On Quantum BCH Codes and Its Duals

J. S. Bhullar and Manish Gupta

Abstract**—**Classical Bose-Chaudhuri-Hocquenghem (BCH) codes C that contain their dual codes can be used to construct quantum stabilizer codes this chapter studies the properties of such codes. It had been shown that a BCH code of length n which contains its dual code satisfies the bound on weight of any non-zero codeword in $C^{\perp}$ and converse is also true. One impressive difficulty in quantum communication and computation is to protect information-carrying quantum states against undesired interactions with the environment. To address this difficulty, many good quantum error-correcting codes have been derived as binary stabilizer codes. We were able to shed more light on the structure of dual containing BCH codes. These results make it possible to determine the parameters of quantum BCH codes in terms of weight of non-zero dual codeword.

Keywords**—**Quantum Codes, BCH Codes, Dual BCH Codes, Designed Distance.

I. Introduction

QUANTUM Error Correction is one of the basic components of quantum information theory. Quantum information processing can be used to solve problems in cryptography, secure communication and physics simulation exponentially faster than any of its possible classical analogues. Quantum computers physical models allow exact realizations of quantum information and its manipulation, provided the underlying assumptions are satisfied. However, it is unrealistic to assume that the practical physical systems will behave like the ideal models. Quantum data is very vulnerable to decoherance, interaction with the environment which is due to incomplete isolation of the system from the rest of the world. Also, control errors, which are caused by calibration errors and fluctuations in control parameters, have to be taken care of. Some kind of error correction is necessary to reduce the effects of these errors. Soon after the existence of quantum error correction was proved in the pioneering paper by Shor [1], the first constructions of good quantum error-correcting codes were given by Steane [2] and Calderbank and Shor [3]. These codes protect the quantum information using additional qubits (A qubit is a unit vector in a two dimensional complex vector space for which a particular basis, denoted by $|0\rangle$, $|1\rangle$, has been fixed.) and make it possible to reverse the effects of the most likely errors.

Encouraged by these positive results, researchers investigated and constructed many new quantum error correcting codes. The fault-tolerant implementations of several quantum operations were also discovered. These implementations make the basic assumption that the effects of all errors are sufficiently small per quantum bit and step of the computation.

Quantum information theory is rapidly becoming a wall-established discipline. It shares many of the concepts of classical information theory but involves new subtleties arising from the nature of quantum mechanics. Among the central concepts in common between classical and quantum information is that of error correction. Quantum error-correcting codes have progressed from their initial discovery [1] to broader analyses of the physical principles [5]-[8] and various code constructions [8], [12], [19].

The first quantum error correcting codes were discovered independently by Shor [1] and Steane [2]. Shor proved that 9 qubits could be used to protect a single qubit against general errors, while Steane described a general code construction whose simplest example does the same job using 7 qubits. A general theory of quantum error correction dates from subsequent papers of Calderbank and Shor [3] and Steane [4] in which general code constructions, existence proofs, and correction methods were given. Knill and Laflamme [5] and Bennett et al. [6] provided a more general theoretical framework, describing requirements for quantum error correcting codes, and measures of the fidelity of corrected states. The important concept of the stabilizer is due to Gottesman [7] and independently Calderbank et al. [8]; this found many useful insights into the subject, and permitted many new codes to be discovered [7]-[9]. Stabilizer methods will probably make a valuable contribution to other areas in quantum information physics. The idea of recursively encoding and encoding again was explored by several authors [10]-[12], using quantum resources in a hierarchical way, to permit communication over arbitrarily long times or distances. Building upon the ideas of quantum error correction, fault-tolerant quantum computation was first proposed by Shor [13]. These ideas were summarized by Preskill [14]. Gottesman put forward a significant number of further ideas on fault-tolerant quantum computing [15], which allow fault tolerant methods to be found for a wide class of Quantum error correction codes, and the methods were further improved in [16], [17].

II. Principles of Error Correction of Quantum Codes

Although quaternary constructions [18] yield good quantum codes, building quantum codes form binary was suggested by Calderbank and Shor [3] and Steane [4], [22]. Recently, Steane [9] proposed an enlargement of the Calderbank-Shor-Steane construction, leading to several families of codes with fixed minimum distance and growing length. Cohen et al. [23] further improved the estimates of code parameters obtained

Jaskarn S. Bhullar is currently the in charge of the Department of Applied Sciences at MIMIT, Malout, Punjab, India. (phone: +919356737037; e-mail: bhullarjaskarn@rediffmail.com).

Manish Gupta is Associate Professor at the Baba Farid College of Engineering and Technology, Bathinda, Punjab, India. (Phone: +919815138274; e-mail: manish_guptabti@yahoo.com).

from Steane's construction, and presented examples of new codes, and analyze asymptotic non constructive bounds.

The minimum distance d of the quantum code C is the largest generalized weight of a vector in $C \setminus C^{\perp}$. This code has parameters $[[n, k, d]]$ where is $\log_2[C] - n$.

Let $C[n, k, d]$ denoted a binary linear code of length n, dimension k, and minimum distance d.

For a more description Quantum theory of codes see [20].

III. Some New Quantum Codes

Steane [16] proved that the primitive BCH codes of length $2^m - 1$ contain their duals if and only if their designed distance $d = 2t + 1$ satisfies

$$d \leq 2^{\lceil m/2 \rceil} - 1$$

It following form [20] that in this case the codes have parameter

$$[2^m - 1, 2^m - 1 - mt, 2t + 1]$$

Moreover, these codes are nested, i.e. form a chain for the inclusive relation when t increases. Extending them with a parity bit, [23] derived the families of codes.

Calderbank in [18] shows how to construct an $[[n, k + 1, d - 1]]$- code from an [[n, K, d]]-code. Using it [23] constructed from F_0 the following family

$$F_5\ [[2^m\ , 2^m - (5l + 3)m - 1 + b, 6l + 5]]$$

for $6l + 6 \leq 2^{\lceil m/2 \rceil}$

It is tempting to conjecture the existence of families of codes with parameters

$$F_a[[2^m, 2^m - (5l + a - 2)m + b, 6l + a]]$$

where $a = 0,1,2,3,4,5$ and b is a small integer constant. Cohen et al [20] also proved the following result:

Theorem 1 [23]: For $6l + 4 \leq 2^{\lceil m/2 \rceil}$ there exist quantum codes with parameters

$$F_4[[2^m, 2^m - (5l + 2)m - 1{,}6l + 4]]$$

Theorem 2 [16]: Let $C[n, k, d]$, $C^{\perp} \subseteq C$, be a classical binary linear error-correcting code with generator matrix G. Let C be a subcode of a code $C'[n, k' > k + 1, d']$ with generator matrix $\binom{G}{G'}$, then

$$G = \begin{bmatrix} G & 0 \\ o & G \\ G' & PG' \end{bmatrix}$$

where P is an invertible fix-point free map generates a quantum code of parameters

$$\left[n\ , k + k' - n, \geq \min\left(d, \left\lceil\frac{3d'}{2}\right\rceil\right)\right]$$

Thangaraj and McLaughlin [28] used the ideas of Calderbank et al. [8] to construct a new class of quantum codes from cyclic over $GF(4^m)$. In particular, the following theorem from [8] can be used directly to obtain quantum codes from the certain codes from certain code over GF(4).

Theorem 3 [22]: Suppose C is an (n, k) linear code over GF(4) self-orthogonal with respect to the Hermitian inner product. Suppose also that the minimum weight $C^{\perp} \setminus C$ is d. Then an $[[n, n - 2k, d]]$ quantum code can be obtained from C

The Hermitian inner product of $u.v \in GF(4)^n$ is defined to be

$$u.v = u_1\overline{v_1} + u_2\overline{v_2} + \cdots + u_n\overline{v_n}$$

where $\overline{\omega} = \omega^2$ for $\omega \in GF(4)$.

Thangaraj and McLaughlin [28] considered self - orthogonal codes over GF(4) that are obtained as 4- ary images of $4^m -$ ary cyclic codes of the length $n|(4^m - 1)$. Binary images of the self – orthogonal codes over $GF(2^m)$ have been used to obtain Quantum codes in [27].

IV. Quantum BCH Codes

Calderbank, Shor, Rains, and Sloane outlined the construction of binary quantum BCH codes in [8]. Grassl, Beth and Pellizari developed the theory further by formulating a nice condition for BCH codes [24], [25]. Steane simplified it futher for the special case of binary narrow-sense primitive BCH codes [9] and gave a very simple criterion based on the design distance along. Very little was done with respect to the nonprimitive and nonbinary quantum BCH codes.

Aly et al [26] gave very simple conditions based on design distance alone. Further he gave precisely the dimension and tighten ruslts on the purity of the quantum codes from classical codes

Theorem 4 [26] Let $m = \mathrm{ord}_n(q) \geq 2$, where q is a power of a prime and δ_1, δ_2 are integers such that $2 \leq \delta_1 < \delta_2 \leq \delta_{max}$ where

$$\delta_{max} = \frac{n}{q^m - 1}\left(q^{\left\lceil\frac{m}{2}\right\rceil} - 1 - (q - 2)[m\ \mathrm{odd}]\right)$$

Then there exist a Quantum code with parameter

$$\left[\left[n, m\left(\delta_2 - \delta_1 - \left\lfloor\frac{\delta_2 - 1}{q}\right\rfloor + \left\lfloor\frac{\delta_1 - 1}{q}\right\rfloor\right), \geq \delta_1\right]\right]_q$$

pure to δ_2.

When BCH codes contain there duals then following result is derived by [21]

Theorem 5 [26] Let $m = \mathrm{ord}_n(q)$ where q is a power of a prime and $.. \leq \delta \leq \delta_{max}$, with

$$\delta_{max} = \frac{n}{q^m - 1}\left(q^{\lceil \frac{m}{2} \rceil} - 1 - (q-2)[m \text{ odd}]\right),$$

Then there exists a quantum code with parameters

$$[[n, n - 2m\lceil(\delta-1)(1-1/q)\rceil, \geq \delta]]_q$$

pure to $\delta_{max} + 1$

Theorem 6 [26] Let $m = ord_n(q^2) \geq 2$ where q is a power of a prime and $2 \leq \delta \leq \delta_{max} = \lfloor n(q^m - 1)/(q^{2m} - 1) \rfloor$, then there exists a quantum code with parameters

$$[[n, n - 2m\lceil(\delta-1)(1-1/q^2)\rceil, \geq \delta]]_q$$

that is pure up to $\delta_{max} + 1$

In the above theorem, quantum codes can also be constructed when the design distance exceeds the given value of δ_{max}.

These are not the only possible families of quantum codes that can derived from BCH codes over F_{q^l} to get codes makes it very easy to specify such codes. Similar results can be derived for the Hermitian case.

Theorem 7 [26] Let $m = ord_n(q^l)$ where q is a power of a prime and $2 \leq \delta \leq \delta_{max}$, with

$$\delta_{max} = \frac{n}{q^{lm} - 1}\left(q^{l\lceil \frac{m}{2} \rceil} - 1 - \left(q^l - 2\right)[m \text{ odd}]\right)$$

Than there exists a quantum code with parameters

$$[[ln, ln - 2lm\lceil(\delta-1)(1-1/q^{l)}\rceil, \geq \delta]]_q$$

The Next theorem from [1] used mainly for the construction of the quantum BCH codes [24] describes a necessary and sufficient conditions for the self – orthogonality of the cyclic codes over GF (4).

Theorem 8 A linear cyclic codes over GF(4) of the length $n|(4^m - 1)$and the generator of the polynomials g(x) is self – orthogonal if any only if

$$g(x)g^{\dagger}(x) \equiv 0 \bmod (x^n - 1)$$

where if

$$g(x) = \sum_{r=0}^{n-1} g_r x^r$$

$$g^{\dagger}(x) = \mathrm{GCD}\left(\overline{g_0} + \sum_{r=0}^{n-1} \overline{g_{n-r}}\, x^r, x^n - 1\right)$$

and $\bar{g_i} = g_i^2$.

Generator polynomials of cyclic codes of the length $n|(4^m - 1)$ over GF(4) are usually specified in the terms of their zeros in $GF(4^m)$.

Lemma 1 [20] Suppose C is a binary BCH code of length $n = 2^m - 1$ with designed distance $\delta = 2t + 1$, where $2t - 1 \leq 2^{\lceil m/2 \rceil} + 1$, then the weight w of any non-zero codeword in $C^{\perp}$ lies in the range

$$2^{m-1} - (t-1)2^{m/2} \leq w \leq 2^{m-1} + (t-1)2^{m/2}$$

Theorem 10 Let C be binary BCH code of length $n = 2^m - 1$ with designed distance $\delta = 2t + 1$, where

$$2t - 1 \leq 2^{\lceil m/2 \rceil} + 1$$

and w be the weight of any non-zero codeword in $C^{\perp}$, then $C^{\perp} \subset C$ if and only if weight w lies in the range of

$$\frac{(n-3)^2}{16} - (t-1)\frac{n-5}{2} < w < (n-5)\frac{t}{2}$$

Proof:

$$2^{m-1} - (t-1)2^{m/2} \leq w \leq 2^{m-1} + (t-1)2^{m/2}$$
$$-(t-1)2^{m/2} \leq w - 2^{m-1} \leq (t-1)2^{m/2}$$
$$|w - 2^{m-1}| \leq (t-1)2^{m/2}$$
$$2t - 1 \leq 2^{\lceil m/2 \rceil} + 1$$
$$\delta - 2 \leq 2^{\lceil m/2 \rceil} + 1$$
$$\delta \leq 2^{\lceil m/2 \rceil} + 3 = \delta_{max}$$

But from [26]

$$\delta \leq \delta_{max} = \left\lfloor \frac{n+1}{2} \right\rfloor$$

So $\quad 2^{\lceil m/2 \rceil} + 3 = \left\lfloor \frac{n+1}{2} \right\rfloor$

$$2.\,2^{(m/2)-\{m/2\}} = \frac{n+1}{2} - \left\{\frac{n+1}{2}\right\} - 3 \leq \frac{n+1}{2} - 3$$
$$2^{m/2} < \frac{n-5}{2}$$

Again

$$2.\,2^{(m/2)-\{m/2\}} = \frac{n+1}{2} - \left\{\frac{n+1}{2}\right\} - 3 \geq \frac{n+1}{2} + 1 - 3$$
$$2^{(m/2)} > \frac{n-3}{4}$$
$$\frac{(n-3)^2}{16} - (t-1)\frac{n-5}{2} < 2^{m-1} - (t-1)2^{m/2} \leq w$$
$$\leq 2^{m-1} + (t-1)2^{m/2}$$
$$< \frac{n-5}{2} + (t-1)\frac{n-5}{2}$$
$$\frac{(n-3)^2}{16} - (t-1)\frac{n-5}{2} < w < (n-5)\frac{t}{2}$$

V. Conclusion

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

REFERENCES

[1] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," Phys. Rev. A, vol 52, pp. R2493-R2496, October 1995.

[2] A. M. Steane, "Error correcting codes in quantum theory," Phys. Rev. Lett., vol. 77, pp. 793-797, July 1996.

[3] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A, vol. 54, pp. 1098-1105, August 1996.

[4] A. Steane, "Multiple particle interference and quantum error correction," Proc. Roy. Soc. Lond. A, vol. 452, pp. 2551-2577, November 1996.

[5] E. Knill and R. Laflamme, "A theory of quantum error-correcting codes," Phys. Rev. A, vol. 55, pp. 900-911, February 1997.

[6] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wooters, "Mixed state entanglement and quantum error correcting codes," Phys. Rev. A, vol. 54, pp. 3824-3851, November 1996.

[7] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum hamming bound," Phys. Rev. A, vol. 54, pp. 1862-1868, September 1996.

[8] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. Sloane, "Quantum error correction and orthogonal geometry," Phys. Rev. Lett., vol. 78, pp. 405-408, January, 1997.

[9] A. M. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," IEEE Trans. Inf. Theory, vol. 45, pp. 2492-2495, November 1999.

[10] A. Y. Kitaev, "Quantum error correction with imperfect gates," in Proc. 3rd Int. Conf. of Quantum Communication and Measurement, New York, May 1997, pp. 181-188.

[11] D. Aharonov and M. Ben-Or, "Fault-tolerant quantum computation with constant error rate," in Proc. 29th Ann. ACM Symp. on Theory of Computing, New York, May 1997, pp.176-188.

[12] E. Knill and R. Laflamme, "Concatenated quantum codes," quant ph/9608012, August 1996.

[13] P. W. Shor, "Fault-tolerant quantum computation," in Proc. 37th FOCS, Los Alamitos, CA, March 1996, pp. 56-65.

[14] J. Preskill, "Reliable quantum computers," Proc. R. Soc. Lond. A, pp. 454-385, August 1997.

[15] D. Gottesman, "A theory of fault-tolerant quantum computation," Phys. Rev. A, vol. 57, pp. 127-137, January 1998.

[16] A. M. Steane, "Efficient fault-tolerant quantum computing," Nature, vol. 399, pp.124-126, May 1999.

[17] D. Gottesman, "Fault-tolerant quantum computation with local gates," J. Modern Optics, vol. 47, pp. 333-345, February 2000.

[18] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF (4)," IEEE Trans. Inform. Theory, vol. 44, pp. 1369–1387, July 1998.

[19] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error-correcting code," Phys. Rev. Lett., vol. 77, pp. 198–201, July 1996.

[20] F. J. MacWilliams and N. J. A. Sloane, Theory of Error-Correcting Codes. Amsterdam, the Netherlands: Elsevier, 1977.

[21] E. M. Rains, "Nonbinary quantum codes," IEEE Trans. Inform. Theory, vol. 45, pp. 1827–1832, Sept. 1999.

[22] A. M. Steane, "Simple quantum error correcting codes," Phys. Rev. Lett., vol. 77, pp. 793–797, 1996.

[23] G. Cohen, S. Encheva and S. Litsyn, "On Binary Construction of Quantum Codes," IEEE Trans. Inf. Theory, vol. 45, pp. 2495-2498, November 1999.

[24] M. Grassl and T. Beth, "Quantum BCH codes," in Proc. X. Int. Symp. Theoret. Elec. Eng., Magdeburg, 1999, pp. 207–212.

[25] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," Phys. Rev. Lett. A, vol. 56, no. 1, pp. 33–38, 1997.

[26] Salah A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On Quantum and Classical BCH Codes," IEEE Trans. Inf. Theory, vol. 53, pp. 1183-1188, 2007.

[27] M. Grassl, W. Geiselmann, and T. Beth, "Quantum reed-solomon codes," in Proc. AAECC Conf., 1999.

[28] A. Thangaraj, S. W. McLaughlin, "Quantum Codes form Cyclic Codes over GF(4^m)," IEEE Trans. Inf. Theory, vol. 47, pp. 1176-1178, 2001.

Dr. Jaskarn S. Bhullar was born in Malout, Punjab, India in 1971. He received his M.Sc. degree from Ajmer University, Rajasthan, India and Ph.D. degree in Information and Coding Theory from Ajmer University, Rajasthan in 2004.

In 1999, he joined the Department of Applied Sciences, Malout Institute of Management and Information Technology (MIMIT), Malout, Punjab, India.as a Lecturer, and in 2008 became a Associate Professor. He is currently the in charge of Department of Applied Sciences at MIMIT, Malout, Punjab, India. His current research interests include Information Theory, Coding Theory, Quantum Codes. Dr. Bhullar is Executive Member of Indian Society of Information Theory and its Applications (ISITA), India. He is a Life Member of the International Association of Engineers (IAENG); Indian Society for Technical Education (ISTE). He had published more than 20 papers in different International/National Journals and Conferences.

Dr. Manish Gupta was born in Bathinda, Punjab, India in 1977. He received his M.Sc. degree from Ajmer University, Rajasthan, India in 2000 and Ph.D. degree in Information and Coding Theory from Punjab Technical University, Jalandhar in 2012.

In 2002 he joined Department of Mathematics, D.A.V. College, Bathinda, Punjab, India as Lecturer and in 2013 became Associate Professor at Baba Farid College of Engineering and Technology, Bathinda, Punjab, India.His current research interests include Error Correcting Codes, Quantum Codes and Network Coding. Dr. Gupta is Life Member of International Association of Engineers (IAENG); Indian Society for Technical Education (ISTE); Indian Mathematical Society (IMS). He is also the member of IEEE. He had published more than 20 papers in different International/National Journals and Conferences.