[6] ——, "Codes on graphs: Generalized state realizations," *IEEE Trans. Inform. Theory*, submitted for publication.

[7] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 242–245, Jan. 1993.

[8] R. Kötter and A. Vardy, "Construction of minimal tail-biting trellises," in *Proc. IEEE Information Theory Workshop*, Killarney, Ireland, June 1998, pp. 72–74.

[9] F. R. Kschischang and V. Sorokine, "On the trellis structure of block codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1924–1937, Nov. 1995.

[10] A. Lafourcade and A. Vardy, "Optimal sectionalization of a trellis," *IEEE Trans. Inform. Theory*, vol. 42, pp. 689–703, May 1996.

[11] C.-C. Lu and S.-H. Huang, "On bit-level trellis complexity of Reed–Muller codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 2061–2064, Nov. 1995.

[12] R. J. McEliece, "On the BCJR trellis for linear block codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1072–1092, July 1996.

[13] D. J. Muder, "Minimal trellises for block codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1049–1053, Sept. 1988.

[14] V. R. Sidorenko, "The Euler characteristic of the minimal code trellis is maximum," *Probl. Inform. Transm.*, vol. 33, no. 1, pp. 87–93, Mar. 1997.

[15] G. Solomon and H. C. A. van Tilborg, "A connection between block and convolutional codes," *SIAM J. Appl. Math.*, vol. 37, pp. 358–369, Oct. 1979.

[16] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 533–547, Sept. 1981.

[17] A. Vardy, "Trellis structure of codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, Dec. 1998.

[18] A. Vardy and F. R. Kschischang, "Proof of a conjecture of McEliece regarding the expansion index of the minimal trellis," *IEEE Trans. Inform. Theory*, vol. 42, pp. 2027–2034, Nov. 1996.

[19] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1412–1418, Sept. 1991.

[20] N. Wiberg, "Codes and decoding on general graphs," Ph.D. dissertation, Dept. Elec. Eng., Univ. Linköoping, Sweden, Apr. 1996.

[21] N. Wiberg, H.-A. Loeliger, and R. Kötter, "Codes and iterative decoding on general graphs," *Euro. Trans. Telecommun.*, vol. 6, pp. 513–526, Sept. 1995.

Bounds on the State Complexity of Codes from the Hermitian Function Field and its Subfields

Yaron Shany and Yair Be'ery, *Senior Member, IEEE*

***Abstract*—An upper bound on the minimal state complexity of codes from the Hermitian function field and some of its subfields is derived. Coordinate orderings under which the state complexity of the codes is not above the bound are specified. For the self-dual Hermitian code it is proved that the bound coincides with the minimal state complexity of the code. Finally, it is shown that Hermitian codes over fields of characteristic 2 admit a recursive twisted squaring construction.**

***Index Terms*—Geometric Goppa codes, Hermitian codes, minimal state complexity, trellises, twisted squaring construction.**

I. Introduction

A *trellis diagram* can be regarded as an efficient representation of a code for the purpose of soft-decision decoding. Formally, a trellis $T = (V, E)$ of rank n is a finite-directed graph, with vertex set V and edge set E, in which every vertex is assigned a "depth" in the range $\{0, 1, \cdots, n\}$, and each edge connects a vertex at depth $i - 1$ to one at depth i, $1 \le i \le n$. The class of vertices at depth i, $0 \le i \le n$, is denoted by V_i. We assume that each edge of T is labeled with an element of $\mathbb{F}_q$, the finite field of q elements. In addition, we only consider trellises for which $|V_0| = |V_n| = 1$. Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_q$ (i.e., $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d). We say that the rank-n trellis T *represents* the code $\mathcal{C}$ if $\mathcal{C}$ is identical to the set of n-tuples read from all paths of T connecting the vertex in V_0 to the one in V_n. It is well known that any length-n linear code under a fixed coordinate ordering has a unique trellis representation (up to isomorphism), $T = (V, E)$, that minimizes $|V_i|$ simultaneously for all i, $0 \le i \le n$ (see [7], [15], and references therein for a summary of the subject). This trellis is called the *minimal* trellis of the code. For the code $\mathcal{C}$ we define $s_i := \log_q |V_i|$, $0 \le i \le n$, where V_i corresponds to the minimal trellis of $\mathcal{C}$. The *state complexity profile* of $\mathcal{C}$ is the sequence $s_0, s_1, \cdots, s_n$. The *state complexity* of $\mathcal{C}$ is defined as $s := \max_{0 \le i \le n} s_i$. Forney [3] demonstrated that the state complexity of $\mathcal{C}$ may vary with respect to different ordering of coordinates. The *minimal state complexity* of $\mathcal{C}$ is the minimal state complexity attainable by any ordering of the coordinates.

For a fixed coordinate ordering of the $[n, k]$ linear code $\mathcal{C}$, the entire state complexity profile can be calculated from $s_i = k - k_{i_-} - k_{i_+}$, $1 \le i \le n - 1$, where k_{i_-} is the dimension of the *past subcode* at i, i.e., the subcode consisting of all codewords $(c_1, c_2, \cdots, c_n) \in \mathcal{C}$ with $(c_{i+1}, c_{i+2}, \cdots, c_n) = (0, 0, \cdots, 0)$, and k_{i_+} is the dimension of the *future subcode* at i, i.e., the subcode consisting of all codewords $(c_1, c_2, \cdots, c_n) \in \mathcal{C}$ with $(c_1, c_2, \cdots, c_i) = (0, 0, \cdots, 0)$ [3].

The determination of the minimal state complexity and the attempt to find "good" coordinate orderings with respect to the trellis complexity of some important classes of codes were considered in several papers, e.g., [10], [11], [1], [16], [2]. These papers addressed the trellises of Reed–Muller, Bose–Chaudhuri–Hocquenghem (BCH), and quadratic-residue codes, and it seems only natural to investigate the trellis of *geometric Goppa codes*. Among geometric Goppa codes, the class of *Hermitian codes* (geometric Goppa codes arising from the *Hermitian function field*) was extensively studied. A simple presentation of the Hermitian function field and the related codes was given by Stichtenoth in [12]. The results of [12] were used in [19] to give a description of Hermitian codes which will be useful for our purposes. The *generalized Hemming weights (GHW) hierarchy* [17] of Hermitian codes and of geometric Goppa codes arising from some subfields of the Hermitian function field was studied in [20], [8], and [9].

In this correspondence, we give an upper bound on the state complexity of codes associated with the Hermitian function field and some of its subfields. For self-dual Hermitian codes, the minimal state complexity is determined, and coordinate orderings under which the state complexity coincides with the minimal state complexity are specified. The correspondence is organized as follows. In the following section we give some background on geometric Goppa codes. A lower bound on the minimal state complexity of geometric Goppa codes is presented. Then, in Section III, we give an upper bound on the state complexity profile of Hermitian codes and codes from certain subfields of the Hermitian function field, and specify coordinate orderings for which the state complexity profile is actually not above the bound. A simple formula for an upper bound on the minimal state complexity of self-dual codes from the Hermitian function field and some of its subfields is then derived. Finally, it is proved that the bound on the minimal state complexity of self-dual Hermitian codes is indeed the minimal state complexity itself. We conclude in Section IV by showing

Manuscript received September 29, 1999; revised March 9, 2000.

The authors are with the Department of Electrical Engineering–Systems, Tel-Aviv University, Ramat-Aviv 69978, Israel (e-mail: shany@eng.tau.ac.il; ybeery@eng.tau.ac.il).

Communicated by I. F. Blake, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(00)05294-9.

that Hermitian codes over fields of characteristic 2 admit a *recursive twisted squaring construction* [3], [2].

II. Geometric Goppa Codes and Hermitian Codes

This section contains a brief description of geometric Goppa codes in general, and codes from the Hermitian function field and some of its subfields in particular. A lower bound on the minimal state complexity of geometric Goppa codes is presented. We follow the notation of Stichtenoth [14], and the reader is referred to [14] for the basic theory of algebraic function fields and a detailed description of geometric Goppa codes.

Let F/K be an algebraic function field of genus g over a constant field $K = \mathbb{F}_q$. The set of all places of F/K is denoted by $\mathbb{P}_F$. For a divisor A of F/K we set

$$\mathcal{L}(A) := \{x \in F \,|\, (x) \geq -A\} \cup \{0\}$$

where (x) is the principal divisor of x. We denote by $\dim A$ and $\deg A$ the dimension of $\mathcal{L}(A)$ over K and the degree of A, respectively.

Let $\{P_1, P_2, \cdots, P_n\}$ be a set of pairwise distinct places of degree 1 in F/K, and define the divisor D of F/K as $D := P_1 + P_2 + \cdots + P_n$. Suppose that G is a divisor of F/K with $\operatorname{supp} G \cap \operatorname{supp} D = \phi$, where $\operatorname{supp} A$ stands for the support of the divisor A. The geometric Goppa code $C_{\mathcal{L}}(D, G)$ associated with the divisors D and G is defined by

$$C_{\mathcal{L}}(D, G) := \{(z(P_1), z(P_2), \cdots, z(P_n)) \,|\, z \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

The code $C_{\mathcal{L}}(D, G)$ is an $[n, k, d]$ code over K with parameters $k = \dim G - \dim(G - D)$, and $d \geq n - \deg G$. In particular, when $\deg G < n$, we have $k = \dim G \geq \deg G - g + 1$ [14]. The integer $d^* := n - \deg G$ is called the *designed distance* of the code $C_{\mathcal{L}}(D, G)$. When $\deg G < n$, we have $d^* \geq (n - k + 1) - g$, that is, the designed minimum distance of $C_{\mathcal{L}}(D, G)$ is within g of the Singleton bound. It is therefore clear that for codes derived from function fields of small genus it is not possible to have a significant improvement upon the *Wolf bound* [18] under any coordinate ordering (cf. [4]). Indeed, using the *dimention/length profile (DLP) bound* on the state complexity profile [4], it can be verified that for an $[n, k, d]$ code with $d \geq (n-k+1)-g$, we have $s_{\lfloor n/2 \rfloor} \geq \min\{k, n-k-2g\}$ under any coordinate ordering. Using Clifford's theorem [14], this bound can be slightly sharpened.

Proposition 1: The minimal state complexity of $C_{\mathcal{L}}(D, G)$ is smaller than the Wolf bound only if $\lfloor n/2 \rfloor \leq \deg G \leq \lceil n/2 \rceil + 2g - 2$. If $\deg G$ is in the above interval and $2g - 2 < \lfloor n/2 \rfloor$, then the minimal state complexity is at least $\lceil n/2 \rceil - g - 1$.

Proof: Observe that the past subcode at index i, $1 \leq i \leq n-1$, of $C_{\mathcal{L}}(D, G)$ is exactly $C_{\mathcal{L}}(D, G - P_{i+1} - P_{i+2} - \cdots - P_n)$. Similarly, the future subcode at index i, $1 \leq i \leq n-1$, of $C_{\mathcal{L}}(D, G)$ is exactly $C_{\mathcal{L}}(D, G - P_1 - P_2 - \cdots - P_i)$. Since we are only interested in the dimensions of these subcodes, we can replace the past subcode at i with

$$C_{\mathcal{L}}(D - P_{i+1} - P_{i+2} - \cdots - P_n, G - P_{i+1} - P_{i+2} - \cdots - P_n)$$

(the code obtained by truncating the last $n - i$ zero coordinates) and the future subcode at i with

$$C_{\mathcal{L}}(D - P_1 - P_2 - \cdots - P_i, G - P_1 - P_2 - \cdots - P_i)$$

(the code obtained by truncating the first i zero coordinates). Note that for each one of these truncated codes the two divisors involved are of disjoint supports. The state complexity of $C_{\mathcal{L}}(D, G)$ at index i, $1 \leq i \leq n - 1$, is therefore

$$\begin{aligned} s_i = {} & \dim G + \dim(G - D) \\ & - \dim(G - (P_{i+1} + P_{i+2} + \cdots + P_n)) \\ & - \dim(G - (P_1 + P_2 + \cdots + P_i)). \end{aligned} \tag{1}$$

Let us choose $i = \lfloor n/2 \rfloor$. If $\deg G < \lfloor n/2 \rfloor$, then, since the dimension of a negative–degree divisor is zero, we obtain $s_{\lfloor n/2 \rfloor} = \dim G = k$, where $k := \dim C_{\mathcal{L}}(D, G)$. On the other hand, if $\deg G > \lceil n/2 \rceil + 2g - 2$, then, by the Riemann–Roch theorem and (1), we have

$$\begin{aligned} s_{\lfloor n/2 \rfloor} &= \dim G + \dim(G - D) \\ &\quad - (\deg G - g + 1 - \lceil n/2 \rceil + \deg G - g + 1 - \lfloor n/2 \rfloor) \\ &= \dim G + \dim(G - D) - (2 \dim G - n) = n - k. \end{aligned}$$

Finally, if

$$2g - 2 < \lfloor n/2 \rfloor \leq \deg G \leq \lceil n/2 \rceil + 2g - 2$$

then in particular $2g-2 < \deg G < n$. In this case, Clifford's theorem and (1) give

$$\begin{aligned} s_{\lfloor n/2 \rfloor} &\geq \dim G - \Big(1 + \tfrac{1}{2} \deg G - \frac{1}{2} \lceil n/2 \rceil \\ &\qquad + 1 + \frac{1}{2} \deg G - \frac{1}{2} \lfloor n/2 \rfloor \Big) \\ &= n/2 - g - 1. \end{aligned} \tag{2}$$

Since $s_{\lfloor n/2 \rfloor}$ is an integer, (2) becomes $s_{\lfloor n/2 \rfloor} \geq \lceil n/2 \rceil - g - 1$. □

In view of Proposition 1 and the preceding discussion, it seems reasonable to investigate the trellis representation of Hermitian codes and codes from certain subfields of the Hermitian function field. Let $K = \mathbb{F}_{q^2}$, and let $F = K(x, y)$ be the function field defined by

$$F = K(x, y) \text{ with } y^q + y = x^a \text{ and } a | q + 1$$

(see [14], [20]). When $a = q+1$, F/K is called the Hermitian function field over K. When $a < q + 1$, F/K is isomorphic to a subfield of the Hermitian function field [14], [20], and is, therefore, referred to as a subfield of the Hermitian function field. The genus of F/K is $g = (q - 1)(a - 1)/2$, and there are exactly $1 + q(1 + a(q - 1))$ places of degree one in F/K. Let P_∞ be the pole of x in $\mathbb{P}_{K(x)}$, and for $\alpha \in K$ let P_α be the zero of $(x - \alpha)$ in $\mathbb{P}_{K(x)}$. The places in $\{P_\infty\} \cup \{P_\alpha | \alpha \in K\}$, are exactly all the places of degree 1 in $\mathbb{P}_{K(x)}$. Let U^* be the subgroup of order $(q - 1)a$ in the multiplicative group K^*, and let $U := U^* \cup \{0\}$. Then for each $\alpha \in U$ there are q solutions in K for the equation $T^q + T = \alpha^a$, and for each solution $\beta \in K$ there is a unique place of $\mathbb{P}_F$ *lying over* P_α that contains $(y - \beta)$ [14]. This place is denoted by $P_{\alpha, \beta}$. In fact, all places of degree one in F/K are exactly

$$\{P_{\alpha, \beta} | \alpha \in U, \, \beta^q + \beta = \alpha^a\} \cup \{Q_\infty\}$$

where Q_∞ is the common pole of x and y in $\mathbb{P}_F$. Define the divisor D as

$$D := \sum_{\alpha \in U} \sum_{\substack{\beta \in K \\ \beta^q + \beta = \alpha^a}} P_{\alpha, \beta}$$

i.e., D is the sum of all places of degree 1 in F/K, except for Q_∞. Let n be the degree of D, i.e., $n = q(1 + (q - 1)a)$. In order to use D in the definition of a geometric Goppa code, we must fix an ordering of the places in its support. So, let $\operatorname{Ind} : \operatorname{supp} D \to \{1, 2, \cdots, n\}$ be a bijection, so that $\operatorname{Ind}(P_{\alpha, \beta})$ is the index corresponding to $P_{\alpha, \beta}$. For an integer $m \geq 0$, the set $\{x^i y^j | i \geq 0, \, 0 \leq j \leq q-1, \, iq + ja \leq m\}$ constitutes a basis for $\mathcal{L}(mQ_\infty)$ over K [14]. The code C_m is defined as $C_m := C_{\mathcal{L}}(D, mQ_\infty)$. We shall refer to the cases $a = q + 1$ and $a < q + 1$ as the Hermitian and non-Hermitian cases, respectively. In the Hermitian case, we refer to C_m as a Hermitian code. The duals of Hermitian codes are also Hermitian codes [14]. For an $n \times n$ matrix A over K and a length-n linear code $\mathcal{C}$, let $\mathcal{C}A := \{\boldsymbol{c}A \,|\, \boldsymbol{c} \in \mathcal{C}\}$. Using the results of [13], it was mentioned in [20] that for the non-Hermitian case, there is an $n \times n$ diagonal matrix $A = (a_{ij})$ with $0 \neq a_{ii} \in K$, $1 \le i \le n$, such that the dual of C_m is $C_{n+2g-2-m}A$. Moreover, if $a \equiv 1 \mod p$, where p is the characteristic of K, then the dual of C_m is $C_{n+2g-2-m}$.

In order to give a description of C_m similar to the one given in [19] (where only the Hermitian case was considered), some additional definitions are required. Let $\overline{D}$ be the divisor of $K(x)/K$ defined by $\overline{D} := \sum_{\alpha \in U} P_\alpha$. Let

$$\overline{\mathrm{Ind}}: \mathrm{supp}\,(\overline{D}) \rightarrow \{1, 2, \cdots, (q-1)a+1\}$$

be a bijection, so that $\overline{\mathrm{Ind}}(P_\alpha)$ assigns an index to P_α, $\alpha \in U$. For an integer $\overline{m} \ge 0$, let $\overline{C}_{\overline{m}}$ be the code from the rational function field defined by $\overline{C}_{\overline{m}} := C_{\mathcal{L}}(\overline{D}, (\overline{m} - 1)P_\infty)$. In the Hermitian case $(a = q+1)$, $\overline{C}_{\overline{m}}$ is an extended Reed–Solomon code. For $l \in \mathbb{Z}_+$ and a length-n' (n' being a positive integer) linear code $\mathcal{C}$, define

$$\mathcal{C}^{[l]} := \Bigg\{ (\underbrace{c_1, \cdots, c_1}_{l \text{ times}}, \underbrace{c_2, \cdots, c_2}_{l \text{ times}}, \cdots, \underbrace{c_{n'}, \cdots, c_{n'}}_{l \text{ times}}) \\ \mid (c_1, c_2, \cdots, c_{n'}) \in \mathcal{C} \Bigg\}$$

and let $\overline{G}_{\overline{m}}$ be a generator matrix of $\overline{C}^{[q]}_{\overline{m}}$. Let $\kappa := \min(q-1, \lfloor \frac{m}{a} \rfloor)$ be the maximum power of y in the above basis for $\mathcal{L}(mQ_\infty)$, and for $0 \le j \le \kappa$ let

$$k(j) := |\{i \ge 0 | iq + ja \le m\}| = \left\lfloor \frac{m - ja}{q} \right\rfloor + 1.$$

We say that the code C_m is under a *valid* coordinate ordering when, for every $\alpha \in U$, all the extensions of P_α in $\mathbb{P}_F$ are mapped to consecutive indices, that is, for every $P_{\alpha,\beta} \in \mathrm{supp}\,(D)$, it holds that

$$q(\overline{\mathrm{Ind}}\,(P_\alpha) - 1) + 1 \le \mathrm{Ind}\,(P_{\alpha,\beta}) \le q(\overline{\mathrm{Ind}}\,(P_\alpha)).$$

Let $\Sigma = (\sigma_{ij})$ be the $n \times n$ diagonal matrix defined by $\sigma_{ii} = \beta$, $1 \le i \le n$, if $i = \mathrm{Ind}\,(P_{\alpha,\beta})$ for some $\alpha \in U$. Define the matrix G_m by

$$G_m := \begin{pmatrix} \overline{G}_{k(0)} \\ \overline{G}_{k(1)}\Sigma \\ \vdots \\ \overline{G}_{k(\kappa)}\Sigma^\kappa \end{pmatrix}. \tag{3}$$

Then it follows directly from the definition of the code C_m and the above described basis of $\mathcal{L}(mQ_\infty)$ that if $m < n$, then G_m is a generator matrix of C_m under a valid coordinate ordering [19].

III. An Upper Bound on the State Complexity of the Codes

In this section, we use the generator matrix given in the previous section to show that, for some values of m, when C_m is under a valid coordinate ordering its state complexity is below the Wolf bound. For the self-dual Hermitian code $C_{(q^3+q^2-q-2)/2}$ (q is a power of 2), we shall see that an improvement of $q^2/4$ upon the Wolf bound is possible. Furthermore, for this case we shall see that $q^2/4$ is the maximum possible improvement upon the Wolf bound over all coordinate orderings of the code.

Let $\mathcal{C}$ be an $[n', k, d]$ code, and let G be a *minimal-span generator matrix (MSGM)* of $\mathcal{C}$ [7] (i.e., G is a generator matrix of $\mathcal{C}$ in which there are no two rows whose first nonzero entries are at the same index, and no two rows whose last nonzero entries are at the same index). Then s_i, $1 \le i \le n'-1$, is equal to the number of *active rows* in G at index i [5], [7], where $s_0, s_1, \cdots, s_{n'}$ is the state complexity profile of $\mathcal{C}$. From the structure of G_m in (3), we have the following proposition.

Proposition 2: Suppose that $0 \le m \le \lfloor n/2 \rfloor + g - 1$ so that $\dim\, C_m \le \lfloor n/2 \rfloor$, and let $(s_0, s_1, \cdots, s_n)$ be the state complexity profile of C_m when under a valid coordinate ordering. Then

$$s_i \le \begin{cases} \min\left\{i,\, n-i,\, \sum_{j=0}^{\kappa} (\min\{k(j),\, n/q - k(j)\})\right\}, & \text{if } q|i \\ \min\left\{s_{\lfloor i/q \rfloor q} + (i - \lfloor i/q \rfloor q),\, s_{\lceil i/q \rceil q} + (\lceil i/q \rceil q - i)\right\}, & \text{otherwise} \end{cases} \tag{4}$$

for $i \in \{0, 1, \cdots, n\}$.

Proof: Suppose that $\mathcal{C}$ is a length-n' (n' being a positive integer) linear code over a finite field K', $l \in \mathbb{Z}_+$, and $\Gamma = (\gamma_{uv})$ is an $n'l \times n'l$ diagonal matrix over K'. Assume that for every u, $1 \le u \le n'$, it holds that at least one of

$$\gamma_{(u-1)l+1,\,(u-1)l+1},\, \gamma_{(u-1)l+2,\,(u-1)l+2},\, \cdots,\, \gamma_{ul,\,ul}$$

is not zero. Then it is clear that the number of active rows at index il, $1 \le i \le n'$, in an MSGM of $\mathcal{C}^{[l]}\Gamma$ is equal to the number of active rows at index i in an MSGM of $\mathcal{C}$. Now consider the generator matrix G_m from (3). Suppose that each one of the submatrices $\overline{G}_{k(j)}\Sigma^j$, $0 \le j \le \kappa$ is an MSGM. By the above argument, the number of active rows at index i with $q|i$ in $\overline{G}_{k(j)}\Sigma^j$ is no more than $\min\{k(j),\, n/q - k(j)\}$. This proves the part of (4) concerning indices divisible by q. The other part of (4) follows from the fact that

$$s_i \le \min\{s_{i-1},\, s_{i+1}\} + 1, \qquad 1 \le i \le n-1. \qquad \square$$

Note that for the cases where $\dim\, C_m > n/2$, the bound on the state complexity profile of C_m is identical to the bound on the state complexity of $C_{n+2g-2-m}$, where the latter can be obtained from Proposition 2. This follows from combining the fact that the state complexity profiles of a linear code and its dual are identical [3], and the fact that there is a diagonal matrix A (in which every diagonal element is nonzero) such that $C_{n+2g-2-m}A$ is the dual of C_m. (Observe that the state complexity profile of $C_{n+2g-2-m}A$ is identical to that of $C_{n+2g-2-m}$.)

As a result of Proposition 2, we have the following corollary.

Corollary 3: Let $(s_0, s_1, \cdots, s_n)$ be as in Proposition 2, and let $m_0 := q\lfloor \frac{n}{2q} \rfloor$. Then for $m_0 \le m \le n + 2g - 2 - m_0$ and $q \ge 4$, we have that $\max_{0 \le i \le n/q} s_{iq}$ is smaller than the Wolf bound by at least

$$\sum_{j=0}^{j_m} (k(j) - (n/q - k(j)))$$

where $j_m := \lfloor (\tilde{m} - m_0)/a \rfloor$, and $\tilde{m} := \min(m,\, n + 2g - 2 - m)$.

Proof: Let us first assume that $m_0 \le m \le \lfloor n/2 \rfloor + g - 1$. Under this assumption $\dim\, C_m \le \lfloor n/2 \rfloor$, and we can use (4). Since

$$\dim\, C_m = \sum_{j=0}^{\kappa} k(j)$$

it is clear that each j for which $n/q - k(j) < k(j)$ contributes $k(j) - (n/q - k(j))$ to the difference between the Wolf bound and $\max_{0 \le i \le n/q} s_{iq}$. Some arithmetics show that $n/q - k(j) < k(j)$ if and only if $j \le j_m$, where j_m is defined in the corollary. This finishes the proof for $m_0 \le m \le \lfloor n/2 \rfloor + g - 1$. The proof for

$\lceil n/2 \rceil + g - 1 \leq m \leq n + 2g - 2 - m_0$ follows (as before) from the fact that the state complexity profiles of a linear code and its dual are identical. □

The results of Corollary 3 can be expressed in a more concise manner when C_m is self-dual, i.e., q is a power of 2 and $m = n/2 + g - 1$. In this case, it can be shown that the value of j_m from Corollary 3 is $j_m = q/2 - (t+1)/2$, where $t := (q+1)/a$. In addition, it is straightforward to verify that in this case

$$k(j) = \frac{qa}{2} - \left\lceil \frac{(2j+1)a+1}{2q} \right\rceil + 1.$$

Therefore, for

$$0 \leq j \leq j_m = q/2 - (t+1)/2$$

we have $k(j) = qa/2 - \lfloor j/t \rfloor$. Now, evaluating the sum from Corollary 3 we obtain that

$$\frac{n}{2} - \max_{0 \leq i \leq n/q} s_{iq} \geq \frac{(q+1)a - t}{4}$$

where $s_0, s_1, \cdots, s_n$ is the state complexity profile of C_m. We have therefore proved the following corollary.

Corollary 4: Let $q \geq 4$ be a power of 2, and let $m = n/2 + g - 1$. Suppose that $a > 1$, and let $t := (q+1)/a$. Then the state complexity of the self-dual code C_m when under a valid coordinate ordering is not more than

$$\frac{n}{2} - \left(\frac{(q+1)a - t}{4} - \frac{q}{2} \right).$$

We will now show that at least for the Hermitian case ($a = q + 1$), there are no coordinate orderings under which the state complexity of the self-dual code $C_{q^3/2+g-1}$ is smaller than that obtained in Corollary 4. This will be done using the DLP bound on the state complexity profile, and will require some results concerning the GHW hierarchy of Hermitian codes. From this point on, we consider only the Hermitian case $a = q + 1$. Let p_r, $r \geq 1$, be the rth *pole number* [14] of Q_∞. Then $\{p_r \,|\, r \geq 1\}$ is the semigroup generated by q and $q + 1$. For $m < n = q^3$, the Hermitian code C_m is *nonabundant* [8], and we have

$$d_r(C_m) \geq q^3 - m + p_r, \qquad 1 \leq r \leq k, \tag{5}$$

where $d_r(C_m)$ is the rth *generalized Hamming weight* [17] of C_m and $k := \dim C_m$ [20, Footnote 2 and Theorem 12], [8, Corollary 2 and Lemma 2]. For an integer $l \geq 0$ define $I(l) := \{u | u$ as a pole number of Q_∞, $u \leq l\}$.

Lemma 5: For $1 \leq i \leq q^3$ and $m < q^3$, we have

$$k_i(C_m) \leq \left| I(i - (q^3 - m)) \right|$$

where $k_i(C_m)$ is the ith entry of the DLP [4] of C_m.

Proof: Recall that for a length-n linear code $\mathcal{C}$ we have

$$k_i(\mathcal{C}) = |\{d_r(\mathcal{C}) \,|\, d_r(\mathcal{C}) \leq i\}|, \qquad 1 \leq i \leq n$$

[4], where $k_i(\mathcal{C})$ is the ith entry of the DLP of $\mathcal{C}$. The lemma then follows from (5). □

Remark 6: Suppose that $0 \leq l \leq 2g - 2 = q^2 - q - 2$, and write $l = cq + d$, where c, d are nonnegative integers, $0 \leq d \leq q - 1$. Then

$$|I(l)| = c(c+1)/2 + \min(c, d) + 1.$$

Proof: See [20]. □

The main result of this section can now be stated.

Theorem 7: Let $q \geq 4$ be a power of 2, and let

$$m = q^3/2 + g - 1 = q^3/2 + q^2/2 - q/2 - 1.$$

Then the minimal state complexity of the self-dual Hermitian code C_m is exactly $q^3/2 - q^2/4$. The minimal state complexity is achieved when C_m is arranged under a valid coordinate ordering.

Proof: In view of Corollary 4, we only have to find a single index i, $1 \leq i \leq q^3$, for which the DLP bound on the state complexity profile of C_m is $q^3/2 - q^2/4$. We choose $i = q^3/2 - q/2$. By Lemma 5 and Remark 6 we obtain that $k_i(C_m) + k_{q^3-i}(C_m) \leq q^2/4$. □

IV. The Twisted Squaring Construction of Hermitian Codes Over Fields of Characteristic 2

In this section it is shown that Hermitian codes over fields of characteristic 2 admit a recursive twisted squaring construction [3], [2]. Upper bounds on the state complexity profile of linear codes admitting a twisted squaring construction were given in [2]. Whereas the fact that some Hermitian codes admit a twisted squaring construction does not seem to contribute any knowledge regarding their trellis complexity beyond what is already given in Section III, it seems that the fact that these codes do admit such a construction is of interest.

Let $\mathcal{C}$ be an $[n, k, d]$ code over the finite field K, let $I := \{1, 2, \cdots, n\}$, and let $J := \{j_1, j_2, \cdots, j_{|J|}\}$ be a subset of I. The *projection* of $\boldsymbol{c} = (c_1, c_2, \cdots, c_n) \in \mathcal{C}$ onto J is defined by $\boldsymbol{c}^J := (c_{j_1}, c_{j_2}, \cdots, c_{j_{|J|}})$. The projection of $\mathcal{C}$ onto J is defined by $\mathcal{C}^J := \bigcup_{\boldsymbol{c} \in \mathcal{C}} \boldsymbol{c}^J$. The J*-subcode* of $\mathcal{C}$, $\mathcal{C}_J$, is the subcode of $\mathcal{C}$ consisting of all codewords $(c_1, c_2, \cdots, c_n) \in \mathcal{C}$ with $c_i = 0$ for all $i \in I \backslash J$, where $I \backslash J$ stands for the complementary set of J in I. For $1 \leq i!leqn$ we define $i_- := \{1, 2, \cdots, i\}$. Similarly, for $0 \leq i \leq n-1$, i_+ stands for $\{i+1, i+2, \cdots, n\}$. The code $\mathcal{C}$ is said to admit a twisted squaring construction if it is of even length, and both $\mathcal{C}^{(n/2)-} = \mathcal{C}^{(n/2)+}$ and $(\mathcal{C}_{(n/2)_-})^{(n/2)-} = (\mathcal{C}_{(n/2)_+})^{(n/2)+}$ (see [2] for a detailed exposition of the subject). When $\mathcal{C}$ admits a twisted squaring construction, we say that $\mathcal{C}^{(n/2)-}$ and $(\mathcal{C}_{(n/2)_-})^{(n/2)-}$ are the *component codes* of $\mathcal{C}$. If $n = 2^l$ for some $l \in \mathbb{Z}_+$, then the code $\mathcal{C}$ is said to admit a *recursive* twisted squaring construction when not only that the code itself admits a twisted squaring construction, but also its component codes admit a twisted squaring construction, the component codes of the component codes admit a twisted squaring construction, and so forth.

Proposition 8: Let C_m be the Hermitian code over $K = \mathbb{F}_{q^2}$, where $q^2 = 2^l$ for some even $l \in \mathbb{Z}_+$. Then there exists a coordinate ordering under which C_m admits a recursive twisted squaring construction.

Proof: The proof is based on the automorphisms of the Hermitian codes, and is quite similar to the proof of [2, Theorem 4]. Let σ be the $\mathbb{F}_{q^2}$-automorphism of the Hermitian function field $H = \mathbb{F}_{q^2}(x, y)$ defined by $\sigma(x) = \epsilon x + \delta$ and $\sigma(y) = \epsilon^{q+1} y + \epsilon \delta^q x + \mu$, where $\epsilon \in \mathbb{F}_{q^2} \backslash \{0\}$, $\delta \in \mathbb{F}_{q^2}$, and $\mu^q + \mu = \delta^{q+1}$ ($\mu \in \mathbb{F}_{q^2}$) [14]. The permutation of the Hermitian code C_m that takes the coordinate corresponding to $\sigma(P_{\alpha, \beta})$ to the coordinate corresponding to $P_{\alpha, \beta}$ for all α, $\beta \in \mathbb{F}_{q^2}$ with $\beta^q + \beta = \alpha^{q+1}$, is within the automorphism group of the code [14, Ch. VII]. It can be verified that the above automorphism of C_m can be defined by $\mathrm{Ind}(P_{u,v}) \mapsto \mathrm{Ind}\,(P_{\alpha, \beta})$, where α, $\beta \in \mathbb{F}_{q^2}$ satisfy $\beta^q + \beta = \alpha^{q+1}$, and u, $v \in \mathbb{F}_{q^2}$ satisfy

$\beta = \epsilon^{q+1}v+\epsilon\delta^q u+\mu$, $\alpha = \epsilon u+\delta$ (and indeed $v^q+v = u^{q+1}$). Choose a basis $\{a_1, a_2, \cdots, a_l\}$ for $\mathbb{F}_{q^2}/\mathbb{F}_2$ such that $\{a_1, a_2, \cdots, a_{l/2}\}$ is a basis for $\mathbb{F}_q/\mathbb{F}_2$. To any element $\gamma \in \mathbb{F}_{q^2}$ we attach the element $(\gamma_1, \gamma_2, \cdots, \gamma_l) \in \mathbb{F}_2^l$ defined by $\gamma = \sum_{i=1}^{l} \gamma_i a_i$. We begin by ordering the coordinates of C_m according to

$$\mathrm{Ind}\,(P_{\alpha,\beta}) = q\sum_{i=1}^{l}\alpha_i 2^{i-1} + \sum_{i=1}^{l/2}\beta_i 2^{i-1} + 1.$$

Note that for any $\alpha \in \mathbb{F}_{q^2}$, the set of solutions of $T^q + T = \alpha^{q+1}$ in $\mathbb{F}_{q^2}$ is $\beta_0 + \mathbb{F}_q$ for some $\beta_0 \in \mathbb{F}_{q^2}$ with $\beta_0^q + \beta_0 = \alpha^{q+1}$. Hence, the above choice of a basis for $\mathbb{F}_{q^2}/\mathbb{F}_2$ assures that the first $l/2$ bits in the representations of two different solutions of $T^q + T = \alpha^{q+1}$ are not identical. The existence of the automorphism corresponding to $\epsilon = 1$, δ with $\delta_l = 1$ and $\delta_j = 0$ for $1 \le j < l$, and some μ with $\mu^q + \mu = \delta^{q+1}$, implies that we can permute the last $q^3/2$ coordinates of the code so that both

$${C_m}^{(q^3/2)-} = {C_m}^{(q^3/2)+}$$

and

$$({C_m}_{(q^3/2)_-})^{(q^3/2)-} = ({C_m}_{(q^3/2)_+})^{(q^3/2)+}.$$

Hence, there is a coordinate ordering under which C_m admits a twisted squaring construction , and this coordinate ordering differs from the initial coordinate ordering only in the last $q^3/2$ coordinates. The existence of the automorphism corresponding to $\epsilon = 1$, δ with $\delta_{l-1} = 1$ and $\delta_j = 0$ for $1 \le j \le l, j \ne l-1$, and some μ with $\mu^q + \mu = \delta^{q+1}$, implies that we can permute the last $q^3/4$ coordinates of the component codes so that they admit a twisted squaring construction . Continuing in that way until $\delta_1 = 1$ and $\delta_j = 0$ for $1 < j \le l$, it is proved that the twisted squaring construction of C_m can be iterated l times. As C_m is of length $q^3 = 2^{l+l/2}$, we still have to show that the twisted squaring construction of C_m can be further iterated $l/2$ times. Observe that when $\delta = 0$, μ can take any value from $\mathbb{F}_q$. For $1 \le i \le l/2$, the existence of the automorphisms corresponding to $\epsilon = 1$, $\delta = 0$, and μ with $\mu_i = 1$ and $\mu_j = 0$ for $j \ne i$, $1 \le j \le l$ completes the proof, since, under the above defined coordinate ordering, these automorphisms show that all the relevant component codes are *symmetric*, and hence admit a twisted squaring construction [2, Theorem 3]. □

REFERENCES

[1] Y. Berger and Y. Be'ery, "Bounds on the trellis size of linear block codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 203–209, Jan. 1993.

[2] ——, "The twisted squaring construction, trellis complexity, and generalized weights of BCH and QR codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1817–1827, Nov. 1996.

[3] G. D. Forney Jr., "Coset codes—Part II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152–1187, Sept. 1988.

[4] ——, "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1741–1752, Nov. 1994.

[5] F. R. Kschischang and V. Sorokine, "On the trellis structure of block codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1924–1937, Nov. 1995.

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[7] R. J. McEliece, "On the BCJR trellis for linear block codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1072–1092, July 1996.

[8] C. Munuera, "On the generalized Hamming weights of geometric Goppa codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 2092–2099, Nov. 1994.

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

[10] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 242–245, Jan. 1993.

[11] ——, "On complexity of trellis structure of linear block codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1057–1064, May 1993.

[12] H. Stichtenoth, "A note on Hermitian codes over GF (q^2)," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1345–1348, Sept. 1988.

[13] ——, "Self-dual Goppa codes," *J. Pure Appl. Math.*, vol. 55, pp. 199–211, 1988.

[14] ——, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 1993.

[15] A. Vardy, "Trellis structure of codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, Dec. 1998.

[16] A. Vardy and Y. Be'ery, "Maximum-likelihood soft decision decoding of BCH codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 546–554, Mar. 1994.

[17] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1412–1418, Sept. 1991.

[18] J. K. Wolf, "Efficient maximum likelihood decoding of linear block codes using a trellis," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 76–80, Jan. 1978.

[19] T. Yaghoobian and I. F. Blake, "Hermitian codes as generalized Reed-Solomon codes," *Des., Codes, Cryptogr.*, vol. 2, pp. 5–17, 1992.

[20] K. Yang, P. V. Kumar, and H. Stichtenoth, "On the weight hierarchy of geometric Goppa codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 913–920, May 1994.

A Class of Linear Codes with Good Parameters from Algebraic Curves

Chaoping Xing and San Ling

***Abstract*—A class of linear codes with good parameters is constructed in this correspondence. It turns out that linear codes of this class are subcodes of the subfield subcodes of Goppa's geometry codes. In particular, we find 61 improvements on Brouwer's table [1] based on our codes.**

***Index Terms*—Algebraic curves, algebraic-geometry codes, subfield subcodes.**

I. INTRODUCTION

Algebraic-geometry codes constructed by Goppa [2] make use of algebraic curves with many rational points. These codes have excellent asymptotic parameters. In particular, the q-ary Gilbert–Varshamov bound was broken by Goppa's geometric codes for some sufficiently large q [8], [3].

However, for small q, it seems difficult to find many good codes by Goppa's construction. The reason is that the number of rational points of an algebraic curve over $\boldsymbol{F}_q$ is not satisfactory to construct good Goppa's geometric codes for small q. In order to increase the length of geometric codes, researchers have been looking for possibilities to use points over some extensions of $\boldsymbol{F}_q$ to construct good codes [5], [10], [11], [4], [12]. In this correspondence, we make use of curves

Manuscript received July 23, 1999; revised February 14, 2000. This work was supported under the NUS Grant R-146-000-018-112.

The authors are with the Department of Mathematics, National University of Singapore, Singapore 117543 (e-mail: xingcp@math.nus.edu.sg; matlings@math.nus.edu.sg).

Communicated by I. F. Blake, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(00)05020-3.

0018–9448/00$10.00 © 2000 IEEE