On Optimal Quantum Codes

Markus Grassl[1] * Thomas Beth[1] † Martin Rötteler[2] ‡

[1] *Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, Am Fasanengarten 5, 76 128 Karlsruhe, Germany*
[2] *Department of Combinatorics and Optimization, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1*

Abstract. We present families of quantum error-correcting codes which are optimal in the sense that their minimum distance is maximal. These maximum distance separable (MDS) codes are defined over q-dimensional quantum systems, where q is any 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 MDS codes

1 Introduction

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 [10, 13]. The same is true for quantum error-correcting codes, e. g., for all quantum systems of prime dimension p it is known that a code $((5, p, 3))_p$ of length 5, dimension p, and minimum distance 3 exists [11]. Extending these results, it was shown recently that optimal quantum codes with parameters $[\![6, 2, 3]\!]_p$ and $[\![7, 3, 3]\!]_p$ exist for all primes $p \geq 3$ (see [5]).

Here we consider quantum systems which are composed of subsystems of dimension $d = p^m$, where p is a prime. As a shorthand, we will use the term "qudit". Quantum codes for qudit systems have been studied before, see e. g. [1, 2, 7, 9]. There exist also efficient algorithms for encoding these codes [8].

The codes presented here are optimal in the sense that the minimum distance is maximal for fixed length and dimension. For classical codes, constructions for such maximum distance separable (MDS) codes over a field with q elements are known for length up to $q+1$. We give constructions for quantum error-correcting codes (QECCs) over systems of dimension q with length up to q^2.

As basic ingredients, we use general constructions of QECCs from classical codes [2, 4, 12]. We present families of optimal classical codes suitable for these constructions. Finally, we address the problem of shortening QECCs, i. e., reducing the length and dimension while preserving the minimum distance. Unlike in the classical case, this operation is not trival. Our solution is based on results of Rains [11]. Finally, a table of results is presented.

2 Quantum MDS Codes

The main classes of QECCs for qubit systems are so-called CSS codes [4, 12] and the more general additive or stabilizer codes [3, 6]. Both constructions can be generalized to QECCs for qudit systems [2]. Here we will use the CSS construction with codes over $GF(q)$ and the stabilizer construction with linear codes over $GF(q^2)$.

Before presenting the new families of QECCs, we quote the quantum version of the singleton bound [11] and define quantum MDS codes:

Theorem 1 (Quantum Singleton Bound) *Let $\mathcal{C} = [\![n, k, d]\!]_q$ be a quantum error-correction code. Then*

$$k + 2d \leq n + 2. \tag{1}$$

If equality holds in (1) then $\mathcal{C}$ is pure.

Definition 2 ***(Quantum MDS code)*** *A quantum code for which equality holds in (1), i. e., $\mathcal{C} = [\![n, n-2d+2, d]\!]$, is called a quantum MDS code.*

For Reed-Solomon (RS) codes and extended RS codes over $GF(q)$ (see [10]) one can choose the parameters such that the codes are contained in their duals. Using the CSS construction, one obtains quantum MDS codes of length $q-1$ and q for quantum systems of dimension q:

Theorem 3 *Let q be an arbitrary prime power. Then for $0 \leq \mu < (q-1)/2$ there exist quantum MDS codes with parameters*

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

While the length of these codes does not exceed the dimension q of the subsystems, there are also codes of length q^2. Again, the codes are based on RS codes, but now over $GF(q^2)$. For suitably chosen parameters, these codes are self-orthogonal (with respect to the Hermitian inner product), hence the stabilizer construction applies:

Theorem 4 *For any prime power q and any integer μ, $0 \leq \mu < q-1$, there exist quantum MDS codes with parameters*

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

* grassl@ira.uka.de
† EISS_Office@ira.uka.de
‡ mroetteler@iqc.ca

3 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 [11] it is shown how quantum codes can be shortened. The main idea is outlined as follows: starting from an additive code C, one can define a code $P(C)$, the *puncture code*, with the following property (see [11, Theorem 3]):

Theorem 5 *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 the dual code 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 $d' \geq d$.*

The main problem is now to compute the code $P(C)$ and its weight spectrum, i. e., the set of Hamming weights of all codewords.

For the codes from Theorem 3 one can show that the code $P(C)$ is a classical MDS code. The weight spectrum of these codes contains the full range from the minimum distance to the length. Therefore, shortening of the resulting QECC is possible to all reasonable lengths.

For codes from Theorem 4, however, the situation is more complicated. In this case, the puncture code 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. However, our results which are summarized in Table 1 indicate that many shortenings are possible.

Table 1: Possible shortenings of QECCs of length q^2 for quantum systems of dimension q. Note that 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., a code $[\![7, 1, 4]\!]_5$ cannot be obtained directly via shortening (but we have constructed such a code by other methods).

q	codes from Th. 4	$P(C)$	weights in $P(C)$[a]
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
	$[\![16, 10, 4]\!]_4$	$[16, 17, 8]_4$	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, 12–19, 25–49
	$[\![49, 39, 6]\!]_7$	$[49, 24, 16]_7$	16, 18–49
	$[\![49, 37, 7]\!]_7$	$[49, 13, 24]_7$	24, 25, 28, 30–49

[a] For the last three codes in the table, the weights listed are obtained by random sampling since the complete weight distribution is not known. It is likely that even more shortenings are possible.

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 CSE and MITACS.

References

[1] D. Aharonov and M. Ben-Or, Fault-Tolerant Quantum Computation with Constant Error. In *Proc. of the 29th ACM STOC*, pages 176–118. quant-ph/9611025.

[2] A. Ashikhmin and E. Knill, Nonbinary Quantum Stabilizer Codes, *IEEE Trans. Inf. Theory*, 47(7):3065–3072, 2001. quant-ph/0005008.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Quantum Error Correction Via Codes Over GF(4), *IEEE Trans. Inf. Theory*, 44(4):1369–1387, 1998. quant-ph/9608006.

[4] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, *Phys. Rev. A*, 54(2):1098–1105, 1996. quant-ph/9512032.

[5] K. Feng, Quantum Codes $[\![6, 2, 3]\!]_p$ and $[\![7, 3, 3]\!]_p$ ($p \geq 3$) Exist, *IEEE Trans. Inf. Theory*, 48(8):2384–2391, 2002.

[6] D. Gottesman, A Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound, *Phys. Rev. A*, 54(3):1862–1868, 1996. quant-ph/9604038.

[7] D. Gottesman, Fault-Tolerant Quantum Computation with Higher-Dimensional Systems. In *Proc. QCQC'98*, LNCS 1509, pages 302–313, Springer, 1999.

[8] M. Grassl, M. Rötteler, and Th. Beth, Efficient Quantum Circuits for Non-Qubit Quantum Error-correcting Codes, *IJFCS*, 2003, to appear.

[9] M. Hamada, Information Rates Achievable with Algebraic Codes on Quantum Discrete Memoryless Channels. quant-ph/0207113, 2002.

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

[11] E. M. Rains, Nonbinary Quantum Codes, *IEEE Trans. Inf. Theory*, 45(6):1827–1832, 1999. quant-ph/9703048.

[12] A. M. Steane, Error Correcting Codes in Quantum Theory, *Phys. Rev. Letters*, 77(5):793–797, 1996.

[13] M. A. Tsfasman, S. G. Vladut, and T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Mathematische Nachrichten*, 109:21–28, 1982.