Quantum Convolutional Codes Derived from Generalized Reed-Solomon Codes

Salah A. Aly, Andreas Klappenecker, Pradeep Kiran Sarvepalli
Department of Computer Science, Texas A&M University
College Station, TX 77843-3112, USA
Email: {salah, klappi, pradeep}@cs.tamu.edu

***Abstract*— Convolutional stabilizer codes promise to make quantum communication more reliable with attractive online encoding and decoding algorithms. This paper introduces a new approach to convolutional stabilizer codes based on direct limit constructions. A quantum Singleton bound for pure convolutional stabilizer codes is given. A familiy of quantum convolutional codes is derived from generalized Reed-Solomon codes. These codes are shown to be optimal with respect to the (quantum) Singleton bound.**

I. Introduction

A key obstacle to the communication of quantum information is decoherence, the spontaneous interaction of the environment with the information-carrying quantum system. The protection of quantum information with quantum error-correcting codes to reduce or perhaps nearly eliminate the impact of decoherence has led to a highly developed theory of quantum error-correcting block codes. Somewhat surprisingly, quantum convolutional codes have received less attention.

Ollivier and Tillich developed the stabilizer framework for quantum convolutional codes, and addressed encoding and decoding aspects of such codes [11], [12]. Almedia and Palazzo constructed a concatenated convolutional code of rate $1/4$ with memory $m = 3$ [1]. Forney and Guha constructed quantum convolutional codes with rate $1/3$ [3]. Also, in a joint work with Grassl, they derived rate $(n-2)/n$ convolutional stabilizer codes [2]. Grassl and Rötteler constructed quantum convolutional codes from product codes [6], and they gave a general algorithm to obtain non-catastrophic encoders [5].

In this paper, we give a new approach to quantum convolutional codes based on a direct limit construction, generalize some of the previously known results. We prove a Singleton bound for pure convolutional stabilizer codes. We construct a family of quantum convolutional codes based on classical generalized Reed-Solomon codes. The quantum convolutional codes derived from the generalized Reed-Solomon codes are shown to be optimal.

II. Background

In this section, we give some background concerning classical convolutional codes, following [7, Chapter 14] and [10].

Let $\mathbf{F}_q$ denote a finite field with q elements. An $(n, k, \delta)_q$ *convolutional code* C is a submodule of $\mathbf{F}_q[D]^n$ generated by a right-invertible matrix $G(D) = (g_{ij}) \in \mathbf{F}_q[D]^{k\times n}$,

$$C = \{\mathbf{u}(D)G(D) \mid \mathbf{u}(D) \in \mathbf{F}_q[D]^k\}, \qquad (1)$$

such that $\sum_{i=1}^k \nu_i = \max\{\deg\gamma \mid \gamma \text{ is a } k\text{-minor of } G(D)\} =: \delta$, where $\nu_i = \max_{1\le j\le n}\{\deg g_{ij}\}$. We say δ is the *degree* of C. The *memory* μ of $G(D)$ is defined as $\mu = \max_{1\le i\le k}\nu_i$. The *weight* $\operatorname{wt}(v(D))$ of a polynomial $v(D)$ in $\mathbf{F}_q[D]$ is defined as the number of nonzero coefficients of $v(D)$, and the *weight* of an element $\mathbf{u}(D) \in \mathbf{F}_q[D]^n$ is defined as $\operatorname{wt}(\mathbf{u}(D)) = \sum_{i=1}^n \operatorname{wt}(u_i(D))$. The *free distance* d_f of C is defined as $d_f = \operatorname{wt}(C) = \min\{\operatorname{wt}(u) \mid u \in C, u \neq 0\}$. We say that an $(n, k, \delta)_q$ convolutional code with memory μ and free distance d_f is an $(n, k, \delta; \mu, d_f)_q$ convolutional code.

Let $\mathbf{N}$ denote the set of nonnegative integers. Let $\Gamma_q = \{v\colon \mathbf{N} \to \mathbf{F}_q \mid \text{ all but finitely many coefficients of } v \text{ are } 0\}$. We can view $v \in \Gamma_q$ as a sequence $\{v_i = v(i)\}_{i\ge 0}$ of finite support. We define a vector space isomorphism $\sigma\colon \mathbf{F}_q[D]^n \to \Gamma_q$ that maps an element $\mathbf{u}(D) = (u_1(D), \dots, u_n(D))$ in $\mathbf{F}_q[D]^n$ to the coefficient sequence of the polynomial $\sum_{i=0}^{n-1} D^i u_i(D^n)$, that is, an element in $\mathbf{F}_q[D]^n$ is mapped to its interleaved coefficient sequence. Frequently, we will refer to the image $\sigma(C) = \{\sigma(c) \mid c \in C\}$ of a convolutional code (1) again as C, as it will be clear from the context whether we discuss the sequence or polynomial form of the code. Let $G(D) = G_0 + G_1D + \cdots + G_\mu D^\mu$, where $G_i \in \mathbf{F}_q^{k\times n}$ for $0 \le i \le \mu$. We can associate to the generator matrix $G(D)$ its semi-infinite coefficient matrix

$$G = \begin{pmatrix} G_0 & G_1 & \cdots & G_\mu & & \\ & G_0 & G_1 & \cdots & G_\mu & \\ & & \ddots & \ddots & & \ddots \end{pmatrix}. \qquad (2)$$

If $G(D)$ is the generator matrix of a convolutional code C, then one easily checks that $\sigma(C) = \Gamma_q G$.

In the literature, convolutional codes are often defined in the form $\{p(D)G'(D) \mid p(D) \in \mathbf{F}_q(D)^k\}$, where $G'(D)$ is a matrix of full rank in $\mathbf{F}_q^{k\times n}[D]$. In this case, one can obtain a generator matrix $G(D)$ in our sense by multiplying $G'(D)$ from the left with a suitable invertible matrix $U(D)$ in $\mathbf{F}_q^{k\times k}(D)$, see [7].

We define the *Euclidean inner product* of two sequences u and v in Γ_q by $\langle u \mid v\rangle = \sum_{i\in\mathbf{N}} u_iv_i$, and the Euclidean dual of a convolutional code $C \subseteq \Gamma_q$ by $C^\perp = \{u \in \Gamma_q \mid \langle u \mid v\rangle = 0 \text{ for all } v \in C\}$. A convolutional code C is called self-orthogonal if and only if $C \subseteq C^\perp$. It is easy to see that a convolutional code C is self-orthogonal if and only if $GG^T = 0$.

1-4244-1429-6/07/$25.00 ©2007 IEEE

Consider the finite field $\mathbf{F}_{q^2}$. The *Hermitian inner product* of two sequences u and v in Γ_{q^2} is defined as $\langle u\,|\,v\rangle_h = \sum_{i\in\mathbf{N}} u_i\, v_i^q$. We have $C^{\perp_h} = \{u \in \Gamma_{q^2}\,|\,\langle u\,|\,v\rangle_h = 0 \text{ for all } v\in C\}$. Then, $C\subseteq C^{\perp_h}$ if and only if $GG^\dagger = 0$, where the Hermitian transpose $\dagger$ is defined as $(a_{ij})^\dagger = (a_{ji}^q)$.

III. Quantum Convolutional Codes

The state space of a q-ary quantum digit is given by the complex vector space $\mathbf{C}^q$. Let $\{|x\rangle\,|\,x\in\mathbf{F}_q\}$ denote a fixed orthonormal basis of $\mathbf{C}^q$, called the computational basis. For $a,b\in\mathbf{F}_q$, we define the unitary operators

$$X(a)|x\rangle = |x+a\rangle \text{ and } Z(b)|x\rangle = \exp(2\pi i\,\mathrm{tr}(bx)/p)|x\rangle,$$

where the addition is in $\mathbf{F}_q$, p is the characteristic of $\mathbf{F}_q$, and $\mathrm{tr}(x) = x^p + x^{p^2} + \cdots + x^q$ is the absolute trace from $\mathbf{F}_q$ to $\mathbf{F}_p$. The set $\mathcal{E} = \{X(a), Z(b)\,|\,a,b\in\mathbf{F}_q\}$ is a basis of the algebra of $q\times q$ matrices, called the *error basis*.

A quantum convolutional code encodes a stream of quantum digits. One does not know in advance how many qudits *i.e.*, quantum digits will be sent, so the idea is to impose structure on the code that simplifies online encoding and decoding. Let n, m be positive integers. We will process $n+m$ qudits at a time, m qudits will overlap from one step to the next, and n qudits will be output.

For each t in $\mathbf{N}$, we define the Pauli group $P_t = \langle M | M \in \mathcal{E}^{\otimes (t+1)n+m}\rangle$ as the group generated by the $(t+1)n+m$-fold tensor product of the error basis $\mathcal{E}$. Let $I = X(0)$ be the $q\times q$ identity matrix. For $i,j\in\mathbf{N}$ and $i\le j$, we define the inclusion homomorphism $\iota_{ij}\colon P_i\to P_j$ by $\iota_{ij}(M) = M\otimes I^{\otimes n(j-i)}$. We have $\iota_{ii}(M) = M$ and $\iota_{ik} = \iota_{jk}\circ\iota_{ij}$ for $i\le j\le k$. Therefore, there exists a group

$$P_\infty = \varinjlim (P_i, \iota_{ij}),$$

called the direct limit of the groups P_i over the totally ordered set $(\mathbf{N},\le)$. For each nonnegative integer i, there exists a homomorphism $\iota_i\colon P_i\to P_\infty$ given by $\iota_i(M_i) = M_i\otimes I^{\otimes\infty}$ for $M_i\in P_i$, and $\iota_i = \iota_j\circ\iota_{ij}$ holds for all $i\le j$. We have $P_\infty = \bigcup_{i=0}^\infty \iota_i(P_i)$; put differently, P_∞ consists of all infinite tensor products of matrices in $\langle M\,|\,M\in\mathcal{E}\rangle$ such that all but finitely many tensor components are equal to I. The direct limit structure that we introduce here provides the proper conceptual framework for the definition of convolutional stabilizer codes; see [14] for background on direct limits.

We will define the stabilizer of the quantum convolutional code also through a direct limit. Let S_0 be an abelian subgroup of P_0. For positive integers t, we recursively define a subgroup S_t of P_t by $S_t = \langle N\otimes I^{\otimes n}, I^{\otimes tn}\otimes M\,|\,N\in S_{t-1}, M\in S_0\rangle$. Let Z_t denote the center of the group P_t. We will assume that

S1) $I^{\otimes tn}\otimes M$ and $N\otimes I^{\otimes tn}$ commute for all $N,M\in S_0$ and all positive integers t.

S2) S_tZ_t/Z_t is an $(t+1)(n-k)$-dimensional vector space over $\mathbf{F}_q$.

S3) $S_t\cap Z_t$ contains only the identity matrix.

Assumption **S1** ensures that S_t is an *abelian* subgroup of P_t, **S2** implies that S_t is generated by $t+1$ shifted versions of $n-k$ generators of S_0 and all these $(t+1)(n-k)$ generators are independent, and **S3** ensures that the stabilizer (or $+1$ eigenspace) of S_t is nontrivial as long as $k<n$.

The abelian subgroups S_t of P_t define an abelian group

$$S = \varinjlim (S_i,\iota_{ij}) = \langle \iota_t(I^{\otimes tn}\otimes M)\,|\,t\ge 0, M\in S_0\rangle$$

generated by shifted versions of elements in S_0.

Definition 1: Suppose that an abelian subgroup S_0 of P_0 is chosen such that **S1**, **S2**, and **S3** are satisfied. Then the $+1$-eigenspace of $S = \varinjlim(S_i,\iota_{ij})$ in $\bigotimes_{i=0}^\infty \mathbf{C}^q$ defines an $\mathbf{F}_q$-linear convolutional stabilizer code with parameters $[(n,k,m)]_q$.
If S_tZ_t/Z_t was also a $(t+1)(n-k)/2$ dimensional vector space over $\mathbf{F}_{q^2}$, then we have an $\mathbf{F}_{q^2}$-linear quantum code.

We notice that the rate k/n of the quantum convolutional stabilizer code defined by S is approached by the rate of the stabilizer block code S_t for large t. Indeed, S_t defines a stabilizer code with parameters $[[(t+1)n+m,(t+1)k+m]]_q$; therefore, the rates of these stabilizer block codes approach

$$\lim_{t\to\infty}\frac{(t+1)k+m}{(t+1)n+m} = \lim_{t\to\infty}\frac{k+m/(t+1)}{n+m/(t+1)} = \frac{k}{n}.$$

We say that an error E in P_∞ is *detectable* by a convolutional stabilizer code with stabilizer S if and only if a scalar multiple of E is contained in S or if E does not commute with some element in S. The *weight* wt of an element in P_∞ is defined as its number of non-identity tensor components. A quantum convolutional stabilizer code is said to have *free distance* d_f if and only if it can detect all errors of weight less than d_f, but cannot detect some error of weight d_f. Denote by $Z(P_\infty)$ the center of P_∞ and by $C_{P_\infty}(S)$ the centralizer of S in P_∞. Then the free distance is given by $d_f = \min\{\mathrm{wt}(e)\,|\,e\in C_{P_\infty}(S)\setminus Z(P_\infty)S\}$.

Let (β,β^q) denote a normal basis of $\mathbf{F}_{q^2}/\mathbf{F}_q$. Define a map $\tau\colon P_\infty\to\Gamma_{q^2}$ by $\tau(\omega^c X(a_0)Z(b_0)\otimes X(a_1)Z(b_1)\otimes\cdots) = (\beta a_0+\beta^q b_0, \beta a_1+\beta^q b_1,\dots)$, where $\omega = e^{2\pi i/p}$. Since Z_t consists of $\omega^c I$, for an $\mathbf{F}_{q^2}$-linear quantum code **S2** implies that $\tau(S_tZ_t/Z_t)$ is $(n-k)/2$-dimensional over $\mathbf{F}_{q^2}$. For sequences v and w in Γ_{q^2}, we define a trace-alternating form

$$\langle v\,|\,w\rangle_a = \mathrm{tr}_{q/p}\left(\frac{v\cdot w^q - v^q\cdot w}{\beta^{2q}-\beta^2}\right).$$

Lemma 2: Let A and B be elements of P_∞. Then A and B commute if and only if $\langle\tau(A)\,|\,\tau(B)\rangle_a = 0$.

Proof: This follows from [9] and the direct limit structure. ■

Lemma 3: Let Q be an $\mathbf{F}_{q^2}$-linear $[(n,k,m)]_q$ quantum convolutional code with stabilizer S, where $S = \varinjlim(S_i,\iota_{ij})$ and S_0 an abelian subgroup of P_0 such that **S1**, **S2**, and **S3** hold. Then $C = \sigma^{-1}\tau(S)$ is an $\mathbf{F}_{q^2}$-linear $(n,(n-k)/2;\mu\le\lceil m/n\rceil)_{q^2}$ convolutional code generated by $\sigma^{-1}\tau(S_0)$. Further, $C\subseteq C^{\perp_h}$.

Proof: Recall that $\sigma:\mathbf{F}_{q^2}[D]^n\to\Gamma_{q^2}$, maps $u(D)$ in $\mathbf{F}_{q^2}[D]^n$ to $\sum_{i=0}^{n-1} D^i u_i(D^n)$. It is invertible, thus $\sigma^{-1}\tau(e) = \sigma^{-1}\circ\tau(e)$ is well defined for any e in P_∞. Since S is generated by shifted versions of S_0, it follows that $C =$

$\sigma^{-1}\tau(S)$ is generated as the $\mathbf{F}_{q^2}$ span of $\sigma^{-1}\tau(S_0)$ and its shifts, *i.e.*, $D^l\sigma^{-1}\tau(S_0)$, where $l \in \mathbf{N}$. Since Q is an $\mathbf{F}_{q^2}$-linear $[(n,k,m)]_q$ quantum convolutional code, $\tau(S_0)$ is $(n-k)/2$ dimensional over $\mathbf{F}_{q^2}$. The linearity of σ implies that $\sigma^{-1}\tau(S_0)$ is also $(n-k)/2$ dimensional. As $\sigma^{-1}\tau(e)$ is in $\mathbf{F}_{q^2}[D]^n$ we can define an $(n-k)/2\times n$ polynomial generator matrix that generates C. This generator matrix need not be right invertible, but we know that there exists a right invertible polynomial generator matrix that generates this code. Thus C is an $(n,(n-k)/2;\mu)_{q^2}$ code. Since S is abelian, Lemma 2 and the $\mathbf{F}_{q^2}$-linearity of S imply that $C \subseteq C^{\perp_h}$. Finally, observe that maximum degree of an element in $\sigma^{-1}\tau(S_0)$ is $\lceil m/n\rceil$ owing to σ. Together with [7, Lemma 14.3.8] this implies that the memory of $\sigma^{-1}\tau(S)$ must be $\mu \leq \lceil m/n\rceil$. ∎

We define the degree of an $\mathbf{F}_{q^2}$-linear $[(n,k,m)]_q$ quantum convolutional code Q with stabilizer S as the degree of the classical convolutional code $\sigma^{-1}\tau(S)$. We denote an $[(n,k,m)]_q$ quantum convolutional code with free distance d_f and total constraint length δ as $[(n,k,m;\delta,d_f)]_q$. It must be pointed out this notation is at variance with the classical codes in not just the order but the meaning of the parameters.

Corollary 4: An $\mathbf{F}_{q^2}$-linear $[(n,k,m;\delta,d_f)]_q$ convolutional stabilizer code implies the existence of an $(n,(n-k)/2,\delta)_{q^2}$ convolutional code C such that $d_f = \mathrm{wt}(C^{\perp_h}\setminus C)$.

Proof: As before let $C = \sigma^{-1}\tau(S)$, by Lemma 2 we can conclude that $\sigma^{-1}\tau(C_{P_\infty}(S)) \subseteq C^{\perp_h}$. Thus an undetectable error is mapped to an element in $C^{\perp_h}\setminus C$. While τ is injective on S it is not the case with $C_{P_\infty}(S)$. However we can see that if c is in $C^{\perp_h}\setminus C$, then surjectivity of τ (on $C_{P_\infty}(S)$) implies that there exists an error e in $C_{P_\infty}(S)\setminus Z(P_\infty)S$ such that $\tau(e) = \sigma(c)$. As τ and σ are isometric e is an undetectable error with $\mathrm{wt}(c)$. Hence, we can conclude that $d_f = \mathrm{wt}(C^{\perp_h}\setminus C)$. Combining with Lemma 3 we have the claim stated. ∎

An $[(n,k,m;\delta,d_f)]_q$ code is said to be a *pure code* if there are no errors of weight less than d_f in the stabilizer of the code. In this case, Corollary 4 implies that $d_f = \mathrm{wt}(C^{\perp_h}\setminus C) = \mathrm{wt}(C^{\perp_h})$.

Theorem 5: Let C be $(n,(n-k)/2,\delta;\mu)_{q^2}$ convolutional code such that $C \subseteq C^{\perp_h}$. Then there exists an $[(n,k,n\mu;\delta,d_f)]_q$ convolutional stabilizer code, where $d_f = \mathrm{wt}(C^{\perp_h}\setminus C)$. The code is pure if $d_f = \mathrm{wt}(C^{\perp_h})$.

Proof: [Sketch] Let $G(D)$ be the polynomial generator matrix of C, with the semi-infinite generator matrix G defined as in equation (2). Let $C_t = \langle\sigma(G(D)),\ldots,\sigma(D^tG(D))\rangle = \langle C_{t-1},\sigma(D^tG(D))\rangle$, where σ is applied to every row in $G(D)$. The self-orthogonality of C implies that C_t is also self-orthogonal. In particular C_0 defines an $[n+n\mu,(n-k)/2]_{q^2}$ self-orthogonal code. From the theory of stabilizer codes we know that there exists an abelian subgroup $S_0 \leq P_0$ such that $\tau(S_0) = C_0$, where P_t is the Pauli group over $(t+1)n+m$ qudits; in this case $m = n\mu$. This implies that $\tau(I^{\otimes nt}\otimes S_0) = \sigma(D^tG(D))$. Define $S_t = \langle S_{t-1}, I^{\otimes nt}\otimes S_0\rangle$, then $\tau(S_t) = \langle\tau(S_{t-1},\sigma(D^tG(D))\rangle$. Proceeding recursively, we see that $\tau(S_t) = \langle\sigma(G(D)),\ldots,\sigma(D^tG(D))\rangle = C_t$. By Lemma 2, the self-orthogonality of C_t implies that S_t is abelian, thus **S1** holds. Note that $\tau(S_tZ_t/Z_t) = C_t$, where Z_t is the center of P_t. Combining this with $\mathbf{F}_{q^2}$-linearity of C_t implies that S_tZ_t/Z_t is a $(t+1)(n-k)$ dimensional vector space over F_q; hence **S2** holds. For **S3**, assume that $z \neq \{1\}$ is in $S_t\cap Z_t$. Then z can be expressed as a linear combination of the generators of S_t. But $\tau(z) = 0$ implying that the generators of S_t are dependent. Thus $S_t\cap Z_t = \{1\}$ and **S3** also holds. Thus $S = \varinjlim(S_t,\iota_{tj})$ defines an $[(n,k,n\mu;\delta)]_q$ convolutional stabilizer code. By definition the degree of the quantum code is the degree of the underlying classical code. As $\sigma^{-1}\tau(S) = C$, arguing as in Corollary 4 we can show that $\sigma^{-1}\tau(C_{P_\infty}(S)) = C^{\perp_h}$ and $d_f = \mathrm{wt}(C^{\perp_h}\setminus C)$. ∎

Corollary 6: Let C be an $(n,(n-k)/2,\delta;\mu)_q$ code such that $C \subseteq C^\perp$. Then there exists an $[(n,k,n\mu;\delta,d_f)]_q$ code with $d_f = \mathrm{wt}(C^\perp\setminus C)$. It is pure if $\mathrm{wt}(C^\perp\setminus C) = \mathrm{wt}(C^\perp)$.

Proof: Since $C \subseteq C^\perp$, its generator matrix G as in equation (2) satisfies $GG^T = 0$. We can obtain an $\mathbf{F}_{q^2}$-linear $(n, l = (n-k)/2,\delta;\mu)_{q^2}$ code, C' from G as $C' = \Gamma_{q^2}G$. Since $G_i \in \mathbf{F}_q^{l\times n}$, we have $GG^\dagger = GG^T = 0$. Thus $C' \subseteq C'^{\perp_h}$. Further, it can checked that $\mathrm{wt}(C'^{\perp_h}\setminus C') = \mathrm{wt}(C^\perp\setminus C)$. The claim follows from Theorem 5. ∎

Theorem 7 (Singleton bound): The free distance of an $[(n,k,m;\delta,d_f)]_q$ $\mathbf{F}_{q^2}$-linear pure convolutional stabilizer code is bounded by

$$d_f \quad\leq\quad \frac{n-k}{2}\left(\left\lfloor\frac{2\delta}{n+k}\right\rfloor+1\right)+\delta+1$$

Proof: By Corollary 4, there exists an $(n,(n-k)/2,\delta)_{q^2}$ code C such that $\mathrm{wt}(C^{\perp_h}\setminus C) = d_f$, and the purity of the code implies that $\mathrm{wt}(C^{\perp_h}) = d_f$. The dual code $C^\perp$ or $C^{\perp_h}$ has the same degree as code [8, Theorem 2.66]. Thus, $C^{\perp_h}$ is an $(n,(n+k)/2,\delta)_{q^2}$ convolutional code with free distance d_f. By the generalized Singleton bound [15, Theorem 2.4] for classical convolutional codes, we have

$$d_f \quad\leq\quad (n-(n+k)/2)\left(\left\lfloor\frac{\delta}{(n+k)/2}\right\rfloor+1\right)+\delta+1,$$

which implies the claim. ∎

IV. Convolutional GRS Stabilizer Codes

In this section we will use Piret's construction of Reed-Solomon convolutional codes [13] to derive quantum convolutional codes. Let $\alpha \in \mathbf{F}_{q^2}$ be a primitive nth root of unity, where $n|q^2-1$. Let $w = (w_0,\ldots,w_{n-1})$, $\gamma = (\gamma_0,\ldots,\gamma_{n-1})$ be in $\mathbf{F}_{q^2}^n$ where $w_i \neq 0$ and all $\gamma_i \neq 0$ are distinct. Then the generalized Reed-Solomon (GRS) code over $\mathbf{F}_{q^2}^n$ is the code with the parity check matrix, (cf. [7, pages 175–178])

$$H_{\gamma,w} = \left[\begin{array}{llll} w_0 & w_1 & \cdots & w_{n-1} \\ w_0\gamma_0 & w_1\gamma_1 & \cdots & w_{n-1}\gamma_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ w_0\gamma_0^{t-1} & w_1\gamma_1^{2(t-1)} & \cdots & w_{n-1}\gamma_{n-1}^{(t-1)(n-1)} \end{array}\right].$$

The code is denoted by $\mathrm{GRS}_{n-t}(\gamma,v)$, as its generator matrix is of the form $H_{\gamma,v}$ for some $v \in \mathbf{F}_{q^2}^n$. It is an $[n,n-t,t+1]_{q^2}$ MDS code [7, Theorem 5.3.1]. If we choose $w_i = \alpha^i$, then $w_i \neq 0$. If $\gcd(n,2) = 1$, then α^2 is also a primitive nth root of unity; thus $\gamma_i = \alpha^{2i}$ are all distinct and we have an

$[n, n-t, t+1]_{q^2}$ GRS code with parity check matrix H_0, where

$$H_0 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t-1} & \alpha^{2(2t-1)} & \cdots & \alpha^{(2t-1)(n-1)} \end{bmatrix}.$$

Similarly if $w_i = \alpha^{-i}$ and $\gamma_i = \alpha^{-2i}$, then we have another $[n, n-t, t+1]_{q^2}$ GRS code with parity check matrix

$$H_1 = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(n-1)} \\ 1 & \alpha^{-3} & \alpha^{-6} & \cdots & \alpha^{-3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{-(2t-1)} & \alpha^{-2(2t-1)} & \cdots & \alpha^{-(2t-1)(n-1)} \end{bmatrix}.$$

The $[n, n-2t, 2t+1]_{q^2}$ GRS code with $w_i = \alpha^{-i(2t-1)}$ and $\gamma_i = \alpha^{2i}$ has a parity check matrix H^* that is equivalent to $\left[\begin{smallmatrix} H_0 \\ H_1 \end{smallmatrix}\right]$ up to a permutation of rows.

Our goal is to show that under certain restrictions on n the following semi-infinite coefficient matrix H determines an $\mathbf{F}_{q^2}$-linear Hermitian self-orthogonal convolutional code

$$H = \begin{bmatrix} H_0 & H_1 & 0 & \cdots & \cdots \\ 0 & H_0 & H_1 & 0 & \cdots \\ \vdots & \vdots & \vdots & \cdots & \ddots \end{bmatrix}. \qquad (3)$$

To show that H is Hermitian self-orthogonal, it is sufficient to show that H_0, H_1 are both self-orthogonal and H_0 and H_1 are orthogonal to each other. A portion of this result is contained in [4, Lemma 8], *viz.*, $n = q^2 - 1$. We will prove a slightly stronger result.

Lemma 8: Let $n | q^2 - 1$ such that $q + 1 < n \leq q^2 - 1$ and $2 \leq \mu = 2t \leq \lfloor n/(q+1) \rfloor$, then

$$\overline{H}_0 = (\alpha^{ij})_{1 \leq i < \mu, 0 \leq j < n} \quad \text{and} \quad \overline{H}_1 = (\alpha^{-ij})_{1 \leq i < \mu, 0 \leq j < n}$$

are self-orthogonal with respect to the Hermitian inner product. Further, $\overline{H}_0$ is orthogonal to $\overline{H}_1$.

Proof: Denote by $\overline{H}_{0,j} = (1, \alpha^j, \alpha^{2j}, \cdots, \alpha^{j(n-1)})$ and $\overline{H}_{1,j} = (1, \alpha^{-j}, \alpha^{-2j}, \cdots, \alpha^{-j(n-1)})$, where $1 \leq j \leq \mu - 1$. The Hermitian inner product of $\overline{H}_{0,i}$ and $\overline{H}_{0,j}$ is given by

$$\langle \overline{H}_{0,i} | \overline{H}_{0,j} \rangle_h = \sum_{l=0}^{n-1} \alpha^{il} \alpha^{jql} = \frac{\alpha^{(i+jq)n} - 1}{\alpha^{i+jq} - 1},$$

which vanishes if $i + jq \not\equiv 0 \mod n$. If $1 \leq i, j \leq \mu - 1 = \lfloor n/(q+1) \rfloor - 1$, then $q + 1 \leq i + jq \leq (q+1) \lfloor n/(q+1) \rfloor - (q+1) < n$; hence, $\langle \overline{H}_{0,i} | \overline{H}_{0,j} \rangle_h = 0$. Thus, $\overline{H}_0$ is self-orthogonal. Similarly, $\overline{H}_1$ is also self-orthogonal. Furthermore,

$$\langle \overline{H}_{0,i} | \overline{H}_{1,j} \rangle_h = \sum_{l=0}^{n-1} \alpha^{il} \alpha^{-jql} = \frac{\alpha^{(i-jq)n} - 1}{\alpha^{i-jq} - 1}.$$

This inner product vanishes if $\alpha^{i-jq} \neq 1$ or, equivalently, if $i - jq \not\equiv 0 \mod n$. Since $1 \leq i, j \leq \lfloor n/(q+1) \rfloor - 1 \leq q - 2$, we have $1 \leq i \leq \lfloor n/(q+1) \rfloor - 1 \leq q - 2$ while $q \leq jq \leq q \lfloor n/(q+1) \rfloor - q < n$. Thus $i \not\equiv jq \mod n$ and this inner product also vanishes, which proves the claim. ■

Since H_i is contained in $\overline{H}_i$, we obtain the following:

Corollary 9: Let $2 \leq \mu = 2t \leq \lfloor n/(q+1) \rfloor$, where $n | q^2 - 1$ and $q + 1 < n \leq q^2 - 1$. Then H_0 and H_1 are Hermitian self-orthogonal. Further, H_0 is orthogonal to H_1 with respect to the Hermitian inner product.

Before we can construct quantum convolutional codes, we need to compute the free distances of C and $C^{\perp_h}$, where C is the convolutional code generated by H.

Lemma 10: Let $2 \leq 2t \leq \lfloor n/(q+1) \rfloor$, where $\gcd(n, 2) = 1$, $n | q^2 - 1$ and $q + 1 < n \leq q^2 - 1$. Then the convolutional code $C = \Gamma_{q^2} H$ has free distance $d_f \geq n - 2t + 1 > 2t + 1 = d_f^\perp$, where $d_f^\perp = \mathrm{wt}(C^{\perp_h})$ is the free distance of $C^{\perp_h}$.

Proof: Since $d_f^\perp = \mathrm{wt}(C^{\perp_h}) = \mathrm{wt}(C^\perp)$, we compute $\mathrm{wt}(C^\perp)$. Let $c = (\ldots, 0, c_0, \ldots, c_l, 0, \ldots)$ be a codeword in $C^\perp$ with $c_i \in \mathbf{F}_{q^2}^n$, $c_0 \neq 0$, and $c_l \neq 0$. It follows from the parity check equations $cH^T = 0$ that $c_0 H_1^T = 0 = c_l H_0^T$ holds. Thus, $\mathrm{wt}(c_0), \mathrm{wt}(c_l) \geq t + 1$. If $l > 0$, then $\mathrm{wt}(c) \geq \mathrm{wt}(c_0) + \mathrm{wt}(c_l) \geq 2t + 2$. If $l = 0$, then c_0 is in the dual of H^*, which is an $[n, n-2t, 2t+1]_{q^2}$ code. Thus $\mathrm{wt}(c) = \mathrm{wt}(c_0) \geq 2t + 1$ and $d_f^\perp \geq 2t + 1$. But if c_x is in the dual of H^*, then $(\ldots, 0, c_x, 0, \ldots)$ is a codeword of C. Thus $d_f^\perp = 2t + 1$.

Let $(\ldots, c_{i-1}, c_i, c_{i+1}, \ldots)$ be a nonzero codeword in C. Observing the structure of C, we see that any nonzero c_i must be in the span of H^*. But H^* generates an $[n, 2t, n-2t+1]_{q^2}$ code. Hence $d_f \geq n - 2t + 1$. If $2t \leq \lfloor n/(q+1) \rfloor$, then $t \leq n/6$; thus $d_f \geq n - 2t + 1 > 2t + 1 = d_f^\perp$ holds. ■

The preceding proof generalizes [13, Corollary 4] where the free distance of $C^\perp$ was computed for $q = 2^m$.

Theorem 11: Let q be a power of a prime, n an odd divisor of $q^2 - 1$, such that $q + 1 < n \leq q^2 - 1$ and $2 \leq \mu = 2t \leq \lfloor n/(q+1) \rfloor$. Then there exists a pure quantum convolutional code with parameters $[(n, n-\mu, n; \mu/2, \mu+1)]_q$. This code is optimal, since it attains the Singleton bound with equality.

Proof: The convolutional code generated by the coefficient matrix H in equation (3) has parameters $(n, \mu/2, \delta \leq \mu/2; 1, d_f)_{q^2}$. Inspecting the corresponding polynomial generator matrix shows that $\delta \leq \mu/2$, since $\nu_i = 1$ for $1 \leq i \leq \mu/2$. By Corollary 9, this code is Hermitian self-orthogonal; moreover, Lemma 10 shows that the distance of its dual code is given by $d_f^\perp = \mu + 1 < d_f$. By Theorem 5, we can conclude that there exists a pure convolutional stabilizer code with parameters $[(n, n-\mu, n; \delta \leq \mu/2, \mu+1)]_q$. It follows from Theorem 7 that

$$\begin{aligned} \mu + 1 &\leq (\mu/2)\left(\lfloor 2\delta/(2n-\mu) \rfloor + 1\right) + \delta + 1 \\ &\leq (\mu/2)\left(\lfloor \mu/(2n-\mu) \rfloor + 1\right) + \delta + 1. \end{aligned}$$

Since $\lfloor \mu/(2n-\mu) \rfloor = 0$, the right hand side equals $\mu/2 + \delta + 1$, which implies $\delta = \mu/2$ and the optimality of the quantum code. ■

ACKNOWLEDGMENT

Earlier versions of this paper contained a family of quantum convolutional codes derived from Reed-Muller codes. These have been removed after Grassl and Rötteler kindly pointed out that these codes have degree 0. Readers interested in these codes can contact the authors for details. We would like to thank the referees for their suggestions which greatly improved the paper. This research was supported by NSF CAREER award CCF 0347310 and NSF grant CCF 0622201.

References

[1] A. C. A. de Almeida and R. Palazzo Jr. A concatenated [(4, 1, 3)] quantum convolutional code. In *Proc. IEEE Inform. Theory Workshop (San Antonio, TX)*, Oct. 2004.

[2] G. D. Forney Jr., M. Grassl, and S. Guha. Convolutional and tail-biting quasntum error-correcting codes. *IEEE Trans. Inform. Theory*, 52(3):865–880, 2007.

[3] G. D. Forney Jr. and S. Guha. Simple rate-1/3 convolutional and tail-biting quantum error-correcting codes. In *Proc. 2005 IEEE Intl. Symp. on Inform. Theory, Adelaide, Australia*, pages 1028–1032, 2005.

[4] M. Grassl, T. Beth, and M. Rötteler. On optimal quantum codes. *Intl. J. Quantum Information*, 2(1):757–775, 2004.

[5] M. Grassl and M. Rötteler. Non-catastrophic encoders and encoder inverses for quantum convolutional codes. In *Proc. 2006 IEEE Intl. Symp. on Inform. Theory, Seattle, WA, USA*, pages 1109–1113, 2006.

[6] M. Grassl and M. Rötteler. Quantum block and convolutional codes from self-orthogonal product codes. In *Proc. 2005 IEEE Intl. Symp. on Inform. Theory, Adelaide, Australia*, pages 1018–1022, Sept. 2005.

[7] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. University Press, Cambridge, 2003.

[8] R. Johannesson and K. Sh. Zigangirov. *Fundamentals of Convolutional coding*. Digital and Mobile Communication, Wiley-IEEE Press, 1999.

[9] A. Ketkar, A. Klappenecker, S. Kumar, and P.K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, November, 2006.

[10] K. Lally. Algebraic lower bounds on the free distance of convolutional codes. *IEEE Trans. Inform. Theory*, 52(5):2101–2110, 2006.

[11] H. Ollivier and J.-P. Tillich. Description of a quantum convolutional code. *Phys. Rev. Lett.*, 91(17):1779021–4, 2003.

[12] H. Ollivier and J.-P. Tillich. Quantum convolutional codes: Fundamentals. ArXiv:quant-ph/0401134, 2004.

[13] Ph. Piret. A convolutional equivalent to Reed-Solomon codes. *Philips J. Res.*, 43:441–458, 1988.

[14] L. Ribes and P. Zalesskii. *Profinite groups*. Springer, 2000.

[15] R. Smarandache, H. Gluesing-Luerssen and J. Rosenthal. Constructions of MDS-convolutional codes. *IEEE Trans. Inform. Theory*, 47(5):2045–2049, 2001.