[14] D. C. Youla and N. N. Kazanjian, "Bauer-type factorization of positive matrices and the theory of matrix polynomials orthogonal on the unit circle," *IEEE Trans. Circuits Syst.*, vol. CAS-25, no. 2, pp. 57–69, Feb. 1978.
[15] A. H. Sayed and T. Kailath, "A survey of spectral factorization methods," *Numer. Linear Algebra Appl.*, vol. 8, pp. 467–496, 2001.
[16] B. Dumitrescu, *Positive Trigonometric Polynomials and Signal Processing Applications.*. Dordrecht, The Netherlands: Springer, 2007.
[17] H. Boche and V. Pohl, "BIBO norm in spectral factorization and wiener filtering," in *Proc. 9th Canadian Workshop Inform. Theory (CWIT)*, Montréal, Canada, June 2005, pp. 347–350.
[18] S. U. Pillai and T. I. Shim, *Spectrum Estimation and System Identification.*. New York: Springer-Verlag, 1993, etc..
[19] S. Barry, Orthogonal Polynomials on the Unit Circle. 2005, Providence, RI, American Math. Soc.
[20] J. B. Garnett and D. E. Marshall, . Cambridge, U.K.: Cambridge University Press, 2005.
[21] A. Zygmund, *Trigonometric Series.*. Cambridge, U.K.: Cambridge: University Press, 1968.
[22] S. Treil, "A counterexample on continuous coprime factors," *IEEE Trans. Automat. Contr.*, vol. 39, no. 6, pp. 1262–1263, June 1994.
[23] H. Boche and V. Pohl, "Spectral factorization in the disk algebra," *Complex Var. Theory Appl.*, vol. 50, no. 6, pp. 383–387, May 2005.
[24] H. Boche and V. Pohl, "There exists no always convergent algorithm for the calculation of spectral factorization, Wiener filter, and Hilbert transform," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, WA, USA, Jul. 2006, pp. 118–122.

The Order Bound on the Minimum Distance of the One-Point Codes Associated to the Garcia–Stichtenoth Tower

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

***Abstract*—Garcia and Stichtenoth discovered a tower of function fields that meets the Drinfeld–Vlăduţ bound on the ratio of the number of points to the genus. For this tower, Pellikaan, Stichtenoth, and Torres derived a recursive description of the Weierstrass semigroups associated to a tower of points on the associated curves. In this correspondence, a nonrecursive description of the semigroups is given and from this the enumeration of each of the semigroups is derived as well as its inverse. This enables us to find an explicit formula for the order (Feng–Rao) bound on the minimum distance of the associated one-point codes.**

***Index Terms*—Garcia–Stichtenoth tower, numerical semigroup.**

I. Introduction

Let $\mathbb{N}_0$ denote the set of all nonnegative integers. A *numerical semigroup* is a subset Λ of $\mathbb{N}_0$ containing 0, closed under summation and with finite complement in $\mathbb{N}_0$. The *enumeration* of Λ is the unique increasing bijective map $\lambda : \mathbb{N}_0 \longrightarrow \Lambda$. Usually, λ_i is used instead of $\lambda(i)$. Given a numerical semigroup Λ with enumeration λ define the sequence ν_i by

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

This sequence is important in the theory of one-point algebraic-geometry codes. For a sequence of one-point codes on a curve, where the one point is P, the *Weierstrass semigroup* of P is the numerical semigroup consisting of the pole orders at P of functions having poles only at P. The sequence ν_i for the Weierstrass semigroup 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 [1]–[3]. In particular, the order bound may be compared with the Goppa bound $i - g + 2$, where g is the genus of the curve or, equivalently, the number of gaps of its Weierstrass semigroup. It is proved in [2, Th. 3.8, Corollary 3.9] and [3, Th. 5.24] that the order bound is always at least as large as the Goppa bound and that the two bounds agree beyond a certain point. One can also prove that the unique numerical semigroup for which they coincide in each value is $\mathbb{N}_0$ and so, for any nontrivial sequence of algebraic-geometry codes the order bound is strictly better than the Goppa bound.

Garcia and Stichtenoth first gave in [4] a tower of function fields attaining the Drinfeld–Vlăduţ bound, which became important in the area of algebraic coding theory. This tower is defined over the finite field with q^2 elements $\mathbb{F}_{q^2}$ for q a prime power. It is given by

- $\mathcal{F}^{(1)} = \mathcal{F}_{q^2}(x_1)$;
- $\mathcal{F}^{(m)} = \mathcal{F}^{(m-1)}(x_m)$ with x_m satisfying

$$x_m^q + x_m = \frac{x_{m-1}^q}{x_{m-1}^{q-1} + 1}.$$

It is shown in [4] that the number of its rational points is $N_{q^2}(\mathcal{F}^{(m)}) \geqslant (q^2 - q)q^{m-1}$ and that the genus g_m of $\mathcal{F}^{(m)}$ satisfies $g_m = (q^{\lfloor \frac{m+1}{2} \rfloor} - 1)(q^{\lceil \frac{m-1}{2} \rceil} - 1)$. Hence, the ratio between the genus $g(\mathcal{F}^{(m)})$ and $N_{q^2}(\mathcal{F}^{(m)})$ converges to $1/(q-1)$, the Drinfeld–Vlăduţ bound, as m increases. From these curves one can construct asymptotically good sequences of codes.

For every function field $\mathcal{F}^{(m)}$ in the tower we distinguish the rational point $Q^{(m)}$ that is the unique pole of x_1. The Weierstrass semigroup $\Lambda^{(m)}$ at $Q^{(m)}$ in $\mathcal{F}^{(m)}$ was recursively described in [5]. Indeed, the semigroups are given by

$$\Lambda^{(1)} = \mathbb{N}_0$$
$$\Lambda^{(m)} = q \cdot \Lambda^{(m-1)} \cup \left\{ i \in \mathbb{N}_0 : i \geqslant q^m - q^{\lfloor \frac{m+1}{2} \rfloor} \right\}. \quad (1)$$

In [6], there is a description of the parameters of improved algebraic-geometry codes when the associated numerical semigroup is an inductive numerical semigroup, which is the case for the semigroups in (1). Although these Weierstrass semigroups have been known for a long time, no explicit description of the order bound on the minimum distance for the associated one-point codes has appeared in the literature. Chen found certain bounds on the order bound for a given range and this enabled him to prove that some codes had distance larger than the order bound [7]. The main goal of this correspondence is to find the explicit description of the order bound from a deep analysis of the semigroups in (1).

In Section II, we give a nonrecursive description of these semigroups. This description leads to explicit formulation of their enumerations as well as for the inverses of their enumerations. This is

Manuscript received November 24, 2006; revised June 14, 2007. The work of M. Bras-Amorós was supported by the Catalan Government under Grant BE-2 2006.

M. Bras-Amorós is with the Escola Tècnica Superior d'Enginyeria, Department d'Enginyeria Informàtica i Matemàtiques, Universitat Rovira i Virgili, 43007 Tarragona, Catalonia, Spain (e-mail: maria.bras@urv.cat).

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.2007.907522

presented in Section III. In Section IV we find the explicit formula for the order bound on the minimum distance of the one-point codes associated to the tower of function fields. We finally show in Figs. 7–10, that the order bound is significantly larger than the Goppa bound for these codes before they start coinciding.

II. Nonrecursive Description of the Semigroups

In this section, we will give a nonrecursive description of the semigroups (1). The *conductor* of a numerical semigroup Λ is the unique integer c such that $c-1 \notin \Lambda$ and $c+\mathbb{N}_0 \subseteq \Lambda$. The *gaps* of Λ are the elements in $\mathbb{N}_0 \setminus \Lambda$ and the *nongaps* are the elements in Λ.

From now on we will use c_m for the conductor of $\Lambda^{(m)}$, which is $q^m - q^{\lfloor \frac{m+1}{2} \rfloor}$, and $A_i = \{c_{2i-1}+j : j = 0, \ldots, q^{i-1}(q-1)-1\} = \{j \in \mathbb{N}_0 : q^{2i-1} - q^i \leqslant j \leqslant q^{2i-1} - q^{i-1} - 1\}$. Notice that these are not recursive definitions.

Theorem 1:

$$\Lambda^{(m)} = \bigsqcup_{i=1}^{\lfloor \frac{m}{2} \rfloor} q^{m-2i+1} A_i \sqcup \{j \in \mathbb{N}_0 : j \geq c_m\}.$$

Proof: We will proceed by induction. The case $m = 1$ is obvious. Suppose $m > 1$. If m is even, say $m = 2n$, then

$$\Lambda^{(2n)} = q\Lambda^{(2n-1)} \cup \{i \in \mathbb{N}_0 : i \geq c_{2n}\}.$$

By the induction hypothesis, since $c_{2n-1} = q^{2n-1} - q^n$ and $c_{2n} = q^{2n} - q^n$

$$\begin{aligned}
\Lambda^{(2n)} &= \cup_{i=1}^{n-1} q^{2n-2i+1} A_i \cup q\{j \in \mathbb{N}_0 : j \geq q^{2n-1} - q^n\} \\
&\quad \cup \{j \in \mathbb{N}_0 : j \geq q^{2n} - q^n\} \\
&= \cup_{i=1}^{n-1} q^{2n-2i+1} A_i \\
&\quad \cup q\{j \in \mathbb{N}_0 : q^{2n-1} - q^n \leq j \leq q^{2n-1} - q^{n-1} - 1\} \\
&\quad \cup \{j \in \mathbb{N}_0 : j \geq q^{2n} - q^n\} \\
&= \cup_{i=1}^{n} q^{2n-2i+1} A_i \cup \{j \in \mathbb{N}_0 : j \geq q^{2n} - q^n\} \\
&= \cup_{i=1}^{\lfloor \frac{(2n)}{2} \rfloor} q^{(2n)-2i+1} A_i \cup \{j \in \mathbb{N}_0 : j \geq c_{2n}\}.
\end{aligned}$$

If m is odd, say $m = 2n+1$, then

$$\Lambda^{(2n+1)} = q\Lambda^{(2n)} \cup \{i \in \mathbb{N}_0 : i \geq c_{2n+1}\}.$$

By the induction hypothesis, since $c_{2n} = q^{2n} - q^n$ and $c_{2n+1} = q^{2n+1} - q^{n+1}$

$$\begin{aligned}
\Lambda^{(2n+1)} &= \cup_{i=1}^{n} q^{2n-2i+2} A_i \cup q\{j \in \mathbb{N}_0 : j \geq q^{2n} - q^n\} \\
&\quad \cup \{j \in \mathbb{N}_0 : j \geq q^{2n+1} - q^{n+1}\} \\
&= \cup_{i=1}^{n} q^{2n-2i+2} A_i \cup \{j \in \mathbb{N}_0 : j \geq q^{2n+1} - q^{n+1}\} \\
&= \cup_{i=1}^{\lfloor \frac{(2n+1)}{2} \rfloor} q^{(2n+1)-2i+1} A_i \cup \{j \in \mathbb{N}_0 : j \geq c_{2n+1}\}.
\end{aligned}$$

It remains to see that the unions are disjoint. Let us first see that the sets $q^{m-2i+1}A_i$ are pairwise disjoint. Indeed

$$\begin{aligned}
\max(q^{m-2i+1}A_i) &= q^{m-2i+1}(q^{2i-1} - q^{i-1} - 1) \\
&= q^m - q^{m-i} - q^{m-2i+1}.
\end{aligned}$$

On the other hand

$$\min(q^{m-2(i+1)+1}A_{i+1}) = q^{m-2i-1}(q^{2i+1} - q^{i+1}) = q^m - q^{m-i}.$$

This proves that the sets $q^{m-(2i-1)}A_i$ are pairwise disjoint.

Now, the maximum attained by these sets is $q^m - q^{m-\lfloor \frac{m}{2} \rfloor} - q^{m-2\lfloor \frac{m}{2} \rfloor + 1}$. If m is even then this equals $q^m - q^{\frac{m}{2}} - q = c_m - q$ while if m is odd then this equals $q^m - q^{\frac{m+1}{2}} - q^2 = c_m - q^2$. □

III. Enumeration of the Semigroups

In this section, we use the notations and results in Theorem 1 to find an explicit formula for the enumeration of the semigroups in (1) as well as a formula for its inverse.

Theorem 2: Let λ be the enumeration of $\Lambda^{(m)}$.

1) The conductor c_m is the image by λ of $q^{\lfloor \frac{m}{2} \rfloor} - 1$. That is, $c_m = \lambda_{q^{\lfloor \frac{m}{2} \rfloor} - 1}$.
2) If $t \geq q^{\lfloor \frac{m}{2} \rfloor} - 1$, then $\lambda_t = (q^{\lfloor \frac{m+1}{2} \rfloor} - 1)(q^{\lceil \frac{m-1}{2} \rceil} - 1) + t$.
3) If $0 \leq t < q^{\lfloor \frac{m}{2} \rfloor} - 1$, then $\lambda_t = q^{m-2l-1}(q^{2l+1} - q^{l+1} - q^l + t + 1)$, where $l = \lfloor \log_q(t+1) \rfloor$.

Proof:

1) For any positive integer i it holds $|A_i| = q^{i-1}(q-1)$ and, hence

$$\begin{aligned}
&\left| \bigsqcup_{i=1}^{\lfloor \frac{m}{2} \rfloor} q^{m-2i+1} A_i \right| \\
&= (1 + q + q^2 + \cdot + q^{\lfloor \frac{m}{2} \rfloor - 1})(q-1) \\
&= q^{\lfloor \frac{m}{2} \rfloor} - 1.
\end{aligned}$$

   Since c_m is the first nongap which is not in $\bigsqcup_{i=1}^{\lfloor \frac{m}{2} \rfloor} q^{m-2i+1}A_i$, $c_m = \lambda_{q^{\lfloor \frac{m}{2} \rfloor} - 1}$.
2) If $t \geq q^{\lfloor \frac{m}{2} \rfloor} - 1$, then λ_t is at least the conductor and in this case we know that $\lambda_t = t + g_m = t + (q^{\lfloor \frac{m+1}{2} \rfloor} - 1)(q^{\lceil \frac{m-1}{2} \rceil} - 1)$.
3) If $t < q^{\lfloor \frac{m}{2} \rfloor} - 1$, then the lemma below shows that $t+1$ may be uniquely expressed as $t + 1 = q^l + j$ where $l = \lfloor \log_q(t+1) \rfloor < \lfloor m/2 \rfloor$ and $0 \leq j \leq q^l(q-1) - 1$. Since $|\bigsqcup_{k=1}^{l} q^{m-2k+1}A_k| = q^l - 1$, we have $\lambda_{q^l - 1}$ is the first nongap which is not in $\bigsqcup_{k=1}^{l} q^{m-2k+1}A_k$, namely $q^{m-2l-1}c_{2l+1}$. The next nongaps after $q^{m-2l-1}c_{2l+1}$ are $q^{m-2l-1}(c_{2l+1} + i)$ with $i = 1, \ldots, q^l(q-1)-1$. Therefore, $\lambda_t = q^{m-2l-1}(c_{2l+1}+j) = q^{m-2l-1}(c_{2l+1}+t+1-q^l) = q^{m-2l-1}(q^{2l+1} - q^{l+1} - q^l + t + 1)$. □

Lemma 3: Any integer $x \geq 1$ may be uniquely expressed in the form

$$x = q^e + r$$

for $0 \leq e$ and $0 \leq r < q^e(q-1)$. Furthermore, $e = \lfloor \log_q(x) \rfloor$ and $r = x - q^e$.

Proof: Observe that

$$\begin{aligned}
e = \lfloor \log_q(x) \rfloor &\iff q^e \leq x < q^{e+1} \\
&\iff 0 \leq x - q^e < q^e(q-1)
\end{aligned}$$

Setting $r = x - q^e$ shows that x may be expressed as claimed, and that the choice of e and r are unique. □

We want to find now a formula for the inverse of the enumeration of a numerical semigroup. Given an integer k and a numerical semigroup Λ we define the *semigroup floor* of k with respect to Λ as the largest element in Λ which is not larger than k. It is denoted $\lfloor k \rfloor_\Lambda$. In the next theorem we describe a formula not only to find the inverse of the enumeration of a numerical semigroup, but also to find the index for the semigroup floor of any integer.

Theorem 4: Let λ be the enumeration of $\Lambda^{(m)}$ and let $k \geq 0$ be an integer. Let c_i and g_i be, respectively, the conductor and the genus

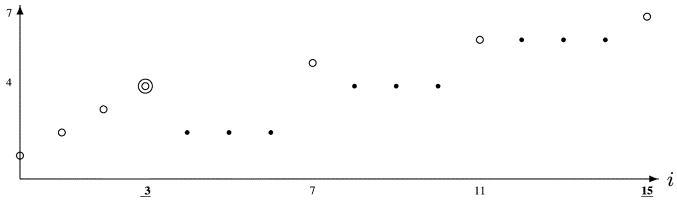

Fig. 1. $\nu^{(2)}$-sequence for $q = 4$. The conductor is $c_2 = \lambda_3^{(2)} = 12$.

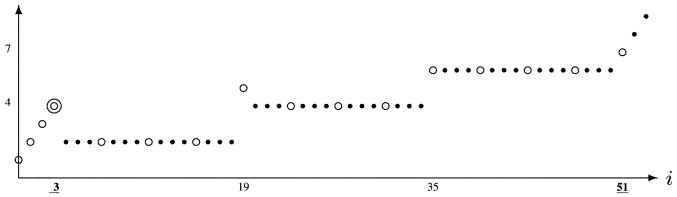

Fig. 2. $\nu^{(3)}$-sequence for $q = 4$. The conductor is $c_3 = \lambda_3^{(3)} = 48$.

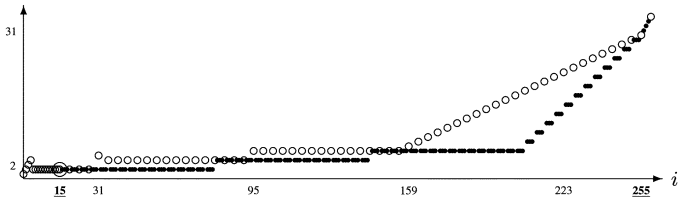

Fig. 3. $\nu^{(4)}$-sequence for $q = 4$. The conductor is $c_4 = \lambda_{15}^{(4)} = 240$.

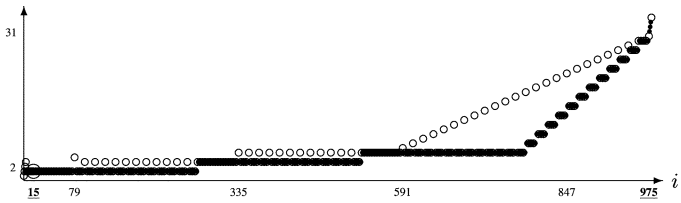

Fig. 4. $\nu^{(5)}$-sequence for $q = 4$. The conductor is $c_5 = \lambda_{15}^{(5)} = 960$.

of $\Lambda^{(i)}$. Then, see the first equation at the bottom of the page, where $l = m + 1 - \lceil \log_q(q^m - k) \rceil$.

Proof: The result for the case when $k \geq c_m$ is obvious. Suppose $k < c_m$. By Theorem 1, $\lfloor k \rfloor_{\Lambda^{(m)}}$ can be expressed as $q^{m-2l+1}(c_{2l-1} + i)$ with $i = 1, \ldots, q^{i-1}(q-1) - 1$ and with l being the largest integer l with $q^{m-2l+1}c_{2l-1} \leq \lfloor k \rfloor_{\Lambda^{(m)}}$. Notice that it is also the largest integer l with $q^{m-2l+1}c_{2l-1} \leq k$. By substituting c_{2l-1} by $q^{2l-1} - q^l$ one gets $l = m + 1 - \lceil \log_q(q^m - k) \rceil$. By the same arguments as in the proof of Theorem 2. 3), it follows that $\lambda^{-1}(\lfloor k \rfloor_{\Lambda^{(m)}}) = q^{l-1} - 1 + \frac{\lfloor k \rfloor_{\Lambda^{(m)}}}{q^{m-2l+1}} - c_{2l-1}$. Now, $\frac{\lfloor k \rfloor_{\Lambda^{(m)}}}{q^{m-2l+1}} = \lfloor \frac{k}{q^{m-2l+1}} \rfloor$ is a consequence of the fact that $\lfloor k \rfloor_{\Lambda^{(m)}}$ belongs to $q^{m-2l+1}A_l$. Substituting c_{2l-1} by $q^{2l-1} - q^l$ gives the result. □

IV. The Order Bound on the Minimum Distance

From now on, $\lambda^{(m)}$ denotes the enumeration of $\Lambda^{(m)}$, c_m, g_m are the conductor and the genus of $\Lambda^{(m)}$, $\nu_i^{(m)}$ is the ith value of the ν-sequence corresponding to the semigroup $\Lambda^{(m)}$ and $\delta_i^{(m)}$ is the order bound on the minimum distance of the ith one point code associated to $\mathcal{F}^{(m)}$.

Lemma 5: $\nu_i^{(1)} = i + 1$ for all i. If $i > 1$ then, see the second equation at the bottom of the page.

Proof: Notice that $c_m \geq qc_{m-1}$ implies that an element in $\Lambda^{(m)}$ is a multiple of q if and only if it is in $q\Lambda^{(m-1)}$.

The case $i \leq q^{\lfloor \frac{m}{2} \rfloor} - 1$ is equivalent to $\lambda_i^{(m)} \leq c_m$. From the inductive definition of $\Lambda^{(m)}$ it is clear that $\lambda_i^{(m)} = q\lambda_i^{(m-1)}$ and consequently, $\nu_i^{(m)} = \nu_i^{(m-1)}$.

The case $i \geq q^m - q^{\lfloor \frac{m+1}{2} \rfloor} + q^{\lfloor \frac{m}{2} \rfloor} - 1 = 2c_m - g_m$ is equivalent to $\lambda_i^{(m)} \geq 2c_m$. It is well known that for any semigroup Λ with conductor c and genus g the sequence ν satisfies that $\nu_i = i - g + 1$ for all $i \geq 2c - g$.

We are left with the case $c_m \leq \lambda_i^{(m)} < 2c_m$. Suppose $\lambda_i^{(m)} = \lambda_j^{(m)} + \lambda_k^{(m)}$ with $\lambda_j^{(m)} \leq \lambda_k^{(m)}$. Then $\lambda_j^{(m)} < c_m$ so $\lambda_j^{(m)} \in q\Lambda^{(m-1)}$. Now, $q \mid i + 1$ if and only if $q \mid i + g_m = \lambda_i^{(m)}$. If $q \mid \lambda_i^{(m)}$ then also $q \mid \lambda_k^{(m)}$, so $\lambda_k^{(m)} \in q\Lambda^{(m-1)}$. This shows that we have a one-to-one correspondence between $\{j \in \mathbb{N}_0 : \lambda_i^{(m)} - \lambda_j^{(m)} \in \Lambda^{(m)}\}$ and $\{j \in \mathbb{N}_0 : \lambda_{i'}^{(m-1)} - \lambda_j^{(m-1)} \in \Lambda^{(m-1)}\}$, where $q\lambda_{i'}^{(m-1)} = \lambda_i^{(m)}$, that is, $i' = (i + g_m)/q - g_{m-1}$. Thus $\nu_i^{(m)} = \nu_{i'}^{(m-1)}$.

If $q \nmid \lambda_i^{(m)}$ then also $q \nmid \lambda_k^{(m)}$. Consequently, $\lambda_k^{(m)} > c_m$ and $\lambda_j^{(m)} < \lambda_i^{(m)} - c_m$. One can see that each $\lambda_j^{(m)} \in \Lambda^{(m)}$ with $\lambda_j^{(m)} < \lambda_i^{(m)} - c_m$ yields a pair of elements in $\{j \in \mathbb{N}_0 : \lambda_i^{(m)} - \lambda_j^{(m)} \in \Lambda^{(m)}\}$. Thus $\nu_i = 2|\{\alpha \in \Lambda^{(m)} : \alpha < \lambda_i^{(m)} - c_m\}| = 2 + 2(\lambda^{(m)})^{-1}(\lfloor i + g_m - c_m - 1 \rfloor_{\Lambda^{(m)}})$. From Theorem 2, it follows that $c_m - g_m = q^{\lfloor \frac{m}{2} \rfloor} - 1$. Hence, $\nu_i = 2 + 2(\lambda^{(m)})^{-1}(\lfloor i - q^{\lfloor \frac{m}{2} \rfloor} \rfloor_{\Lambda^{(m)}})$. □

In Figs. 1– 6, there are the values of the ν-sequences of $\Lambda^{(2)}$, $\Lambda^{(3)}$, $\Lambda^{(4)}$, $\Lambda^{(5)}$, $\Lambda^{(6)}$ and $\Lambda^{(7)}$ for $q = 4$. We used circles for the ν-values of those indices i such that λ_i is a multiple of q and dots for the remaining values. In the horizontal axis, we wrote the indices i such that the corresponding nongap λ_i is a multiple of q^{m-1}, as well as the index of the conductor and twice the conductor. These last two indices have been underlined.

Lemma 6: The order bound on the minimum distance satisfies the first and the second equations shown at the bottom of the following page.

$$\lambda^{-1}(\lfloor k \rfloor_{\Lambda^{(m)}}) = \begin{cases} k - g_m & \text{if } k \geq c_m \\ q^{l-1}(-q^l + q + 1) + \lfloor \frac{k}{q^{m-2l+1}} \rfloor - 1 & \text{if } k < c_m \end{cases}$$

$$\nu_i^{(m)} = \begin{cases} \nu_i^{(m-1)}, & \text{if } i \leq q^{\lfloor \frac{m}{2} \rfloor} - 1 \\ \nu_{\frac{i+g_m}{q} - g_{m-1}}^{(m-1)}, & \text{if } q^{\lfloor \frac{m}{2} \rfloor} - 1 < i \leq q^m - q^{\lfloor \frac{m+1}{2} \rfloor} + q^{\lfloor \frac{m}{2} \rfloor} - 1 \text{ and } q \mid i + 1 \\ 2 + 2(\lambda^{(m)})^{-1}(\lfloor i - q^{\lfloor \frac{m}{2} \rfloor} \rfloor_{\Lambda^{(m)}}), & \text{if } q^{\lfloor \frac{m}{2} \rfloor} - 1 < i \leq q^m - q^{\lfloor \frac{m+1}{2} \rfloor} + q^{\lfloor \frac{m}{2} \rfloor} - 1 \text{ and } q \nmid i + 1 \\ i - g_m + 1, & \text{otherwise.} \end{cases}$$

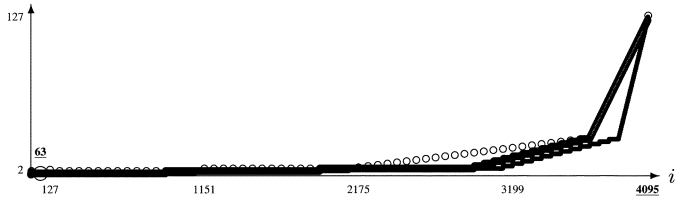

Fig. 5. $\nu^{(6)}$-sequence for $q=4$. The conductor is $c_6=\lambda_{63}^{(6)}=4032$.

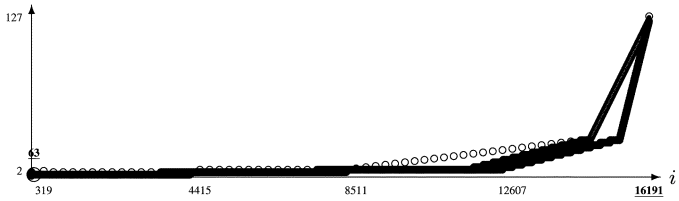

Fig. 6. $\nu^{(7)}$-sequence for $q=4$. The conductor is $c_7=\lambda_{63}^{(7)}=16128$.

Proof: Notice that by Lemma 5, $\nu^{(m)}_{q^{\lfloor \frac{m}{2}\rfloor}}=2$ for all m. Thus, if $i\le q^{\lfloor \frac{m}{2}\rfloor}-1$ then $\delta_i^{(m)}=2$.

By Lemma 5, $\nu^{(m)}$ is increasing in the subset $\{i\in\mathbb{N}_0: q^{\lfloor \frac{m}{2}\rfloor}-1<i\le q^m-q^{\lfloor \frac{m+1}{2}\rfloor}+q^{\lfloor \frac{m}{2}\rfloor}-1, q\nmid i+1\}\cup\{i\in\mathbb{N}_0: i>q^m-q^{\lfloor \frac{m+1}{2}\rfloor}+q^{\lfloor \frac{m}{2}\rfloor}-1\}$. Now it is enough to check that for i such that $q^{\lfloor \frac{m}{2}\rfloor}-1<i\le q^m-q^{\lfloor \frac{m+1}{2}\rfloor}+q^{\lfloor \frac{m}{2}\rfloor}-3$ and $q\mid i+2, \nu^{(m)}_{i+1}\ge\nu^{(m)}_{i+2}$. To see this we will show that $\{(j,k)\in\mathbb{N}_0\times\mathbb{N}_0, j\le k:\lambda_j^{(m)}+\lambda_k^{(m)}=\lambda_{i+2}^{(m)}\}\subseteq\{(j,k)\in\mathbb{N}_0\times\mathbb{N}_0, j\le k:\lambda_j^{(m)}+\lambda_{k-1}^{(m)}=\lambda_{i+1}^{(m)}\}$. Indeed, since $q\mid i+2, q\nmid i+2+g_m=\lambda_{i+2}^{(m)}$. So, $\lambda_{i+2}^{(m)}=\lambda_j^{(m)}+\lambda_k^{(m)}$ with $\lambda_j^{(m)}\le\lambda_k^{(m)}$ is only possible if $\lambda_j^{(m)}<c_m$ and $\lambda_k^{(m)}>c_m$. In this case, $\lambda_{i+1}^{(m)}=\lambda_{i+2}^{(m)}-1=\lambda_j^{(m)}+\lambda_k^{(m)}-1=\lambda_j^{(m)}+\lambda_{k-1}^{(m)}$. □

Theorem 7: The order bound on the minimum distance is shown in the second equation at the bottom of the page,where $l=m+1-\lceil\log_q(q^m+q^{\lfloor \frac{m}{2}\rfloor}-i-2)\rceil$.

Proof: The cases $i\le q^{\lfloor \frac{m}{2}\rfloor}-1$ and $i>q^m-q^{\lfloor \frac{m+1}{2}\rfloor}+q^{\lfloor \frac{m}{2}\rfloor}-3$ follow directly from Lemma 6 and Lemma 5.

Suppose $q^{\lfloor \frac{m}{2}\rfloor}-1<i\le q^m-q^{\lfloor \frac{m+1}{2}\rfloor}+q^{\lfloor \frac{m}{2}\rfloor}-3$.

If $q\mid i+2$, then

$$\begin{aligned}\delta_i^{(m)}&=\nu_{i+2}^{(m)}\\&=2+2(\lambda^{(m)})^{-1}(\lfloor i+2-q^{\lfloor \frac{m}{2}\rfloor}\rfloor_{\Lambda(m)})\\&=2q^{l-1}(-q^l+q+1)+2\left\lfloor\frac{i+2-q^{\lfloor \frac{m}{2}\rfloor}}{q^{m-2l+1}}\right\rfloor.\end{aligned}$$

Here we have used Lemma 6, Lemma 5, and Theorem 4.

For $q\nmid i+2$,

$$\delta_i^{(m)}=\nu_{i+1}^{(m)}=2+2(\lambda^{(m)})^{-1}(\lfloor i+1-q^{\lfloor \frac{m}{2}\rfloor}\rfloor_{\Lambda(m)}).$$

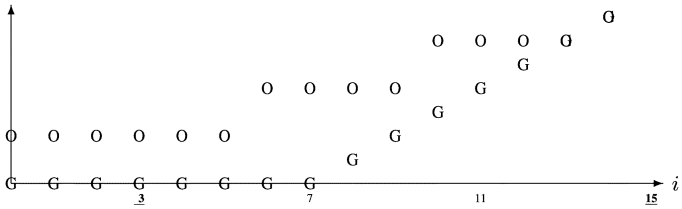

Fig. 7. $d_{FR}-d_G$-sequence of $\Lambda^{(2)}$ for $q=4$.

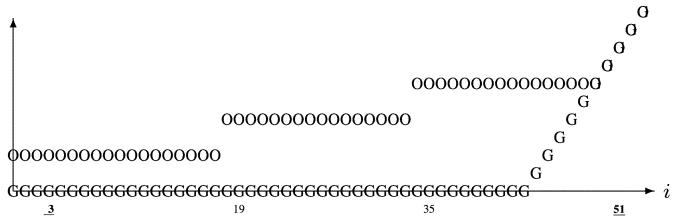

Fig. 8. $d_{FR}-d_G$-sequence of $\Lambda^{(3)}$ for $q=4$.

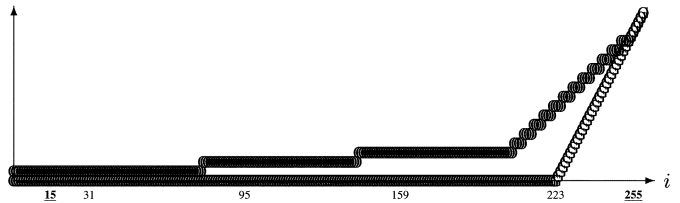

Fig. 9. $d_{FR}-d_G$-sequence of $\Lambda^{(4)}$ for $q=4$.

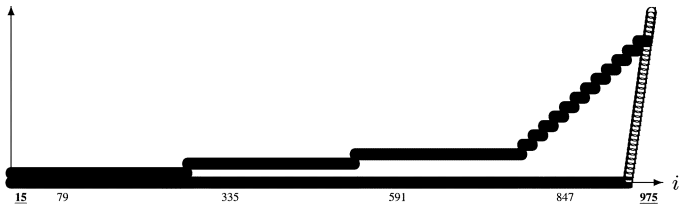

Fig. 10. $d_{FR}-d_G$-sequence of $\Lambda^{(5)}$ for $q=4$.

However, $\lfloor i+2-q^{\lfloor \frac{m}{2}\rfloor}\rfloor_{\Lambda^{(m)}}=\lfloor i+1-q^{\lfloor \frac{m}{2}\rfloor}\rfloor_{\Lambda^{(m)}}$ since in this case $i+2-q^{\lfloor \frac{m}{2}\rfloor}=i+1-c_m+g_m<c_m$ and $q\nmid i+2-q^{\lfloor \frac{m}{2}\rfloor}$. Thus, we can use the same formula as above for $\delta_i^{(m)}$. □

In Figs 7–10, there are the values of the order bound sequence and the values of the Goppa bound sequence for $\Lambda^{(2)}, \Lambda^{(3)}, \Lambda^{(4)}$, and $\Lambda^{(5)}$, for $q=4$. We used O's for the order bound and G's for the Goppa bound. As before, in the horizontal axis we wrote the indices i such that the corresponding nongap λ_i is a multiple of q^{m-1}, as well as the index of the conductor and twice the conductor. These two last indices have been underlined. The Goppa bound has been set to 0 when negative. It is easy to check that for the first values, which correspond to higher

$$\delta_i^{(m)}=\begin{cases}2, & \text{if } i\le q^{\lfloor \frac{m}{2}\rfloor}-1\\ \nu_{i+2}^{(m)} & \text{if } q^{\lfloor \frac{m}{2}\rfloor}-1<i\le q^m-q^{\lfloor \frac{m+1}{2}\rfloor}+q^{\lfloor \frac{m}{2}\rfloor}-3 \text{ and } q\mid i+2\\ \nu_{i+1}^{(m)}, & \text{otherwise.}\end{cases}$$

$$\delta_i^{(m)}=\begin{cases}2, & \text{if } i\le q^{\lfloor \frac{m}{2}\rfloor}-1\\ 2q^{l-1}(-q^l+q+1)+2\left\lfloor\frac{i+2-q^{\lfloor \frac{m}{2}\rfloor}}{q^{m-2l+1}}\right\rfloor, & \text{if } q^{\lfloor \frac{m}{2}\rfloor}-1<i\le q^m-q^{\lfloor \frac{m+1}{2}\rfloor}+q^{\lfloor \frac{m}{2}\rfloor}-3\\ i-g_m+2, & \text{if } i>q^m-q^{\lfloor \frac{m+1}{2}\rfloor}+q^{\lfloor \frac{m}{2}\rfloor}-3.\end{cases}$$

dimension codes, the order bound is significantly better than the Goppa bound. When $\lambda_i^{(m)} \geq 2c_m$ then both bounds coincide.

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, no. 4, pp. 1003–1012, 1994.

[2] C. Kirfel and R. Pellikaan, "The minimum distance of codes in an array coming from telescopic semigroups," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1720–1732, 1995, Special Issue On Algebraic Geometry Codes, Part 1.

[3] T. Høholdt, J. H. van Lint, and R. Pellikaan, *Algebraic Geometry Codes*. Amsterdam, The Netherlands: North-Holland, 1998, pp. 871–961.

[4] A. Garcia and H. Stichtenoth, "On the asymptotic behavior of some towers of function fields over finite fields," *J. Number Theory*, vol. 61, no. 2, pp. 248–273, 1996.

[5] R. Pellikaan, H. Stichtenoth, and F. Torres, "Weierstrass semigroups in an asymptotically good tower of function fields," *Finite Fields Appl.*, vol. 4, no. 4, pp. 381–392, 1998.

[6] R. Pellikaan and F. Torres, "On Weierstrass semigroups and the redundancy of improved geometric goppa codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2512–2519, 1999.

[7] H. Chen, "Codes on Garcia-Stichtenoth curves with true distance greater than Feng-Rao distance," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 706–709, Mar. 1999.

A Generic Construction of Complex Codebooks Meeting the Welch Bound

Cunsheng Ding, *Senior Member, IEEE*, and Tao Feng

***Abstract*—Codebooks (also called signal sets) meeting the Welch bound on the maximum correlation amplitude are called MWBE codebooks and are desirable in code-division multiple-access systems. Two different but related constructions of MWBE codebooks from difference sets were developed by Xia *et al.* and Ding recently. The objectives of this correspondence are to present a generic construction of MWBE codebooks that contains the previous two constructions as special cases and describe new MWBE codebooks that cannot be produced by the earlier two constructions.**

***Index Terms*—Difference sets, frames, MWBE codebooks, packing, signal sets, Welch bounds.**

I. INTRODUCTION

An (N, K) *codebook* $\mathcal{C}$ is a set $\{\mathbf{c}_0, \mathbf{c}_{N-1}\}$ of N unit norm $1 \times K$ complex vectors $\mathbf{c}_i$, which are called *codewords* of the codebook. The *alphabet* of the codebook is the set of all different complex values that the coordinates of all the codewords take. The *alphabet size* is the number of elements in the alphabet.

Manuscript received August 29, 2006; revised July 10, 2007. The work of C. Ding was supported by the Research Grants Council of the Hong Kong Special Administration Region, China (Proj. no. 612405). The work of T. Feng was supported by the Natural Science Foundation of China (Proj. no. 10331030).

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clearwater Bay, Kowloon, Hong Kong, China (e-mail: cding@cse.ust.hk).

T. Feng is with the School of Mathematical Sciences, Peking University, Beijing, 100871, China (e-mail: ift@pku.edu.cn).

Communicated by P. Viswanath, Associate Editor for Communications.

Digital Object Identifier 10.1109/TIT.2007.907343

As measures of performance of a codebook $\mathcal{C}$ in CDMA communication systems, the root-mean-square (RMS) correlation and the maximum correlation amplitudes of $\mathcal{C}$ are introduced and defined as

$$I_{\rm rms}(\mathcal{C}) := \sqrt{\frac{1}{N(N-1)} \sum_{0 \leq i,j \leq N-1 \atop i \neq j} \left|\mathbf{c}_i \mathbf{c}_j^{\mathbf{H}}\right|^2}$$

$$I_{\max}(\mathcal{C}) := \max_{0 \leq i < j \leq N-1} \left|\mathbf{c}_i \mathbf{c}_j^{\mathbf{H}}\right|$$

here and hereafter $\mathbf{c}^H$ stands for the conjugate transpose of the complex vector $\mathbf{c}$.

The following Welch bounds are well known [16], [21]:

Lemma 1: For any codebook $\mathcal{C}$ with $N \geq K$,

$$I_{\rm rms}(\mathcal{C}) \geq \sqrt{\frac{N-K}{(N-1)K}} \tag{1}$$

with equality if and only if $\sum_{i=0}^{N} \mathbf{c}_i^{\mathbf{H}} \mathbf{c}_i = (N/K)\mathbf{I}_K$, where $\mathbf{I}_K$ denotes the $K \times K$ identity matrix. We have also

$$I_{\max}(\mathcal{C}) \geq \sqrt{\frac{N-K}{(N-1)K}} \tag{2}$$

with equality if and only if for all pairs (i, j) with $i \neq j$

$$\left|\mathbf{c}_i \mathbf{c}_j^{\mathbf{H}}\right| = \sqrt{\frac{N-K}{(N-1)K}}. \tag{3}$$

If the equality holds in (1), the codebook $\mathcal{C}_D$ is referred to as a *Welch-bound-equality (WBE) codebook*. A codebook meeting the bound of (2) is called a *maximum-Welch-bound-equality (MWBE) codebook*. An MWBE codebook must be a WBE codebook, but a WBE codebook may not be an MWBE codebook. MWBE codebooks form a proper subset of WBE codebooks.

A well-rounded treatment of MWBE and WBE codebooks was given by Sarwate [17]. They have applications also in quantum information processing [22], packing [6], and coding theory [4], [7].

It is trivially easy to construct WBE codebooks. Every linear error correcting code whose dual code with Hamming distance at least 3 yields a WBE codebook [16], [17]. There are many other constructions of WBE codebooks. The reader is referred to Sarwate [17] for a survey of constructions of WBE codebooks.

However, MWBE codebooks are very hard to construct, as pointed out by Sarwate in ([17, p. 100]) The following are the known classes of MWBE codebooks.

1) (N, N) orthogonal MWBE codebooks for any $N > 1$ [23], [17].
2) $(N, N-1)$ MWBE codebooks for any $N > 1$ obtained from the FFT matrix [23], [17], and some $(N, N-1)$ MWBE codebooks from the m-sequence codes [17].
3) (N, K) MWBE codebooks based on conference matrices [6], [20], when $N = 2K = 2^{d+1}$ and d is a positive integer, and $N = 2K = p^d + 1$ with p a prime number and d a positive integer.
4) (N, K) MWBE codebooks based on (N, K, λ) cyclic difference sets in $\mathbf{Z}_N$ [23] and those based on (N, K, λ) difference sets in finite fields GF(q) [9].

In this correspondence, by extending the ideas of [23] and [9], we present a generic construction of MWBE complex codebooks from difference sets in Abelian groups, and new MWBE codebooks that cannot be produced by the constructions in [23] and [9]. The generic construction contains those in [23] and [9] as special cases, and is thus a generalization of the earlier two constructions.