International Journal of Quantum Information

On optimal quantum codes

Markus Grassl, Thomas Beth
Institut für Algorithmen und Kognitive Systeme,
Universität Karlsruhe, Am Fasanengarten 5, 76 128 Karlsruhe, Germany
grassl@ira.uka.de, EISS_Office@ira.uka.de

Martin Rötteler
Department of Combinatorics and Optimization, Faculty of Mathematics,
University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1
mroetteler@iqc.ca

We present families of quantum error-correcting codes which are optimal in the sense that the minimum distance is maximal. These maximum distance separable (MDS) codes are defined over q-dimensional quantum systems, where q is an arbitrary prime power. It is shown that codes with parameters $[\![n, n-2d+2, d]\!]_q$ exist for all $3 \leq n \leq q$ and $1 \leq d \leq n/2+1$. We also present quantum MDS codes with parameters $[\![q^2, q^2-2d+2, d]\!]_q$ for $1 \leq d \leq q$ which additionally give rise to shortened codes $[\![q^2-s, q^2-2d+2-s, d]\!]_q$ for some s.

Keywords: Quantum error-correcting codes, quantum MDS codes

1. Introduction

In this paper, we consider error-correcting codes for quantum systems which are composed of subsystems of dimension p^m, where p is prime and $m \in \mathbb{N}$. As a shorthand, we will use the term "qudit". In the theory of classical error-correcting codes it is well known that by increasing the size of the underlying alphabet, codes with better parameters can be constructed.[1,2] We will show that the same is true for quantum error-correcting codes.

Quantum codes for qudit systems have been studied before[3,4,5,6] including efficient algorithms for encoding these codes.[7] It is known that codes encoding one qudit into five qudits which are capable to correct one error, denoted by $[\![5, 1, 3]\!]_q$, exist for quantum systems of any dimension.[8] In general, by $[\![n, k, d]\!]_q$ we will denote a quantum error-correcting code (QECC) which encodes k qudits of a q-dimensional quantum system into n qudits. The parameter d is the minimum distance of the code. A QECC with minimum distance d can be used to detect errors that involve

Accepted for publication in the International Journal of Quantum Information.
This work was presented in part at the ERATO Conference on Quantum Information Science (Kyoto, Japan, 2003).

at most $d-1$ of the n subsystems. Alternatively, one can correct errors that involve less than $d/2$ subsystems.

Recently it was shown that optimal quantum codes with parameters $[\![6,2,3]\!]_p$ and $[\![7,3,3]\!]_p$ exist for all primes $p \geq 3$ (see Ref. 9). There also exist quantum codes $[\![p,1,(p+1)/2]\!]_p$ encoding one qudit into many qudits which are capable to correct more than one error.[3] We show that many more optimal quantum codes exist. Note that in this paper we consider only codes of finite length, and not the asymptotic performance of codes when the length tends to infinity (for this, see, e. g., Ref. 6).

First we recall basic constructions of QECCs from classical codes.[5,10,11] Then we present families of optimal classical codes suitable for these constructions. In Section 4 we address the problem of shortening quantum codes and conclude with a table of results.

1.1. *Quantum Codes*

For completeness, we recall some constructions of quantum error-correcting codes from classical ones.

First, on the space $(GF(q) \times GF(q))^n \equiv GF(q)^n \times GF(q)^n$ we consider the symplectic inner product defined by

$$(\boldsymbol{v},\boldsymbol{w}) * (\boldsymbol{v}',\boldsymbol{w}') := \boldsymbol{v}\cdot\boldsymbol{w}' - \boldsymbol{v}'\cdot\boldsymbol{w} = \sum_{i=1}^{n} v_i w_i' - v_i' w_i. \tag{1}$$

For codes over $GF(q)\times GF(q)$ which are $GF(q)$-linear with q^k codewords, denoted by $C = (n, q^k, d)_q$, we use the notation C^* for the dual code with respect to (1), i. e.,

$$C^* := \{(\boldsymbol{v},\boldsymbol{w}) \in GF(q)^n \times GF(q)^n \mid \forall \boldsymbol{c} \in C\colon (\boldsymbol{v},\boldsymbol{w}) * \boldsymbol{c} = 0\}.$$

A code which is contained in its dual is called self-orthogonal. These codes can be used to construct QECCs for qudits:[5]

Theorem 1: Let $C = (n, q^k)_q$ be a self-orthogonal code over $GF(q) \times GF(q)$ with q^k codewords and let $d = \min\{\mathrm{wgt}(\boldsymbol{v})\colon \boldsymbol{v} \in C^* \setminus C\}$. Then there exists a QECC encoding $n-k$ qudits into n qudits with minimum distance d, denoted by $\mathcal{C} = [\![n, n-k, d]\!]_q$.

For $GF(q^2)$-linear codes over $GF(q^2)$ one can also consider duality with respect to the Hermitian inner product on $GF(q^2)^n$, defined by

$$\boldsymbol{v} * \boldsymbol{w} := \sum_{i=1}^{n} v_i w_i^q. \tag{2}$$

Again, classical codes which are self-orthogonal with respect to (2) give rise to QECCs for q-dimensional systems.

Corollary 2: *Let C be a $GF(q^2)$-linear $[n,k]_{q^2}$ self-orthogonal code over $GF(q^2)$ and let $d = \min\{\mathrm{wgt}(\boldsymbol{v})\colon \boldsymbol{v} \in C^* \setminus C\}$. Then there exists a QECC $\mathcal{C} = [\![n, n-2k, d]\!]_q$.*

Proof: From the self-orthogonal code C over $GF(q^2)$ one obtains a self-orthogonal code D over $GF(q)\times GF(q)$ as follows. Let $\gamma \in GF(q^2)\setminus GF(q)$ so that $\gamma^q = -\gamma+\gamma_0$ for some $\gamma_0 \in GF(q)$. Expanding each symbol of $GF(q^2)$ with respect to the basis $\{1,\gamma\}$ of $GF(q^2)/GF(q)$, we can write any element $\boldsymbol{c} \in C$ as $\boldsymbol{v} + \gamma\boldsymbol{w}$ where $\boldsymbol{v},\boldsymbol{w} \in GF(q)^n$. Then the code D is defined as

$$D := \{(\boldsymbol{v},\boldsymbol{w})\colon \boldsymbol{v},\boldsymbol{w} \in GF(q)^n \mid \boldsymbol{v}+\gamma\boldsymbol{w} \in C\}.$$

As C is self-orthogonal with respect to (2), we get

$$\begin{aligned} 0 = \boldsymbol{c} * \boldsymbol{w} &= \sum_{i=1}^n (v_i+\gamma w_i)(v_i'+\gamma w_i')^q \\ &= \sum_{i=1}^n v_i v_i' + \gamma v_i' w_i + \gamma^q v_i w_i' + \gamma^{q+1} w_i w_i' \\ &= \sum_{i=1}^n v_i v_i' + \gamma^{q+1} w_i w_i' + \gamma_0 v_i w_i' + \gamma(v_i' w_i - v_i w_i'). \end{aligned} \tag{3}$$

As γ^{q+1} is the norm of γ and hence $\gamma^{q+1} \in GF(q)$, the coefficient $(v_i'w_i - v_i w_i')$ of γ in (3) vanishes. This implies that D is self-orthogonal with respect to (1). The result follows using Theorem 1 (see also Corollary 1 in Ref. 5). □

Finally, the construction of so-called CSS codes[10,11] uses the notion of duality with respect to the Euclidean inner product

$$\boldsymbol{v}\cdot\boldsymbol{w} := \sum_{i=1}^n v_i w_i, \tag{4}$$

for which the dual code is denoted by $C^\perp$.

Theorem 3: (CSS codes) Let $C_1 = [n,k_1,d_1]_q$ and $C_2 = [n,k_2,d_2]_q$ be linear codes over $GF(q)$ with $C_2^\perp \subseteq C_1$. Furthermore, let $d = \min\{\mathrm{wgt}(\boldsymbol{v})\colon \boldsymbol{v} \in (C_1\setminus C_2^\perp)\cup(C_2\setminus C_1^\perp)\} \geq \min(d_1,d_2)$. Then there exists a QECC $\mathcal{C} = [\![n, k_1+k_2-n, d]\!]_q$.

Proof: It is easy to show that the code $C_1^\perp \times C_2^\perp$ is a self-orthogonal code over $GF(q)\times GF(q)$. Applying Theorem 1 to this code completes the proof. □

In particular, Theorem 3 applies to so-called weakly self-dual codes with $C \subseteq C^\perp$.

Corollary 4: *Let C be an $[n,k]_q$ weakly self-dual code over $GF(q)$ and let $d = \min\{\mathrm{wgt}(\boldsymbol{v})\colon \boldsymbol{v} \in C^\perp\setminus C\}$. Then there exists a QECC $\mathcal{C} = [\![n,n-2k,d]\!]_q$.*

Proof: The results follows setting $C_1^\perp = C_2^\perp = C$ in Theorem 3. Alternatively, one can apply Corollary 2 to the self-orthogonal code $C \otimes GF(q^2)$. □

Before presenting the families of classical error-correcting codes used in our construction, we quote the quantum version of the singleton bound:[12]

Theorem 5: (Quantum Singleton Bound) Let $\mathcal{C} = [\![n,k,d]\!]_q$ be a quantum error-correction code. Then

$$k + 2d \leq n + 2. \tag{5}$$

If equality holds in (5) then $\mathcal{C}$ is pure.

Definition 6: (Quantum MDS code) A quantum code for which equality holds in (5), i. e., $\mathcal{C} = [\![n, n-2d+2, d]\!]_q$, is called a quantum MDS code.

2. Self-orthogonal Classical MDS Codes

Our construction of quantum MDS codes is based on classical MDS codes. Let q be any prime power and let μ, $0 \leq \mu < q-2$, be an integer. By $C^{(q,\mu)}$ we denote the code generated by

$$G^{(q,\mu)} := \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ \alpha^0 & \alpha^1 & \alpha^2 & \ldots & \alpha^{q-2} & 0 \\ \alpha^0 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(q-2)} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha^0 & \alpha^\mu & \alpha^{2\mu} & \ldots & \alpha^{\mu(q-2)} & 0 \end{pmatrix}, \tag{6}$$

where α is a primitive element of $GF(q)$ and hence a primitive $(q-1)$-th root of unity. The code $C^{(q,\mu)}$ is the dual of an extended Reed-Solomon code. It is a maximum distance separable (MDS) code with parameters $C^{(q,\mu)} = [q, \mu+1, q-\mu]_q$ (see Ref. 1). Furthermore, by $C_s^{(q,\mu)}$ we denote the code that is obtained by shortening the code $C^{(q,\mu)}$ at the last coordinate. Again, $C_s^{(q,\mu)} = [q-1, \mu, q-\mu]_q$ is an MDS code. We now show that both codes are contained in their duals.

Lemma 7: *For $0 \leq \mu < (q-1)/2$ the codes $C^{(q,\mu)}$ and $C_s^{(q,\mu)}$ are weakly self-dual with respect to the Euclidean inner product over $GF(q)$.*

Proof: It is sufficient to show that $C^{(q,\mu)}$ is contained in its dual, i. e., $G^{(q,\mu)} \cdot \left(G^{(q,\mu)}\right)^t = 0$. For $i = 0, \ldots, \mu$, let G_i denote the $(i+1)$-th row of $G^{(q,\mu)}$. We have to show that the inner product $G_i \cdot G_j$ vanishes for $0 \leq i,j \leq \mu$. Obviously, $G_0 \cdot G_0 = 0$. If not both i and j are zero, we get

$$G_i \cdot G_j = \sum_{l=0}^{q-2} \alpha^{il}\alpha^{jl} = \sum_{l=0}^{q-2} \left(\alpha^{(i+j)}\right)^l. \tag{7}$$

If $i + j \not\equiv 0 \bmod (q-1)$, then

$$G_i \cdot G_j = \frac{\left(\alpha^{(i+j)}\right)^{q-1} - 1}{\alpha^{(i+j)} - 1} = 0. \tag{8}$$

$\square$

These codes are not only weakly-self dual with respect to the Euclidean inner product, what is more, for suitably chosen parameters they are self-orthogonal with respect to the Hermitian inner product as well. This is the content of the following lemma which will ultimately allow to define MDS codes of length q^2 for quantum systems of dimension q.

Lemma 8: *For $0 \leq \mu \leq q-2$ the codes $C^{(q^2,\mu)}$ and $C_s^{(q^2,\mu)}$ are self-orthogonal with respect to the Hermitian inner product over $GF(q^2)$.*

Proof: We use the notation of the proof of Lemma 7. Again $G_0 * G_0 = 0$. If not both i and j are zero, we get

$$G_i * G_j = \sum_{l=0}^{q^2-2} \alpha^{il} \left(\alpha^{jl}\right)^q = \sum_{l=0}^{q^2-2} \left(\alpha^{(i+qj)}\right)^l. \tag{9}$$

So $G_i * G_j = 0$ if $i + qj \not\equiv 0 \bmod (q^2-1)$. This is true since $0 \leq i, j \leq q-2$. $\square$

3. Quantum MDS Codes

From the classical MDS codes of the previous section one can directly obtain quantum MDS codes.

Theorem 9: Let q be an arbitrary prime power. Then for $0 \leq \mu < (q-1)/2$ there exist quantum MDS codes with parameters

$$\begin{aligned} & \mathcal{C}^{(q,\mu)} = [\![q, q-2\mu-2, \mu+2]\!]_q \\ \text{and} \qquad & \mathcal{C}_s^{(q,\mu)} = [\![q-1, q-2\mu-1, \mu+1]\!]_q. \end{aligned}$$

Proof: By Lemma 7, we obtain $C^{(q,\mu)} = [q, \mu+1, q-\mu]_q \leq {C^{(q,\mu)}}^\perp$ and $C_s^{(q,\mu)} = [q-1, \mu, q-\mu]_q \leq {C_s^{(q,\mu)}}^\perp$. As the dual of an MDS code is again an MDS code (see Theorem 2 in Ch. 11 of Ref. 1), ${C^{(q,\mu)}}^\perp = [q, q-\mu-1, \mu+2]_q$ and ${C_s^{(q,\mu)}}^\perp = [q-1, q-\mu-1, \mu+1]_q$. Using the construction of Cor. 4, we obtain the quantum codes with the desired parameters. $\square$

While the length of these codes is upper bounded by the dimension q of the subsystems, there are also codes of length q^2.

Theorem 10: For any prime power q and any integer μ, $0 \leq \mu < q-1$, there exist quantum MDS codes with parameters

$$\begin{aligned} & \mathcal{D}^{(q^2,\mu)} = [\![q^2, q^2-2\mu-2, \mu+2]\!]_q \\ \text{and} \qquad & \mathcal{D}_s^{(q^2,\mu)} = [\![q^2-1, q^2-2\mu-1, \mu+1]\!]_q. \end{aligned}$$

Proof: By Lemma 8, we obtain $C^{(q^2,\mu)} = [q^2, \mu+1, q^2-\mu]_{q^2} \leq {C^{(q^2,\mu)}}^*$ and $C_s^{(q^2,\mu)} = [q^2-1, \mu, q^2-\mu]_{q^2} \leq {C_s^{(q^2,\mu)}}^*$. The dual codes have parameters ${C^{(q^2,\mu)}}^* = [q^2, q^2-\mu-1, \mu+2]_{q^2}$ and ${C_s^{(q,\mu)}}^* = [q^2-1, q^2-\mu-1, \mu+1]_{q^2}$. We now use the construction of Cor. 2 to obtain quantum codes with the desired parameters. $\square$

4. Shortening Quantum Codes

While classical linear codes can be shortened to any length, i. e., from a code $[n, k, d]$ one obtains a code $[n - r, k' \geq k - r, d' \geq d]$ for any r, $0 \leq r \leq k$, this is in general not true for quantum codes. However, in Ref. 12 it is shown how quantum codes can be shortened. Here we recall the main results. First, consider the vector valued bilinear form on $GF(q)^n \times GF(q)^n$ defined by

$$\{(\boldsymbol{v}, \boldsymbol{w}), (\boldsymbol{v}', \boldsymbol{w}')\} := (v_i w_i' - v_i' w_i)_{i=1}^n \in GF(q)^n. \tag{10}$$

Then, for a $GF(q)$-linear code C over $GF(q) \times GF(q)$, the puncture code of C is defined as

$$P(C) := \Big\langle \{\boldsymbol{c}, \boldsymbol{c}'\} \colon \boldsymbol{c}, \boldsymbol{c}' \in C \Big\rangle^{\perp} \subseteq GF(q)^n, \tag{11}$$

where the angle brackets denote the $GF(q)$ linear span. From Theorem 3 of Ref. 12 we get a characterization of the shortened quantum codes which can be obtained from C:

Theorem 11: Let C be a subspace of $(GF(q) \times GF(q))^n$, not necessarily self-orthogonal, of length n and size q^{n-k} such that C^* has minimum distance d. If there exists a codeword in $P(C)$ of weight r, then there exists a QECC $[\![r, k', d']\!]_q$ for some $k' \geq k - (n - r)$ and $d' \geq d$.

Proof: Let $\boldsymbol{x} \in P(C)$ be a codeword of weight r. We define the code $\widetilde{C}$ to be

$$\widetilde{C} := \{(\boldsymbol{v}, (x_i w_i)_{i=1}^n) \colon (\boldsymbol{v}, \boldsymbol{w}) \in C\}, \tag{12}$$

i. e., we multiply the coordinates of the second component $\boldsymbol{w}$ by the corresponding elements of $\boldsymbol{x}$. For arbitrary $(\widetilde{\boldsymbol{v}}, \widetilde{\boldsymbol{w}}), (\widetilde{\boldsymbol{v}}', \widetilde{\boldsymbol{w}}') \in \widetilde{C}$, we get

$$\begin{aligned}(\widetilde{\boldsymbol{v}}, \widetilde{\boldsymbol{w}}) * (\widetilde{\boldsymbol{v}}', \widetilde{\boldsymbol{w}}') &= \sum_{i=1}^n \widetilde{v}_i \widetilde{w}_i' - \widetilde{v}_i' \widetilde{w}_i \qquad = \sum_{i=1}^n v_i w_i' x_i - v_i' w_i x_i \\ &= \sum_{i=1}^n (v_i w_i' - v_i' w_i) x_i = \{(\boldsymbol{v}, \boldsymbol{w}), (\boldsymbol{v}', \boldsymbol{w}')\} \cdot \boldsymbol{x}. \end{aligned} \tag{13}$$

From (11) it follows that (13) vanishes, i. e., $\widetilde{C}$ is self-orthogonal. As (13) depends only on the coordinates of $\boldsymbol{x}$ that are non-zero, we can delete the other positions in $\widetilde{C}$ and obtain a self-orthogonal code $D \subseteq GF(q)^r \times GF(q)^r$ given by

$$D := \{((v_i), (x_i w_i))_{i \in S} \colon (\boldsymbol{v}, \boldsymbol{w}) \in C\},$$

where the set $S = \{i \colon i \in \{1, \ldots, n\} \mid x_i \neq 0\}$ is the support of the codeword $\boldsymbol{x}$. Deleting some positions, i. e., puncturing the code $\widetilde{C}$ may reduce its dimension, so D has $q^{n-k'}$ codewords, for some $k' \geq k$. The dual code D^* is obtained by shortening the code $\widetilde{C}^*$. So the minimum distance d' of D^* is not smaller than the minimum distance of $\widetilde{C}^*$ which is at least as large as that of C^*. This shows $d' \geq d$. $\square$

In order to apply Theorem 11 to our codes, we study the puncture code. For the codes of CSS type, we have the following:

Theorem 12: Let $C = C_1^\perp \times C_2^\perp \subseteq GF(q)^n \times GF(q)^n$ as in Theorem 3. Then

$$P(C) = \left\langle (c_i d_i)_{i=1}^n \colon \boldsymbol{c} \in C_1^\perp, \boldsymbol{d} \in C_2^\perp \right\rangle^\perp. \tag{14}$$

Proof: In order to find generators of $P(C)$, it suffices to compute the bilinear form (10) for all pairs of elements of a vector space basis for C. Using the basis $\{(\boldsymbol{c}, \boldsymbol{0})\colon \boldsymbol{c} \in C_1^\perp\} \cup \{(\boldsymbol{0}, \boldsymbol{d})\colon \boldsymbol{d} \in C_2^\perp\}$, the result follows. $\square$

For a $GF(q^2)$-linear code C over $GF(q^2)$, the situation is a bit more complicated. The following theorem shows how to compute $P(C)$ in this case:

Theorem 13: Let C be a $GF(q^2)$-linear code. Then

$$P(C) = \left\langle (c_i d_i^q + c_i^q d_i)_{i=1}^n \colon \boldsymbol{c}, \boldsymbol{d} \in C \right\rangle^\perp. \tag{15}$$

Proof: Similar to the proof of Theorem 11, we will show that each codeword of $P(C)$ defined by (15) gives rise to a shortened quantum code. First note that

$$c_i d_i^q + c_i^q d_i = c_i d_i^q + (c_i d_i^q)^q = \operatorname{tr}(c_i d_i^q),$$

where $\operatorname{tr}\colon GF(q^2) \to GF(q), x \mapsto x + x^q$ denotes the trace of the field extension $GF(q^2)/GF(q)$. Hence $P(C)$ is the dual code of the component-wise trace of the code generated by $\left\langle (c_i d_i^q)_{i=1}^n \colon \boldsymbol{c}, \boldsymbol{d} \in C \right\rangle$. As the dual of the trace code equals the restriction of the dual code to the subfield, i.e., $(\operatorname{tr}_K(C))^\perp = (C^\perp)|_K$ (see, e.g., Theorem 11 in Ch. 7, § 7 of Ref. 1), we can rewrite (15) as

$$P(C) = \left\langle (c_i d_i^q)_{i=1}^n \colon \boldsymbol{c}, \boldsymbol{d} \in C \right\rangle^\perp \cap GF(q)^n. \tag{16}$$

As in the proof of Cor. 2, we expand each codeword $\boldsymbol{c} \in C$ as $\boldsymbol{c} = \boldsymbol{v} + \gamma \boldsymbol{w}$ where $\gamma \in GF(q^2) \setminus GF(q)$ with $\gamma^q = -\gamma + \gamma_0$ for some $\gamma_0 \in GF(q)$. This defines a $GF(q)$-linear code over $GF(q) \times GF(q)$ which is given by

$$D = \{(\boldsymbol{v}, \boldsymbol{w})\colon \boldsymbol{v}, \boldsymbol{w} \in GF(q)^n \mid \boldsymbol{v} + \gamma \boldsymbol{w} \in C\}.$$

Then, as in (12), for a codeword $\boldsymbol{x} \in P(C)$ of weight r, we define the code

$$\widetilde{D} := \{(\boldsymbol{v}, (x_i w_i)_{i=1}^n)\colon \boldsymbol{v}, \boldsymbol{w} \in GF(q)^n \mid \boldsymbol{v} + \gamma \boldsymbol{w} \in C\}.$$

From (16) it follows that $\sum_{i=1}^n x_i c_i d_i^q$ vanishes. Similar to the proof of Cor. 2 (see eq. (3)), this implies that $\widetilde{D}$ is self-orthogonal with respect to (1), as well as the code obtained by deleting all coordinates where $\boldsymbol{x}$ is zero. $\square$

5. Results

Applying Theorem 12 and Theorem 13 to the codes of Lemma 7 and Lemma 8, respectively, we obtain

$$P(C^{(q,\mu)}) = \Big\langle G_{i+j}\colon 0 \le i,j \le \mu \Big\rangle^{\perp} = C^{(q,2\mu)\,\perp} \tag{17}$$

$$\text{and} \qquad P(C^{(q^2,\mu)}) = \Big\langle G_{i+qj}\colon 0 \le i,j \le \mu \Big\rangle^{\perp}, \tag{18}$$

where again G_i denotes the $(i+1)$-th row of the matrix $G^{(q,\mu)}$ in (6). Additionally, we have used that the component-wise product of G_i and G_j is G_{i+j}.

In combination with Theorem 11, we finally get:

Theorem 14: Let q be an arbitrary prime power. Then for all $3 \le n \le q$ and $1 \le d \le n/2+1$ there exists quantum MDS codes $[\![n, n-2d+2, d]\!]_q$. Moreover, for $2 \le d \le q$ and some s (at least $s = 0$ and $s = 1$) there exist quantum MDS codes $[\![q^2 - s, q^2 - 2d + 2 - s, d]\!]_q$.

Proof: The puncture code (17) is again an MDS code. As MDS codes contain words of all weights $d_{\min} \le w \le n$ from the minimum distance $d_{\min}$ to the length n of the code[1], shortening of the corresponding quantum MDS code to any length with the obvious constraints is possible.

For the codes of length q^2 from Lemma 8, we do not have an explicit formula for the weights in $P(C)$, but from Theorem 10 one knows that at least quantum MDS codes of length q^2 and $q^2 - 1$ exist. $\square$

The preceding theorem does not give much information about quantum MDS codes of length n with $q < n < q^2 - 1$. For a specific code, however, one can compute the puncture code $P(C)$ using (18). It can also be shown that in that case $P(C)$ is an extended cyclic code, but in general not an MDS code. Hence it is difficult to compute its weight distribution, especially for large codes for which only random sampling is possible. Using the computer algebra system MAGMA[13], we have computed and studied $P(C)$ for quantum MDS codes for quantum systems of dimension $q \in \{2, 3, 4, 5, 7\}$. The results which are summarized in Table 1 indicate that many shortenings are possible.

6. Final Remarks

Following the presentation of these results at the conference EQIS '03, we have learned about the work of Chi et al.[14] The authors constructed also quantum MDS codes, but only for quantum systems of odd dimension p^m, where p is a prime, and maximal length p^m. Our constructions apply to both even and odd prime powers. Moreover, we obtain quantum MDS codes for quantum systems of dimension p^m of length up to p^{2m}.

Table 1. Possible shortenings of QECCs of length q^2 for quantum systems of dimension q. Note that e. g. for the code $[\![16,10,4]\!]_4$, there are only words of even weight in $P(C)$, and for the code $[\![25,19,4]\!]_5$, there is no codeword of weight 7 in $P(C)$. Hence e. g. codes $[\![7,1,4]\!]_4$ and $[\![7,1,4]\!]_5$ cannot be obtained directly via shortening (but at least a code $[\![7,1,4]\!]_5$ can be constructed by other methods).

q	Theorem 10	puncture code $P(C)$	weights in $P(C)$
2	$[\![4,2,2]\!]_2$	$[4,3,2]_2$	2, 4
3	$[\![9,7,2]\!]_3$	$[9,8,2]_3$	2–9
	$[\![9,5,3]\!]_3$	$[9,5,4]_3$	4–9
4	$[\![16,14,2]\!]_4$	$[16,15,2]_4$	2–16
	$[\![16,12,3]\!]_4$	$[16,12,4]_4$	4–16
	$[\![16,10,4]\!]_4$	$[16,7,8]_4$	8, 10, 12, 14, 16
5	$[\![25,23,2]\!]_5$	$[25,24,2]_5$	2–25
	$[\![25,21,3]\!]_5$	$[25,21,4]_5$	4–25
	$[\![25,19,4]\!]_5$	$[25,16,6]_5$	6, 8–25
	$[\![25,17,5]\!]_5$	$[25,9,12]_5$	12–25
7	$[\![49,47,2]\!]_7$	$[49,48,2]_7$	2–49
	$[\![49,45,3]\!]_7$	$[49,45,4]_7$	4–49
	$[\![49,43,4]\!]_7$	$[49,40,6]_7$	6–49
	$[\![49,41,5]\!]_7$	$[49,33,8]_7$	8, 12–49
	$[\![49,39,6]\!]_7$	$[49,24,16]_7$	16, 18–49[a]
	$[\![49,37,7]\!]_7$	$[49,13,24]_7$	24, 25, 28, 30–49

[a] A codeword of weight 17 might exists as well, but the code $[49,24,16]_7$ has too many codewords for complete enumeration.

Finally, we note that we have found a generalization of our constructions that increases the maximal length of the resulting codes by one, i. e., up to $p^{2m}+1$. It remains an open question what the maximal length n of a non-trivial quantum MDS code with minimum weight $d>2$ is.

Acknowledgments

Markus Grassl and Martin Rötteler acknowledge the hospitality of the Mathematical Sciences Research Institute, Berkeley, USA, where part of this work has been performed. M. R. was supported in part by CFI, ORDFC, and MITACS. Funding by *Deutsche Forschungsgemeinschaft (DFG), Schwerpunktprogramm Quanten-Informationsverarbeitung (SPP 1078), Projekt AQUA (Be 887/13)* is also acknowledged.

References

1. Florence J. MacWilliams and Neil J. A. Sloane, *The Theory of Error–Correcting Codes*, North–Holland, Amsterdam, 1977.
2. Michael A. Tsfasman, Serge G. Vladut, and Thomas Zink, "Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound," *Mathematische Nachrichten*, vol. 109, pp. 21–28, 1982.
3. Dorit Aharonov and Michael Ben-Or, "Fault-Tolerant Quantum Computation with Constant Error," in *Proceedings of the 29th Annual ACM Symposium on Theory of Computing*. Association for Computing Machinery, 1997, pp. 176–188, preprint quant-ph/9611025.
4. Daniel Gottesman, "Fault-Tolerant Quantum Computation with Higher-Dimensional Systems," in *Quantum Computing & Quantum Communications; First NASA International Conference; selected papers, QCQC'98*, Colin P. Williams, Ed., Palm Springs, February 17–20, 1998, *Lecture Notes in Computer Science*, vol. 1509, pp. 302–313, Springer.
5. Alexei Ashikhmin and Emanuel Knill, "Nonbinary quantum stabilizer codes," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001, preprint quant-ph/0005008.
6. Mitsuru Hamada, "Information Rates Achievable with Algebraic Codes on Quantum Discrete Memoryless Channels," in *Proceedings IEEE International Symposium on Information Theory*, 2003. p. 480, preprint quant-ph/0207113, 2002.
7. Markus Grassl, Martin Rötteler, and Thomas Beth, "Efficient Quantum Circuits for Non-Qubit Quantum Error-correcting Codes," *International Journal of Foundations of Computer Science*, vol. 14, no. 5, pp. 757–775, Oct. 2003.
8. H. F. Chau, "Five quantum register error correction code for higher spin systems," *Physical Review A*, vol. 56, no. 1, pp. R1–R4, July 1997.
9. Keqin Feng, "Quantum codes $[\![6,2,3]\!]_p$ and $[\![7,3,3]\!]_p$ $(p \geq 3)$ exist," *IEEE Transactions on Information Theory*, vol. 48, no. 8, pp. 2384–2391, Aug. 2002.
10. A. Robert Calderbank and Peter W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996, preprint quant-ph/9512032.
11. A. M. Steane, "Error Correcting Codes in Quantum Theory," *Physical Review Letters*, vol. 77, no. 5, pp. 793–797, 29. July 1996.
12. Eric M. Rains, "Nonbinary Quantum Codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1827–1832, Sept. 1999, preprint quant-ph/9703048.
13. Wieb Bosma, John J. Cannon, and Catherine Playoust, "The Magma Algebra System I: The User Language," *Journal of Symbolic Computation*, vol. 24, no. 3–4, pp. 235–266, 1997.
14. Dong Pyo Chi, Jinsoo Kim, Jeyhoon Lee, and Soojoon Lee, "Quantum MDS Codes," manuscript, presented at *KIAS Workshop on Quantum Computation and Quantum Information*, Seoul, Korea, 2001.