British Journal of Mathematics & Computer Science
6(5): 444-450, 2015, Article no.BJMCS.2015.090
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

On the Construction of Odd Length Quantum Codes

Manish Gupta[1*], R. K. Narula[2] and Divya Taneja[3]

[1]Department of Applied Science, Baba Farid College of Engineering and Technology, Bathinda, P.B., India.
[2]Department of Applied Science, Punjab Institute of Technology (PIT), Mansa, P.B., India.
[3]Department of Applied Science, Yadavindra College of Engineering, Talwandi Sabo, P.B., India.

Article Information

DOI: 10.9734/BJMCS/2015/15059
Editor(s):
(1) Paul Bracken, Department of Mathematics, University of Texas-Pan American, USA.
Reviewers:
(1) Ravi Narayan, Computer Science & Engineering Department, Thapar University, India.
(2) Anonymous, Mexico.
Complete Peer review History: http://www.sciencedomain.org/review-history.php?iid=735&id=6&aid=7758

Original Research Article

Received: 03 November 2014
Accepted: 26 November 2014
Published: 13 January 2015

Abstract

In this paper, we endeavor for an extensive study of [[n,n-3,2]] codes of odd length. We begin with the computation of the linear programming bound on the dimension of distance 2 codes of odd length and show that the [[n,n-3,2]] codes are optimal. We next find their generator matrix, stabilizer structure and also show that these codes are impure or degenerate except the [[3,0,2]] code which is pure by convention. In degenerate codes, distinct errors do not necessarily take the code space to orthogonal space. So sometimes they can correct more errors than that they can identify and has the capacity to store more information than a nondegenerate code. The present paper also establishes the existence of ((2m+1,2^(2m-2),2)) codes from the ((2m,2^(2m-2),2)) codes for all m>1. We have also constructed another class of distance 2 codes which are constructed using distance 3 codes.

Keywords: Additive codes, stabilizer, pure and impure codes, linear programming bound.

1 Introduction

With the discovery of Shor's algorithm, Quantum computing has become an active interdisciplinary field of research. Quantum computers are able to solve hard computational problems more efficiently than present classical computers. But reliability of the quantum computers is questionable since the quantum states are subjected to decoherence i.e. the interaction of the states with the environment which leads to the loss of information. Quantum error correcting codes

**Corresponding author: manish_guptabti@yahoo.com;*

are the means of protecting quantum information against external sources such as noise and decoherence.

Many explicit constructions of quantum error-correcting codes have been proposed so far. Most of the codes known so far are additive or stabilizer codes which are constructed from classical binary code that are self-orthogonal with respect to a certain symplectic inner product. An $[[n, k, d]]$ code is an additive quantum code of minimum-distance d of length n encoding k quantum bits and an $((n, K, d))$ code refers to a general code encoding K states in n qubits with minimum distance d. A code is called nonadditive if it is not equivalent to any additive code Claderbank et al. [1], gave the construction of additive quantum codes using additive classical codes C over GF(4) which are self orthogonal under the trace inner product defined as

$$u * v = \mathrm{Tr}\, u \cdot \bar{v} = \sum_{j=1}^{n} u_j \bar{v}_j + v_j \bar{u}_j,$$

where $u, v \in GF(4)^n$. If C is an additive self orthogonal subcode of $GF(4)^n$, containing 2^k vectors, such that there are no vectors of weight $\leq d-1$ in $C^{\perp}/C$. Then there exists a quantum-error-correcting code with parameters $[[n, n-k, d]]$ .A quantum $[[n, n-k, d]]$ is pure if there are no nonzero vectors of weight < d in $C^{\perp}$; otherwise it is an impure or degenerate.

An important class of quantum codes called Stabilizer codes was defined in Claderbank et.al.[1] and D. Gottesman, [2] which are analogous to the quantum additive codes. An $[[n, k, d]]$ stabilizer code encodes k logical qubits into n physical qubits, and is described by an abelian subgroup, S, of the Pauli group with size $|S| = 2^{n-k}$. The codespace is the set of simultaneous eigenvectors of S with Eigen value 1.

Calderbank et al. [1] showed that the best additive even distance 2 codes are $[[n, n-2, 2]]$, for n even and $[[n, n-3, 2]]$, for n odd. Rains [3] presented a number of results on codes of minimum distance 2. These minimium distance codes correct any single qubit erasure i.e. an error which acts on a qubit at known location in an unknowm way or is used to detect a single qubit error with unknown location. It was shown that the additive $[[n, n-2, 2]]$, where n is even are optimal for they satisfy the Singleton bound. Among odd length distance 2 code the $((5, 6, 2))$ nonadditive code was revealed by Rains et al [4] which generated a family of pure $((2m+1, 3.2^{2m-3}, 2))$ nonadditive codes of Rains [3]. J.A. Smolin et al. [5] presented a new family

$$\left((4k+2l+3, M_{k,l}, 2)\right) \text{ where } M_{k,l} \approx 2^{n-2}\left(1 - \sqrt{\frac{2}{\pi(n-1)}}\right)$$

of nonadditive codes which correct single qubit error while encoding a higher dimensional space than is possible with any additive codes. K. Feng and C. P. Xing [6], conferred a characterization of quantum error correcting codes based on which they constructed a class a binary quantum $\left(\left(n, 2^{n-2} - \frac{1}{2}\binom{n-1}{(n-1)/2}, 2\right)\right)$ codes for odd length $n \geq 5$. For $n \geq 11$, this an improvement on codes of Rains [3]. Aggarwal and Calderbank [7] gave a mathematical framework for the design of both additive and non additive quantum codes based on a correspondence between Boolean functions and projection operators. A. Cross et al. [8] presented a framework for code designs which was described by two objects: a single stabilizer state $|S\rangle$, and a classical code that generates the basis vectors of this code from $|S\rangle$. Such codes were called codeword stabilized quantum codes. In this framework the $((5, 6, 2))$ nonadditive code, the family $((2m+1, 3.2^{2m-3}, 2))$ generated by it and the simple family of minimum distance 2 codes found in J.A.Smolin et.al. [5] were constructed.

In this paper we make an extensive study of $[[\mathrm{n}, \mathrm{n}-3, 2]]$ codes of odd length, by finding their generator matrix, stabilizer structure and also show that these codes are impure or degenerate except the $[[3,0,2]]$ which is pure by convention. In degenerate codes, distinct errors do not necessarily take the code space to orthogonal space. So sometimes they can correct more errors than that they can identify and has the capacity to store more information than a nondegenerate code. We have also shown the existence of $((2\mathrm{m}+1,\ 2^{2\mathrm{m}-2}, 2))$ codes for all $\mathrm{m} \geq 2$.

2 Existence and Construction of $[[\mathbf{n}, \mathbf{n}-\mathbf{3}, \mathbf{2}]]$, for N Odd

Rains [3] explored the structure of quantum codes of minimum distance 2 and showed the existence of quantum $[[\mathrm{n}, \mathrm{n}-2, 2]]$ code, where n is even, which were optimal in the sense that they satisfy the quantum singleton bound. This gave an upper bound on the dimension of a [[2m, k, 2]] code which is $k \leq 2m-2$. In this section we shall find an upper bound on the dimension of odd length distance 2 codes. Quantum MacWilliams identities relate the weight enumerators of a code and its dual which together with linear programming technique is a powerful tool to find the bounds on dimensions of a code. This technique is will be used to find a bound on dimension of an additive distance 2 quantum code of odd length. We shall show the existence of $[[n, n-3, 2]]$ codes where n is odd and also show that their construction is possible using tensor product.

Theorem - 1 For an $[[2m+1, k, 2]]$ quantum code $k \leq 2(m-1)$.

Proof- Consider the weight enumerator $A(x)$, the dual enumerator $B(x)$ and the shadow enumerator $S(x)$ of the $[[2m+1, k, 2]]$ code.

Then according to quantum MacWilliams identity Rains [9]

$$B(x) = \frac{1}{2^{n-k}}(1+3x)^n A\left(\frac{1-x}{1+3x}\right)$$

Also the Shadow enumerator Rains [10]

$$S(x) = \frac{1}{2^{n-k}}(1+3x)^n A\left(\frac{x-1}{1+3x}\right)$$

Thus the coefficients

$$B_0 = \frac{1}{2^{n-k}}\sum_{i=0}^{n} A_i$$

$$B_1 = \frac{1}{2^{n-k}}\sum_{i=0}^{n} (3n-4i)A_i$$

$$S_0 = \frac{1}{2^{n-k}}\sum_{i=0}^{n} (-1)^i A_i$$

Eliminating $\mathrm{A}_{\mathrm{n}-1}$ and A_{n} we get

$$(n-2)B_0 + B_1 - 2S_0 = \frac{1}{2^{n-k}}\sum_{i=0}^{m-1} 4(n-2i-1)(A_{2i} + A_{2i+1})$$

Since the code is of minimum distance 2, we have

$$B_0 = A_0 \; and \; B_1 = A_1$$

Using these we get

$$\left(2^{n-k}(n-2) - (4n-4)\right)A_0 + \left(2^{n-k} - (4n-4)\right)A_1$$

$$= 2S_0 + \sum_{i=1}^{m} 4(n-2i-1)(A_{2i} + A_{2i+1})$$

Now, since the coefficients on the right hand side and A_0 are positive and also $S_0 and\, A_i$, $\forall\, i > 0$ are all non negative, it follows that

$$\left(2^{n-k}(n-2) - (4n-4)\right) \geq 0$$

which is true for $k \leq n-3$.

The next result shows the existence of optimal $[[n, n-3, 2]]$ codes for odd *n* satisfying the above bound.

Theorem-2 If $[[2\mathrm{m}, 2\mathrm{m}-2, 2]]$ code exists where $m > 1$, then $[[2m+1, 2m-2, 2]]$ code exists.

Proof – A $[[2\mathrm{m}, 2\mathrm{m}-2, 2]]$ code is constructed from a classical additive self dual code $C = [2m, 2]$ whose generator matrix is

$$G = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \omega & \omega & \omega & \cdots & \omega \end{bmatrix}$$

Indeed $C = \{000 \ldots 0, 111 \ldots 1, \omega\omega\omega \ldots \omega, \varpi\varpi\varpi \ldots \varpi\}$

Its dual $C^{\perp} = [2m,\ 2m-2]$ code consisting of all vectors of the form $v_1 v_2 v_3 \ldots v_{2m}$ such that $v_1 + v_2 + v_3 + \ldots + v_{2m} \equiv 0\ (mod 2)$.

The direct sum of C with $C_1 = \{0, 1\}$ is $C' = [2m+1, 3]$ additive code

The generator matrix of this code is

$$G' = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ \omega & \omega & \omega & \ldots & \omega & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{bmatrix}$$

Its dual $C'^{\perp}$ consists of direct sum of $C^{\perp}$ with $C_1 = \{0, 1\}$ and also $C' \subseteq C'^{\perp}$.

Thus, by the construction of additive quantum codes given in Calderbank et al. [1], we have the existence of $[[2m+1, 2m-2, 2]]$ code. The distance is 2 since there is no vector of weight less than 2 in $C'^{\perp}/C'$

In this $C'^{\perp}$ contains the vector 000...01 of weight < 2, so this code is impure and we know that a $[[n, 0, d]]$ code is pure by convention, therefore $m > 1$.

It can be easily verified that the explicit basis of the $[[2m+1, 2m-2, 2]]$ code is obtained by taking the tensor product of the $[[2m, 2m-2, 2]]$ code with $|0\rangle + |1\rangle$.

For example the explicit basis of $[[5,2,2]]$ code is

$$|00000\rangle + |11110\rangle + |00001\rangle + |11111\rangle,$$
$$|00110\rangle + |11000\rangle + |00111\rangle + |11001\rangle,$$
$$|01010\rangle + |10100\rangle + |01011\rangle + |10101\rangle,$$
$$|01100\rangle + |10010\rangle + |01101\rangle + |10011\rangle$$

which is a joint Eigen space of

$$\sigma_x \otimes \sigma_x \otimes \sigma_x \otimes \ldots \otimes \sigma_x \otimes \sigma_x$$
$$\sigma_z \otimes \sigma_z \otimes \sigma_z \otimes \ldots \otimes \sigma_z \otimes I$$
$$I \otimes I \otimes I \otimes \ldots \otimes I \otimes \sigma_x$$

If we observe the basis vectors obtained above, is just the tensor product of the basis vector of $[[4,2,2]]$ with $|0\rangle + |1\rangle$ so this result can also be interpreted as following

Construction of $((2m+1,\ 2^{2m-2},2))$ codes for $m > 1$

Theorem - 3 If there exists a pure $((n\ ,K,2))$, then there exists a $((n+1,K,2))$ code.

Proof- Let *Q* be a $((n\ ,K,2))$ code and *v* be the state $|0\rangle + |1\rangle$.
Then the new code $Q' = Q \otimes v$ is a $((n+1,K,2))$ code.
Now there exist additive $((2m, 2^{2m-2}, 2\ ))$ codes. (Rains [3])

Thus combining the two results we have the existence of $((2m+1,\ 2^{2m-2},2))$ codes for $m > 1$.

So far we have proved the existence of $[[2m+1, 2m-2, 2]]$ codes for m > 1.These codes were impure so the above theorem is not applicable for m = 1 as the $[[n,0,d]]$ codes are pure by convention. So our next aim is to construct the $[[3,0,2]]$ code. For this we will find a self dual code of length 3 over GF(4) and then by construction of additive quantum codes given in Calderbank *et.al*.[1], we have the existence of $[[3,\ 0,2]]$ code.

Consider the additive code $C = [2, 2^2\ ]$ over GF(4). Generator matrix of this code is

$$G = \begin{bmatrix} 1 & 1 \\ \omega & \omega \end{bmatrix}$$

It is a self dual code. This code can be extended to self dual code $C' = [3, 2^3]$.

$$G' = \begin{bmatrix} 1 & 1 & \omega \\ \omega & \omega & \omega \\ 1 & \omega & 1 \end{bmatrix}$$

This generates the desired self dual code and it can be easily verified that there is no vector of weight < 2 in C'.

Hence the existence of pure quantum code [[3, 0, 2]]. This code is non linear as there does not exist a linear; trace self dual $(n, 2^n)$ code for odd n.

The stabilizer of this code is

$$\sigma_x \otimes \sigma_x \otimes \sigma_z$$
$$\sigma_z \otimes \sigma_z \otimes \sigma_z$$
$$\sigma_x \otimes \sigma_z \otimes \sigma_x$$

having $|000\rangle + |110\rangle + |101\rangle - |011\rangle$ as the joint Eigen space.

3 Construction of Another Family of Quantum Codes of Distance 2

In this section another family of distance 2 quantum codes has been constructed using quantum codes of distance 3.

Theorem – 4 There exists quantum $\left[[n-1, n-m-1, 2]\right]$ and $[[n-1, n-m-2, 2]]$ codes where

$$n = \begin{cases} \sum_{i=0}^{m/2} 2^{2i} & , \ m \text{ even} \\ \sum_{i=1}^{m-1/2} 2^{2i+1} & , \ m \text{ odd} \end{cases}$$

Proof – It was proved in Calderbank et al. [1] that for $m \geq 2$ there exists an $[[n, n-m-2, 3]]$ code where n is

(i) $\sum_{i=0}^{m/2} 2^{2i}$ (m even)

(ii) $\sum_{i=1}^{m-1/2} 2^{2i+1}$ (m odd)

These codes are pure and additive but in general are not linear.
Also it was proved that if $[[n, k, d]]$ code exists and

(a) If code is pure for $n \geq 2$ then $[[n-1, k+1, d-1]]$ code exists.
(b) If $n \geq 2$ then $[[n-1, k, d-1]]$ code exists.

Using the above two results we have the existence of $\left[[n-1, n-m-1, 2]\right]$ and $[[n-1, n-m-2, 2]]$ codes where

$$n = \begin{cases} \sum_{i=0}^{m/2} 2^{2i} & , \ m \text{ even} \\ \sum_{i=1}^{m-1/2} 2^{2i+1} & , \ m \text{ odd} \end{cases}$$

4 Conclusion

In this paper it has been proved that $[[n, n-3, 2]]$ codes are optimal. We have also constructed another family of additive quantum codes of distance 2 using quantum codes of distance 3. It has also been established that there exists a and $[[n-1, n-m-2, 2]]$ $((n+1, K, 2))$ code.

Acknowledgements

This research work is supported by National Board for Higher Mathematics (NBHM), Mumbai, sanction number 2/48(1)/2012/NBHM/R&D II/10924 dated October 30, 2012

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Calderbank A, Rains EM, Shor PW, Sloane NJA. Quantum error correction via codes over GF(4). IEEE Trans. Inf. Theory. 1998;44:1369-1387.

[2] Gottesman D. Stabilizer codes and quantum error correction. Caltech Ph.D. dissertation, California Institute of Technology, Psadena, CA; 1997.

[3] Rains EM. Quantum codes of minimum distance two. IEEE Trans. Inf. Theory. 1999;45(1):266-271.

[4] Rains EM, Hardin RH, Shor PW, Sloane NJA. A nonadditive quantum code. Phys Rev Lett. 1997;79:953–954.

[5] Smolin JA. Smith G. Wehner S. A simple family of nonadditive quantum codes. arXiv:quant-ph/0701065v2; 2007.

[6] Feng K, Xing CP. A new construction on quantum error-correcting codes. Trans. Amer. Math. Soc. 2008;360:2007–2019.

[7] Aggarwal V, Calderbank A. Boolean functions, projection operators and quantum error correcting codes. IEEE Trans. Inf. Theory. 2008;54:1700-1707.

[8] Cross A, Smith G, Smolin JA, Zeng B. Codeword stabilized quantum codes. IEEE Trans. Inf. Theory. 2009;55:433-438.

[9] Rains EM. Quantum shadow enumerators. IEEE Trans. Inf. Theory. 1999;45(7):2361-2366.

[10] Rains EM. Quantum weight enumerators. IEEE Trans. Inf. Theory. 1998;44:1388-1394.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
www.sciencedomain.org/review-history.php?iid=735&id=6&aid=7758