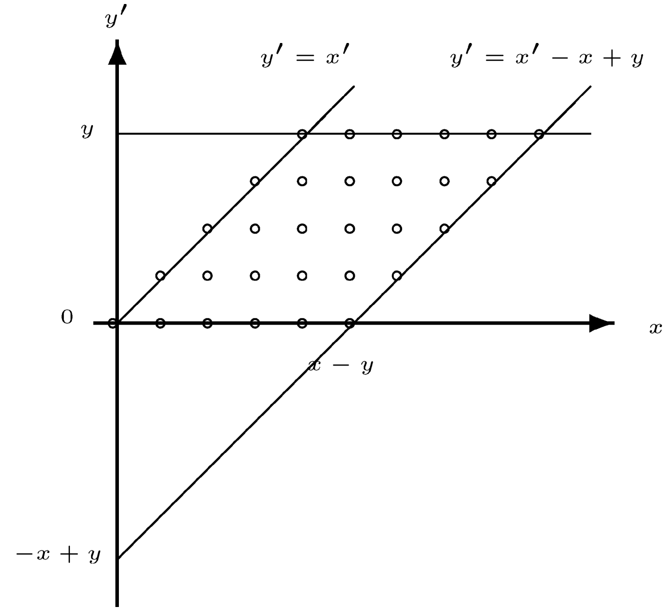

Fig. 1. Parallelogram in proof of Lemma 2.2.

In this subsection we derive the sequence ν_i as well as the order bound for numerical semigroups generated by two consecutive integers. For Hermitian codes this information has appeared previously (see [8], [2], and [10]). We choose to include our own proofs since our methods are new and will be needed later in the analysis of improved codes.

From now on, let Λ be the semigroup generated by a and $a+1$ and let g and c be respectively its genus and its conductor, and let λ be its enumeration. In order to compute the values in the sequence ν_i we need to distinguish between those elements $\lambda_i \in \Lambda$ for which $\lambda_i = ax + y$ for unique nonnegative integers x, y with $y \leq x$ from those for which x, y are not unique.

Let us denote by Λ^x the subset of Λ containing the elements $l = ax + y$ with $0 \leq y \leq x$. Then l is uniquely expressible as $l = ax + y$ for nonnegative integers x, y with $y \leq x$ if and only if $l \in \Lambda^x \setminus (\cup_{x' \neq x} \Lambda^{x'})$. Suppose $l = ax + y \in \Lambda^x$. Then $l = a(x-1) + a + y$ and $l \in \Lambda^{x-1}$ if and only if $a + y \leq x - 1$, i.e., $y \leq x - a - 1$. Similarly, $l = a(x+1) - a + y$ and $l \in \Lambda^{x+1}$ if and only if $-a + y \geq 0$, i.e., $y \geq a$. From this argument we have that $ax + y$ with $y \leq x$ is in $\Lambda^x \setminus (\cup_{x' \neq x} \Lambda^{x'})$ if and only if $x - a \leq y \leq a - 1$.

Lemma 2.2: Let $\lambda_i \in \Lambda$ and suppose that the Euclidean division of λ_i by a has quotient x and remainder y. If $x - a \leq y \leq a - 1$, then $\nu_i = (x - y + 1)(y + 1) = xy - y^2 + x + 1$.

Proof: Suppose $\lambda_i = \lambda_j + \lambda_k$. It is easy to check that if $\lambda_i \in \Lambda^x \setminus (\cup_{z \neq x} \Lambda^z)$ for some x, then $\lambda_j \in \Lambda^{x'} \setminus (\cup_{z \neq x'} \Lambda^z)$ and $\lambda_k \in \Lambda^{x''} \setminus (\cup_{z \neq x''} \Lambda^z)$ for some x', x''.

So

$$\begin{aligned} \nu_i &= |\{(x',y') \in \mathcal{P} : \lambda_i - ax' - y' \in \Lambda\}| \\ &= |\{(x',y') \in \mathcal{P} : (x - x', y - y') \in \mathcal{P}\}| \\ &= |\{(x',y') \in \mathbb{N}_0 \times \mathbb{N}_0 \\ &\qquad x' \leq x,\ y' \leq y,\ y' \leq x',\ y' \geq x' - x + y\}| \\ &= \sum_{0 \leq x' \leq x} |\{y' : \max\{0, y + x' - x\} \leq y' \leq \min\{y, x'\}\}|. \end{aligned}$$

This last number is the number of integer points inside a parallelogram with base $x - y + 1$ and height $y + 1$ (see Fig. 1). Hence it is equal to $(x - y + 1)(y + 1)$. □

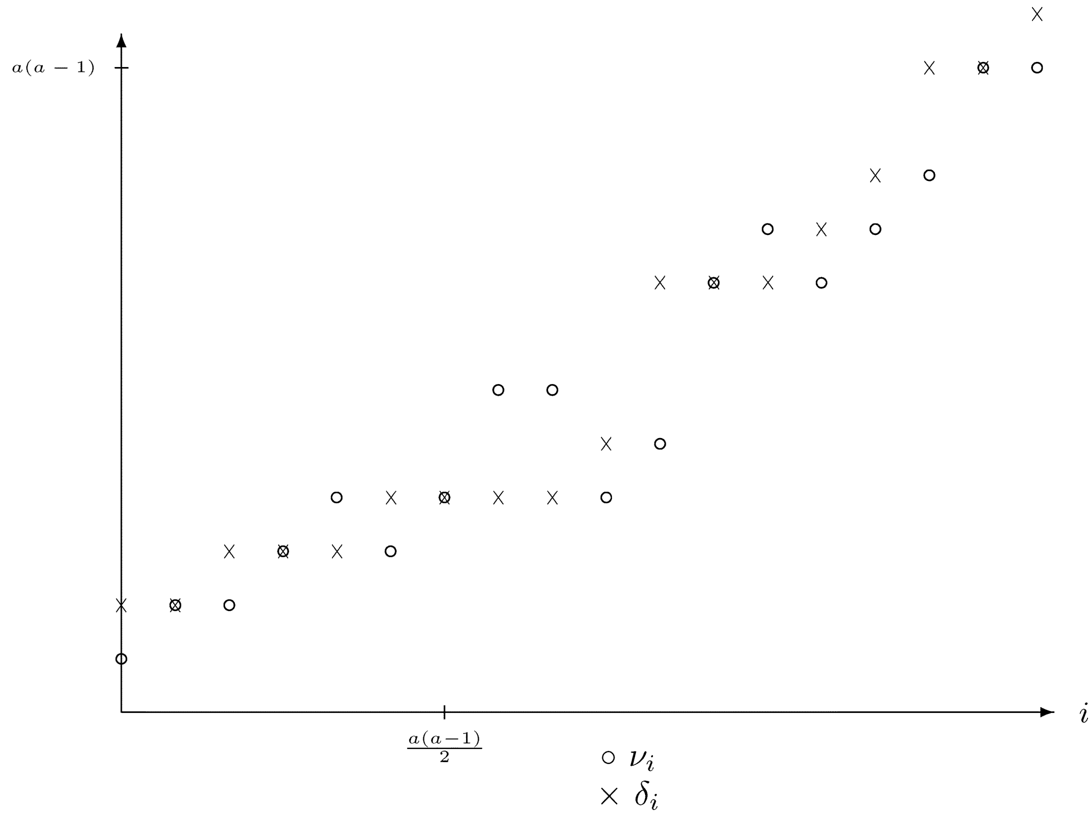

Fig. 2. Graph of ν_i and δ_i for the Hermitian code over $\mathbb{F}_{4^2}$.

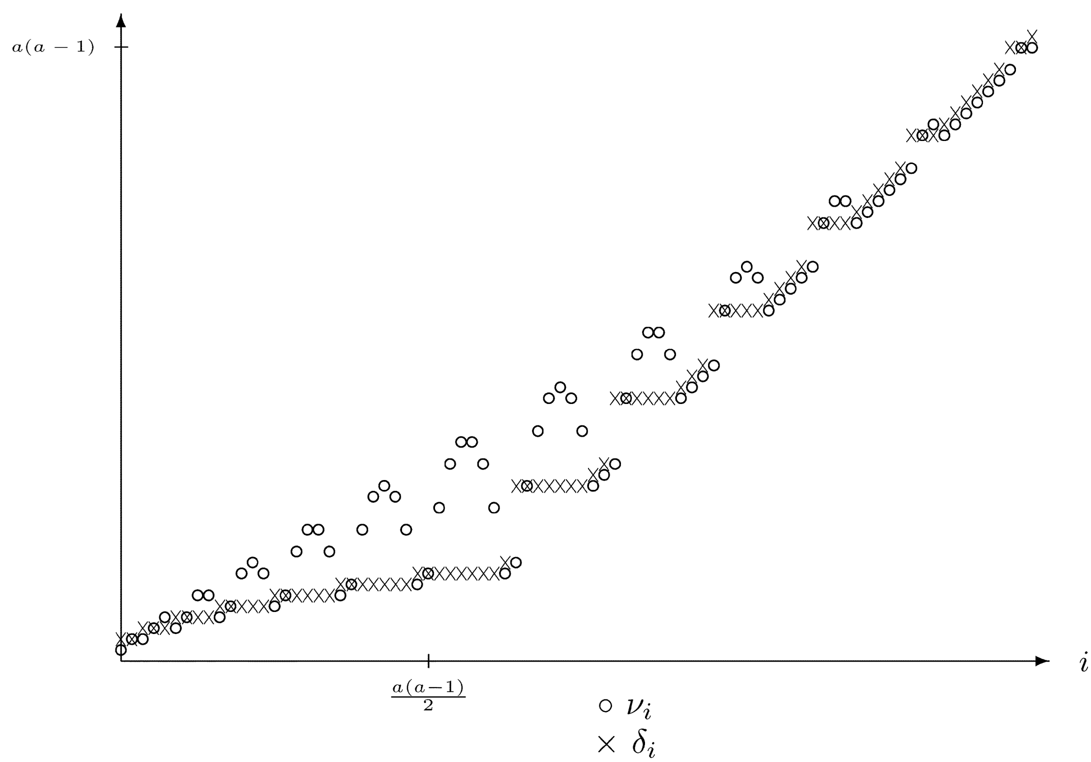

Fig. 3. Graph of ν_i and δ_i for the Hermitian code over $\mathbb{F}_{8^2}$.

To approach the case in which $\lambda_i = ax+y = ax'+y'$ with $x \neq x'$, $y \neq y'$, we need [4, Th. 4.6]. It says that if a numerical semigroup Λ is such that its conductor c is two times its genus, then for all $\lambda_i \in \Lambda$ such that $\lambda_i - c + 1 \in \Lambda$, we have $\nu_i = \lambda_i - c + 1$. We already know that for the numerical semigroup generated by $a, a+1$ the conductor is two times the genus. Let us check that if $\lambda_i \in \Lambda^x \cap \Lambda^{x+1}$ then $\lambda_i - c + 1 \in \Lambda$. Indeed, suppose $\lambda_i \in \Lambda^x \cap \Lambda^{x+1}$. Since $\lambda_i \in \Lambda^{x+1}$, $\lambda_i = (x+1)a + y$ with $y \leq x+1$. Now, since $\lambda_i \in \Lambda^x$ and

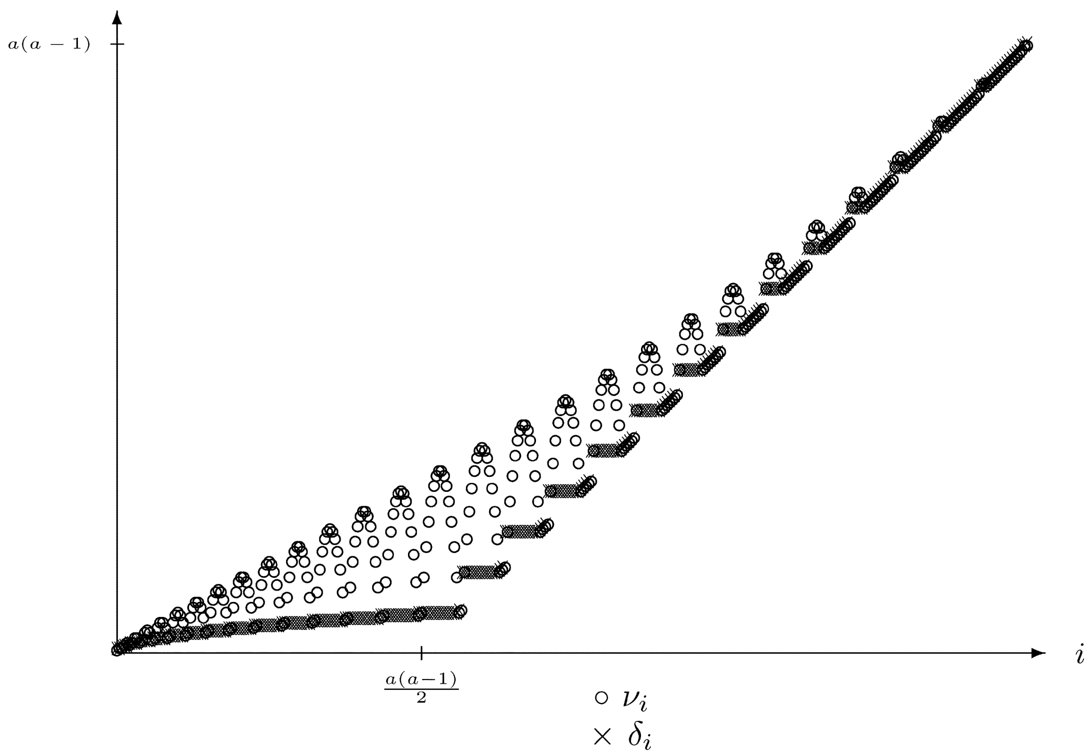

Fig. 4. Graph of ν_i and δ_i for the Hermitian code over $\mathbb{F}_{16^2}$.

$\lambda_i = xa + (a+y)$, we have $a+y \le x$. Thus, $\lambda_i - c + 1 = (x+1)a + y - a(a-1) + 1 = a(x-a+2)+y+1$ with $y+1 \le x-a+2$ and so $\lambda_i - c + 1 \in \Lambda$. Consequently, if $\lambda_i = ax+y = ax'+y'$ with $x \ne x'$, $y \ne y'$, then $\nu_i = \lambda_i - c + 1$.

The next theorem is a consequence of the former arguments.

Theorem 2.3: Let $\lambda_i \in \Lambda$ and suppose that the Euclidean division of λ_i by a has quotient x and remainder y. Then,

$$\nu_i = \begin{cases} (x-y+1)(y+1), & \text{if } -a+x \le y \le a-1, \\ \lambda_i - c + 1, & \text{otherwise.} \end{cases}$$

Once we have found a formula for the values in the sequence ν_i, the next step is to find a formula for the values of the order bound defined as $\delta_i = \min\{\nu_j : j > i\}$. Notice that this definition has a lot to do with the increasingness of the sequence ν_i.

From Theorem 2.3, we deduce that ν_i is quadratic in y for the integers i corresponding to the values $\lambda_i = ax + y$ inside Λ^x with $-a + x \le y \le a - 1$, while it is increasing elsewhere. See Figs. 2–5. By analyzing the parabola we see that ν_i is increasing for $y \le \frac{x}{2}$ and decreasing for $y \ge \frac{x}{2}$, being symmetric with respect to $y = \frac{x}{2}$. In the case when $x < a$ all values $ax + y \in \Lambda^x$ satisfy $-a + x \le y \le a - 1$. Then the first and last elements in Λ^x (i.e., $y = 0, y = x$) have the same value for ν_i, which is $x + 1$ and which is minimal. In the case when $x \ge a$, the first element (i.e., $y = -a + x$) attains the minimal value for ν_i, which is $ax - a^2 + x + 1$; the second and last elements (i.e., $y = -a + x + 1, y = a - 1$) have the same value for ν_i, which is $a(x - a + 2)$ and which is minimal if we take the first element away. Thus, we may conclude the following.

If $x \ge 2a$ then $\Lambda^x \setminus (\cup_{x' \ne x} \Lambda^{x'}) = \emptyset$ and

$$\min\{\nu_j : j > i\} = \nu_{i+1} = \lambda_i - c + 2.$$

If $x < a$ then $\Lambda^x \cap \Lambda^{x'} = \emptyset$ for any $x' \ne x$ and

$$\begin{aligned} \min\{\nu_i : \lambda_i \in \Lambda^x\} &= \nu_{\lambda^{-1}(ax)} = \nu_{\lambda^{-1}(ax+x)} \\ &= x + 1. \end{aligned} \tag{1}$$

The region $a \le x < 2a$ is more complicated. We have both $\Lambda^x \setminus (\cup_{x' \ne x} \Lambda^{x'}) \ne \emptyset$ and $\Lambda^x \cap \Lambda^{x+1} \ne \emptyset$. On one hand

$$\begin{aligned} \min\{\nu_i : \lambda_i \in \Lambda^x \setminus (\cup_{x' \ne x} \Lambda^{x'})\} &= \nu_{\lambda^{-1}(ax-a+x)} \\ &= ax + x - a^2 + 1 \end{aligned} \tag{2}$$

$$\begin{aligned} \min\{\nu_i : \lambda_i \in \Lambda^x \setminus (\cup_{x' \ne x} \Lambda^{x'}),\ \lambda_i \ne ax - a + x\} & \\ = \nu_{\lambda^{-1}(ax-a+x+1)} &= \nu_{\lambda^{-1}(ax+a-1)} \\ = a(x - a + 2) & \end{aligned} \tag{3}$$

$$\begin{aligned} \min\{\nu_i : \lambda_i \in \Lambda^x \cap \Lambda^{x+1}\} &= \nu_{\lambda^{-1}(ax+a)} \\ &= ax + 2a - a^2 + 1. \end{aligned} \tag{4}$$

On the other hand, one can show that for λ_i the largest element of $\Lambda^x \setminus (\cup_{x' \ne x} \Lambda^{x'})$, we have that ν_i is smaller than the minimum in (4), whereas for λ_i the largest element of $\Lambda^x \cap \Lambda^{x-1}$, we have ν_i smaller than the minimum in (2). Thus, for $\lambda_i \in \Lambda^x \setminus (\cup_{x' \ne x} \Lambda^{x'})$ but λ_i not the largest element of $\Lambda^x \setminus (\cup_{x' \ne x} \Lambda^{x'})$ and also for λ_i the largest value of $\Lambda^x \cap \Lambda^{x-1}$

$$\min\{\nu_j : j > i\} = \min\{\nu_j : j > i, \lambda_j \in \Lambda^x \setminus (\cup_{x' \ne x} \Lambda^{x'})\}.$$

Similarly, for $\lambda_i \in \Lambda^x \cap \Lambda^{x+1}$, but λ_i not the largest element of $\Lambda^x \cap \Lambda^{x+1}$, and also for λ_i the largest value of $\Lambda^x \setminus (\cup_{x' \ne x} \Lambda^{x'})$

$$\min\{\nu_j : j > i\} = \min\{\nu_j : j > i, \lambda_j \in \Lambda^x \cap \Lambda^{x+1}\}.$$

With these results it is easy to prove the following theorem, which was already proved in [2, pp. 932–933]. We leave the details for the reader.

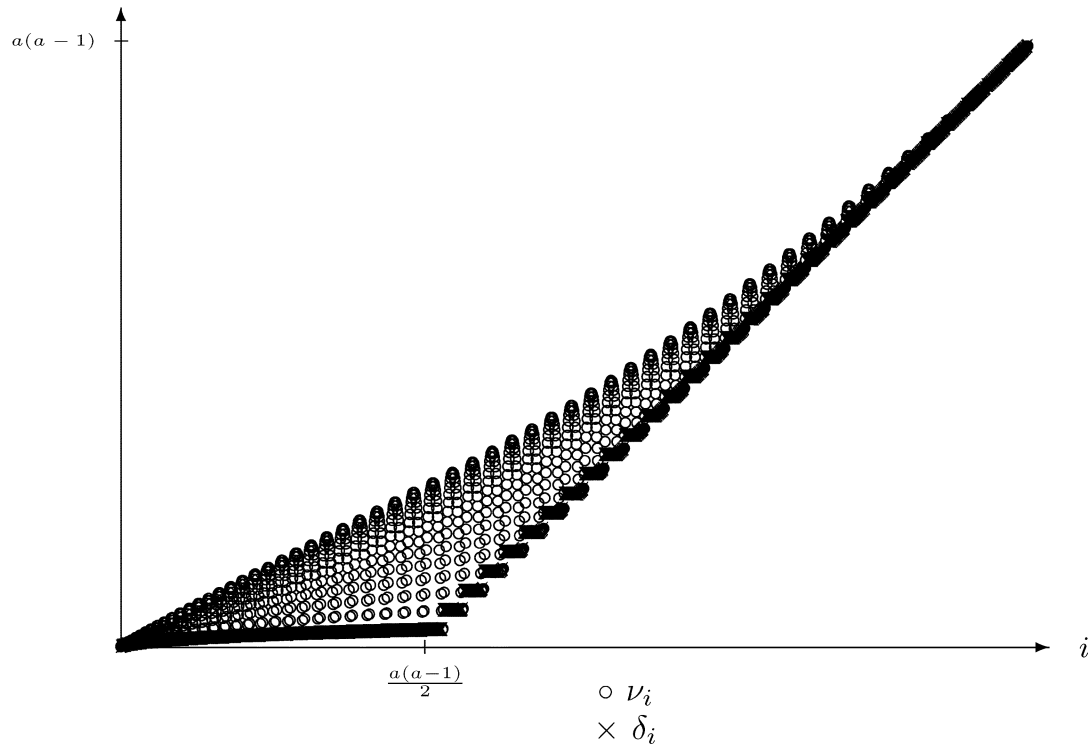

Fig. 5. Graph of ν_i and δ_i for the Hermitian code over $\mathbb{F}_{32^2}$.

Theorem 2.4: Let $\lambda_i \in \Lambda$ and suppose that the Euclidean division of λ_i by a has quotient x and remainder y. Then

$$\delta_i = \begin{cases} x+1, & \text{if } x < a \text{ and } y \neq x \\ x+2, & \text{if } x < a \text{ and } y = x \\ a(x-a+2), & \text{if } x \geq a \text{ and } -a+x \leq y < a-1 \\ \lambda_i - c + 2, & \text{otherwise.} \end{cases}$$

The graphics in Figs. 2–5 show the first values of ν_i and δ_i for the Hermitian codes over $\mathbb{F}_{4^2}$, $\mathbb{F}_{8^2}$, $\mathbb{F}_{16^2}$, and $\mathbb{F}_{32^2}$, respectively.

In fact, it is proven [11], [2] that for Hermitian codes the order bound on the minimum distance is exactly the real minimum distance of the codes.

III. Minimizing Redundancy

The decoding algorithm commonly used for one-point codes is an adaptation of the Berlekamp–Massey–Sakata algorithm [12] together with the majority voting algorithm of Feng–Rao–Duursma [13], [14], [2]. By analyzing majority voting, one realizes that only some of the parity checks are really necessary to perform correction of a given number of errors. New codes can be defined with just these few checks, yielding larger dimensions while keeping the same correction capability as standard codes [5], [2]. These codes are often called Feng-Rao improved codes. The redundancy of standard one-point codes correcting a given number t of errors is

$$r(t) = \max\{i \in \mathbb{N}_0 : \nu_i < 2t+1\} + 1$$

where the enumeration λ and the sequence ν are derived from the Weierstrass semigroup of the distinguished point. The redundancy of the Feng–Rao improved codes correcting the same number of errors is

$$\tilde{r}(t) = |\{i \in \mathbb{N}_0 : \nu_i < 2t+1\})|.$$

This section is devoted to finding explicit formulae for these redundancies in the case when the associated Weierstrass semigroup is generated by two consecutive integers $a, a+1$. Recall that this is the case of Hermitian codes. In [8, p. 2513], Pellikaan and Torres remarked that the formula for $\tilde{r}$ was not known for Hermitian codes.

Theorem 3.1: Let $a > 1$. Then, we have the first equation shown at the bottom of the following page, where

$$\delta_{xt} = \begin{cases} 1, & \text{if } x = \lfloor\sqrt{x^2+4x-8t}\rfloor \bmod 2 \\ 0, & \text{if } x \neq \lfloor\sqrt{x^2+4x-8t}\rfloor \bmod 2 \end{cases}$$

or, equivalently,

$$\delta_{xt} = x + \lfloor\sqrt{x^2+4x-8t}\rfloor + 1 \bmod 2.$$

Proof: By the arguments in the previous section, the maximum nongap whose ν is bounded by a certain constant must be 1) the last element in a parabola, that is, $ax+x$ for some $x < a$ or $ax+a-1$ for some $x \geq a$; 2) the first element in a parabola for some $x \geq a$, that is, $ax+x-a$; 3) some value in $\Lambda^{x'} \cap \Lambda^{x'+1}$ for some x'. In case 1) and 2), x is the largest integer such that $\Lambda^x \setminus (\cup_{x' \neq x}\Lambda^{x'}) \neq \emptyset$ and such that the minimum ν value in $\Lambda^x \setminus (\cup_{x' \neq x}\Lambda^{x'})$ is at most $2t$. That is, the corresponding parabola is not empty and its minimum value is at most $2t$. In case 3), if the largest integer x such that $\Lambda^x \setminus (\cup_{x' \neq x}\Lambda^{x'}) \neq \emptyset$ and such that the minimum ν value in $\Lambda^x \setminus (\cup_{x' \neq x}\Lambda^{x'})$ is at most $2t$, satisfies $x < 2a-1$, then $x' = x$. Otherwise, $x' \geq x$.

By formulas (1) and (2), the set of all minimum ν values among all nonempty parabolas is

$$\begin{aligned} M &= \{\min\{\nu_i : \lambda_i \in \Lambda^{x'} \setminus (\cup_{x'' \neq x'}\Lambda^{x''})\} : \\ &\quad \Lambda^{x'} \setminus (\cup_{x'' \neq x'}\Lambda^{x''}) \neq \emptyset\} \\ &= \{x'+1 : 0 \leq x' \leq a-1\} \\ &\quad \cup \{(a+1)x' - a^2 + 1 : a \leq x' < 2a\} \\ &= \{z : 1 \leq z \leq a\} \cup \{z(a+1) : 1 \leq z \leq a\}. \end{aligned}$$

Now, the maximum among these values, which is at most $2t$, is

$$\max\{m \in M : m \le 2t\} = \begin{cases} 2t, & \text{if } 2t \le a \\ \lfloor \frac{2t}{a+1} \rfloor (a+1), & \text{if } a+1 \le 2t \le a(a+1) \\ a(a+1), & \text{if } 2t > a(a+1). \end{cases}$$

Therefore

$$x = \begin{cases} 2t-1, & \text{if } 2t \le a \\ \lfloor \frac{2t}{a+1} \rfloor + a - 1, & \text{if } a+1 \le 2t \le a(a+1) \\ 2a-1 & \text{if } 2t > a(a+1). \end{cases}$$

If $2t \le a$ then $\Lambda^x \cap \Lambda^{x+1} = \emptyset$ and we are in case 1). Otherwise, if $2t > a$ then $\Lambda^x \cap \Lambda^{x+1} \ne \emptyset$. If $2t < a(x-a+2)$, by formulas (2) and (3), then we are in case 2). Otherwise, we will be either in case 1) or 3). Consequently, we have the second equation shown at the bottom of the page.

Replacing x by its value and taking into consideration that the value ν_i increases constantly by one within $\{\lambda_i \in \cup_{x'>x} \Lambda^{x'} : \nu_i \le 2t\}$, we obtain

$$r(t) = \begin{cases} t(2t+1), & \text{if } t \le a/2 \\ (a^2-a)/2 + (a+1)\lfloor \frac{2t}{a+1} \rfloor, & \text{if } a/2 < t < a(\lfloor \frac{2t}{a+1} \rfloor + 1)/2 \\ (a^2-a)/2 + 2t, & \text{if } t \ge a(\lfloor \frac{2t}{a+1} \rfloor + 1)/2. \end{cases}$$

For the result on $\tilde{r}(t)$ recall that the parabola $(x-y+1)(y+1)$ gives the values of ν_i for the nongaps $\lambda_i = ax+y$ with $x-a \le y \le a-1$. Fixed x, the maximum on y of $(x-y+1)(y+1)$ is attained at $y = x/2$ and it is equal to $x^2/4+x+1$. From the values λ_i with $i < r(t)$ we want to take away all those values whose corresponding ν_i is larger than $2t$. Our first aim is to identify which parabolas have nonempty intersection with the line at height $2t+1$. That is, $x^2/4 + x + 1 \ge 2t+1$. Those are exactly the parabolas for which $x \ge \lceil 2\sqrt{2t+1} - 2 \rceil$.

Now, from each parabola we need to know which is the number of integers y for which the ν_i corresponding to $\lambda_i = ax+y$ is at least $2t+1$. Since the parabola $(x-y+1)(y+1)$ is symmetric with respect to $y = x/2$, there will be an odd number of such integers if x is even and an even number if x is odd. The real values y where the parabola equals $2t+1$ are given by the equation $-y^2+xy+x+1 = 2t+1$, and are exactly $\frac{x \pm \sqrt{x^2+4x-8t}}{2}$. Thus, the length of the real interval where the parabola is at least $2t+1$ is $\sqrt{x^2+4x-8t}$. Now, from this interval we only want its integer values. It is easy to check that the number of such integers is $\lfloor \sqrt{x^2+4x-8t} \rfloor + \delta_{xt}$. □

IV. Minimizing Redundancy for Correcting Generic Errors

In [15]another improvement on one-point codes is described. Under the Berlekamp–Massey–Sakata algorithm with majority voting, an error vector whose weight is larger than half the minimum distance of the code is often correctable. In particular this occurs for *generic errors* (also called independent errors in [16], [17]), whose technical algebraic definition can be found in [18]. Generic errors of weight t can be a very large proportion of all possible errors of weight t [19], [15]. This suggests that a code be designed to correct only *generic errors* of weight t rather than all error words of weight t. Using this restriction, one obtains new codes with much larger dimension than that of standard one-point codes correcting the same number of errors. In [18], the redundancy of standard one-point codes correcting all generic errors of weight up to t is shown to be

$$r^*(t) = \lambda^{-1}(\max(\Lambda \setminus \{\lambda_i + \lambda_j : i, j \ge t\}) + 1.$$

However, taking full advantage of the Feng and Rao improvements due to the majority voting step [5], one can get optimal codes correcting all generic errors of weight up to t with redundancy

$$\tilde{r}^*(t) = |\Lambda \setminus \{\lambda_i + \lambda_j : i, j \ge t\}|.$$

For the details of these two formulas see [18].

This section is devoted to finding explicit formulae for these redundancies.

It is easy to check that if t is such that λ_t is larger than or equal to the conductor then both $r^*(t)$ and $\tilde{r}^*(t)$ are equal to $\lambda_t + t$. If c is the conductor and g is the genus, $\lambda_t \ge c$ is equivalent to $t \ge c - g$. More specifically, for the semigroup generated by $a, a+1$ this is equivalent to $t \in \Lambda^x$ for $x \ge a-1$. In the next theorem we deal with the case when t is strictly less than the conductor, that is, when $t \in \Lambda^x$ with $x < a-1$.

$$r(t) = \begin{cases} t(2t+1), & \text{if } t \le a/2 \\ (a^2-a)/2 + (a+1)\lfloor \frac{2t}{a+1} \rfloor, & \text{if } a/2 < t < a(\lfloor \frac{2t}{a+1} \rfloor + 1)/2 \\ (a^2-a)/2 + 2t, & \text{if } t \ge a(\lfloor \frac{2t}{a+1} \rfloor + 1)/2. \end{cases}$$

$$\tilde{r}(t) = \begin{cases} t(2t+1) - \sum_{x'=\lceil 2\sqrt{2t+1}-2 \rceil}^{2t-1} (\lfloor \sqrt{x'^2+4x'-8t} \rfloor + \delta_{x't}), & \text{if } t \le a/2 \\ (a^2-a)/2 + (a+1)\lfloor \frac{2t}{a+1} \rfloor & \\ - \sum_{x'=\lceil 2\sqrt{2t+1}-2 \rceil}^{a-2+\lfloor \frac{2t}{a+1} \rfloor} (\lfloor \sqrt{x'^2+4x'-8t} \rfloor + \delta_{x't}), & \text{if } a/2 < t < a(\lfloor \frac{2t}{a+1} \rfloor + 1)/2 \\ (a^2-a)/2 + 2t - \sum_{x'=\lceil 2\sqrt{2t+1}-2 \rceil}^{a-1+\lfloor \frac{2t}{a+1} \rfloor} (\lfloor \sqrt{x'^2+4x'-8t} \rfloor + \delta_{x't}), & \text{if } a(\lfloor \frac{2t}{a+1} \rfloor + 1)/2 \le t \le \frac{a(a+1)}{2} \\ (a^2-a)/2 + 2t, & \text{if } t > \frac{a(a+1)}{2} \end{cases}$$

$$r(t) = \begin{cases} \lambda^{-1}(ax+x)+1, & \text{if } 2t \le a \\ \lambda^{-1}(ax+x-a)+1, & \text{if } a < 2t < a(x-a+2) \\ \lambda^{-1}(ax+a-1)+1+ \mid \{\lambda_i \in \cup_{x'>x} \Lambda^{x'} : \nu_i \le 2t\} \mid, & \text{if } 2t \ge a(x-a+2). \end{cases}$$

Theorem 4.1: Suppose $t = \frac{x(x+1)}{2} + y$ with $0 \leq y \leq x < a-1$. That is, $\lambda_t = xa + y$ with $0 \leq y \leq x < a-1$. Then

$$r^*(t) = \begin{cases} 2x^2 + x & \text{if } 2x < a, y = 0, \\ 2x^2 + 3x + y + 1 & \text{if } 2x < a, y > 0, \\ 2xa + y - \frac{a^2-3a}{2} & \text{if } 2x \geq a, y > 2x - a + 1, \\ 2xa + 2y - \frac{a^2-a}{2} & \text{if } 2x \geq a, y \leq 2x - a + 1. \end{cases}$$

$$\tilde{r}^*(t) = \begin{cases} 2x^2 + x + 3y & \text{if } 2x < a, \\ 2xa + 3y - 2x - \frac{a^2-3a}{2} - 1 & \text{if } 2x \geq a, y > 2x - a + 1, \\ 2xa + 2y - \frac{a^2-a}{2} & \text{if } 2x \geq a, y \leq 2x - a + 1. \end{cases}$$

Proof: We have

$$\{\lambda_i + \lambda_j : i, j \geq t\} = \{l \in \Lambda^{2x} : l \geq 2xa + 2y\} \cup \{l \in \Lambda^{2x+1} : l \geq (2x+1)a + y\} \cup (\cup_{x' \geq 2x+2} \Lambda^{x'}).$$

Notice that $\{l \in \Lambda^{2x+1} : l < (2x+1)a + y\} \cap \Lambda^{2x+2} = \emptyset$ because $y < a$. So,

$$\Lambda \setminus \{\lambda_i + \lambda_j : i, j \geq t\} = \{l \in \Lambda : l < 2xa + 2y\} \sqcup (\{l \in \Lambda^{2x+1} : l < (2x+1)a + y\} \setminus \Lambda^{2x}).$$

Let

$$A = \{l \in \Lambda : l < 2xa + 2y\},$$
$$B = \{l \in \Lambda^{2x+1} : l < (2x+1)a + y\} \setminus \Lambda^{2x}.$$

If $2x < a$ then $|A| = \frac{2x(2x+1)}{2} + 2y$ and $|B| = y$ because $\Lambda^{2x} \cap \Lambda^{2x+1} = \emptyset$. So,

$$\begin{aligned} \tilde{r}^*(t) &= |\Lambda \setminus \{\lambda_i + \lambda_j : i, j \geq t\}| \\ &= |A| + |B| \\ &= 2x^2 + x + 3y, \end{aligned}$$

$$r^*(t) = \begin{cases} \frac{2x(2x+1)}{2} = 2x^2 + x & \text{if } y = 0, \\ \frac{(2x+1)(2x+2)}{2} + y = 2x^2 + 3x + y + 1 & \text{if } y > 0. \end{cases}$$

If $2x \geq a$, then all elements in Λ^{2x} are larger than the conductor and $|A| = 2xa + 2y - g = 2xa + 2y - \frac{a^2-a}{2}$. In order to compute $|B|$, notice that $|\{l \in \Lambda^{2x+1} : l < (2x+1)a + y\}| = y$, while $|\Lambda^{2x} \cap \Lambda^{2x+1}| = 2x - a + 1$. Now, if $y > 2x - a + 1$, then $\Lambda^{2x} \cap \Lambda^{2x+1} \subseteq \{l \in \Lambda^{2x+1} : l < (2x+1)a + y\}$, so $|B| = y - 2x + a - 1$ and

$$\tilde{r}^*(t) = |A| + |B| = 2xa + 3y - 2x - \frac{a^2 - 3a}{2} - 1$$
$$r^*(t) = 2xa + y - \frac{a^2 - 3a}{2}.$$

Otherwise, if $y \leq 2x - a + 1$, then $\Lambda^{2x} \cap \Lambda^{2x+1} \supseteq \{l \in \Lambda^{2x+1} : l < (2x+1)a + y\}$, so $|B| = 0$ and

$$\tilde{r}^*(t) = |A| = 2xa + 2y - \frac{a^2 - a}{2}$$
$$r^*(t) = |A| = 2xa + 2y - \frac{a^2 - a}{2}.$$

□

ACKNOWLEDGMENT

The authors would like to express their appreciation for the editor's clear, thoughtful, and timely communication regarding revision of this correspondence.

REFERENCES

[1] G. L. Feng and T. R. N. Rao, "A simple approach for construction of algebraic-geometric codes from affine plane curves," *IEEE Trans. Inf. Theory*, vol. 40, pp. 1003–1012, 1994.

[2] T. Høholdt, J. H. van Lint, and R. Pellikaan, "Algebraic geometry codes," in *Handbook of Coding Theory*, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam: North-Holland, 1998, vol. I, pp. 871–961.

[3] C. Kirfel and R. Pellikaan, "The minimum distance of codes in an array coming from telescopic semigroups," Special issue on algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 41, pt. 1, pp. 1720–1732, 1995.

[4] A. Campillo and J. I. Farrán, "Computing Weierstrass semigroups and the Feng-Rao distance from singular plane models," *Finite Fields Appl.*, vol. 6, no. 1, pp. 71–92, 2000.

[5] G.-L. Feng and T. R. N. Rao, "Improved geometric Goppa codes. I. basic theory," Special issue on algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 41, pt. 1, pp. 1678–1693, 1995.

[6] H. Stichtenoth, "A note on Hermitian codes over $\mathrm{GF}(q^2)$," Coding techniques and coding theory," *IEEE Trans. Inf. Theory*, vol. 34, pt. 2, pp. 1345–1348, 1988.

[7] O. Geil, "On codes from norm-trace curves," *Finite Fields Appl.*, vol. 9, no. 3, pp. 351–371, 2003.

[8] R. Pellikaan and F. Torres, "On Weierstrass semigroups and the redundancy of improved geometric Goppa codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2512–2519, 1999.

[9] P. A. García-Sánchez and J. C. Rosales, "Numerical semigroups generated by intervals," *Pacific J. Math.*, vol. 191, no. 1, pp. 75–83, 1999.

[10] C. Munuera and D. Ramirez, "The second and third generalized Hamming weights of Hermitian codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 709–712, 1999.

[11] K. Yang and P. V. Kumar, "On the true minimum distance of Hermitian codes," in *Coding Theory and Algebraic Geometry (Luminy, 1991)*. Berlin, Germany: Springer, 1992, vol. 1518, Lecture Notes in Math., pp. 99–107.

[12] S. Sakata, "Extension of the Berlekamp-Massey algorithm to N dimensions," *Inf. Comput.*, vol. 84, no. 2, pp. 207–239, 1990.

[13] G. L. Feng and T. R. N. Rao, "Decoding algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inf. Theory*, vol. 39, pp. 37–45, 1993.

[14] I. M. Duursma, "Majority coset decoding," *IEEE Trans. Inf. Theory*, vol. 39, pp. 1067–1070, 1993.

[15] M. E. O'Sullivan, "Decoding of Hermitian codes beyond $(d_{min} - 1)/2$," in *Proc. IEEE Int. Symp. Inf. Theory*, Ulm, Germany, 1997, p. 384.

[16] R. Pellikaan, "On decoding by error location and dependent sets of error positions," A collection of contributions in honor of Jack van Lint," *Discrete Math.*, vol. 106/107, pp. 369–381, 1992.

[17] H. E. Jensen, R. R. Nielsen, and T. Høholdt, "Performance analysis of a decoding algorithm for algebraic-geometry codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1712–1717, 1999.

[18] M. Bras-Amorós and M. E. O'Sullivan, "The correction capability of the Berlekamp-Massey-Sakata algorithm with majority voting," *Applicable Algebra in Eng., Commun. Comput.*, vol. 17, no. 5, pp. 315–335, 2006.

[19] J. P. Hansen, "Dependent rational points on curves over finite fields—Lefschetz theorems and exponential sums," in *Int. Workshop on Coding and Cryptography (Paris, 2001)*, Amsterdam, 2001, vol. 6, Electron. Notes Discrete Math., pp. 297–309.