American Journal of Applied Mathematics and Statistics, 2015, Vol. 3, No. 2, 76-79
Available online at http://pubs.sciepub.com/ajams/3/2/6

DOI:10.12691/ajams-3-2-6

Undetected Error Probability for Quantum Codes

Manish Gupta[1], R.K. Narula[2], Divya Taneja[3,4,*]

[1]Baba Farid College of Engineering & Technology Bathinda, Punjab, India
[2]PIT, Mansa, Punjab, India
[3]Yadavindra College of Engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo, Punjab, India
[4]Research Scholar Punjab Technical University, Jalandhar, Punjab, India
*Corresponding author: dtaneja25@yahoo.co.in

Received April 02, 2015; Revised April 10, 2015; Accepted April 15, 2015

Abstract From last fourteen years the work on undetected error probability for quantum codes has been silent. The undetected error probability has been discussed by Ashikhmin [3] in which it was proved that the average probability of undetected error for a given code is essentially given by a function of its weight enumerators. In this paper, new upper bounds on undetected error probability for quantum codes used for error detection on depolarization channel are given. It has also been established that the probability of undetected errors for quantum codes over depolarization channel do satisfy the upper bound analogous to classical codes.

Keywords: *additive codes, stabilizer, pure and impure codes, weight enumerator, probability of undetected error*

Cite This Article: Manish Gupta, R.K. Narula, and Divya Taneja, "Undetected Error Probability for Quantum Codes." *American Journal of Applied Mathematics and Statistics*, vol. 3, no. 2 (2015): 76-79. doi: 10.12691/ajams-3-2-6.

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. Quantum error correcting codes 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.

The construction of additive quantum codes using additive classical codes C over GF(4) is given in [1]. An important class of quantum codes called Stabilizer codes is defined in [1] and [4] which are analogous to the quantum additive codes. Among the additive codes the minimum distance two codes are those which correct any single qubit erasure. These distance two codes have been extensively studied and several constructions of both additive and nonadditive distance 2 codes are available in [1,2,5,7,8,9,11]. In our earlier work [14], we have also studied these distance 2 codes and now are in a position to find their undetected error probability.

In classical coding theory decoding is done by observing the received vector. If the received vector is not contained in the code space then an error is detected. An error remains undetected if the sent vector and the error vector sum up to a code word in the code space itself. The probability of undetected error for a $[n,k,d]$ code is given by

$$P_u(p)=\sum_{i=1}^{n}A_i(p)^i(1-p)^{n-i},0\le p\le\frac{1}{2}$$

where A_i is the number of code words of weight *i* in code. It was shown in [13] that the undetected error probability, when used solely for error detection on binary symmetric channel with crossover probability $p\le\frac{1}{2}$, is upper bounded by $2^{-(n-k)}$. In quantum case, the error will not be detected if the measured transmission results in the code itself and is not orthogonal or collinear to transmitted state vector. The probability of undetected error in this case, as shown by [3] can be computed via the weight enumerators of quantum codes. For a stabilizer code this probability is given by

$$P_{ue}(Q,p)=\sum_{i=0}^{n}(B_i^{\perp}-B_i)\left(\frac{p}{3}\right)^i(1-p)^{n-i}$$

where $0\le p\le\frac{3}{4}$ and B_i and $B_i^{\perp}$ are the weight distributions of the quantum codes as defined in [10].

The optimal distance 2 codes along with their stabilizer structures and their explicit basis were found in our earlier work [14]. In this paper, the probability of undetected error for both $\left[\left[n,n-2,2\right]\right]$ and $[[n,n-3,2]]$ code have been found. This probability function is further proved to be monotonic increasing having an upper bound $2^{-(n-k)}$ which is same as classical codes as given in [13].

2. Probability of Undetected Error

In [14] we have shown that the $[\left[2m,2m-2,2\right]]$ code is constructed from a classical additive self dual code $C=[2m,2]$ whose generator matrix is

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

The direct sum of C with $C_1=\{0,1\}$ is used to construct the $[\left[2m+1,2m-2,2\right]]$ code whose generator matrix is

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

In this paper, the probability of undetected error for both $\left[\left[n,n-2,2\right]\right]$ and $[\left[n,n-3,2\right]]$ code have been found. This probability function is further proved to be monotonic increasing having an upper bound $2^{-(n-k)}$ which is same as classical codes.

2.1. Undetected Error Probability for Even Length $[\left[\mathbf{n},\mathbf{n}-2,2\right]]$ Quantum Code

The weight enumerators of the $[\left[n,n-2,2\right]]$ quantum code are

$$B(x)=1+3x^n$$

and

$$B^{\perp}(x)=\sum_{i=0}^{n}B_i^{\perp}x^i.$$

Also by MacWilliams Identity [6]

$$B^{\perp}(x)=\frac{dimQ}{2^n}(1+3x)^n\,B\left(\frac{1-x}{1+3x}\right)$$

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

$$=\frac{1}{4}\left((1+3x)^n+3(1-x)^n\right)$$

$$P_{ue}(Q,p)=\sum_{i=0}^{n}(B_i^{\perp}-B_i)\left(\frac{p}{3}\right)^i(1-p)^{n-i}$$

$$=(1-p)^n\sum_{i=0}^{n}(B_i^{\perp}-B_i)\left(\frac{p}{3(1-p)}\right)^i$$

$$=\frac{1}{4}\left[1+3\left(\frac{3-4p}{3}\right)^n\right]-(1-p)^n-3\left(\frac{p}{3}\right)^n$$

$$\frac{dP_{ue}}{dp}=n\left[(1-p)^{n-1}-\left(1-\frac{4p}{3}\right)^{n-1}-\left(\frac{p}{3}\right)^{n-1}\right].$$

We shall prove by induction that for

$$0\le p\le\frac{3}{4},\frac{dP_{ue}}{dp}\ge 0.$$

Now for $n=2$

$$\frac{dP_{ue}}{dp}=0.$$

Let us assume for $n=k,\frac{dP_{ue}}{dp}\ge 0$

$$(1-p)^{k-1}-\left(1-\frac{4p}{3}\right)^{k-1}-\left(\frac{p}{3}\right)^{k-1}\ge 0.$$

Now

$$(1-p)^k=(1-p)(1-p)^{k-1}$$

$$\ge\left(\frac{p}{3}+\left(1-\frac{4p}{3}\right)\right)\left(\left(1-\frac{4p}{3}\right)^{k-1}+\left(\frac{p}{3}\right)^{k-1}\right)$$

$$\ge\left(1-\frac{4p}{3}\right)^k+\left(\frac{p}{3}\right)^k\quad\text{for}\quad 0\le p\le\frac{3}{4}$$

Thus

$$\frac{dP_{ue}}{dp}\ge 0,\text{ for } n=k+1.$$

Thus by induction

$$\frac{dP_{ue}}{dp}\ge 0\quad\text{for}\quad 0\le p\le\frac{3}{4}.$$

and hence $P_{ue}(Q,p)$ s an increasing function in this interval.

Now for $0\le p\le\frac{3}{4}$

$$P_{ue}(Q,p)\le\frac{1}{4},\quad\forall n\ge 2.$$

Thus $P_{ue}(Q,p)$ is upper bounded by $2^{-(n-k)}$.

2.2. Undetected Error Probability of Odd Length $\left[\left[\mathbf{n},\mathbf{n}-3,2\right]\right]$ Quantum Code

The odd length $[\left[n,n-3,2\right]]$ quantum codes are obtained by taking the direct sum of the classical even length $[n-1,2]$ code C over $GF(4)$ with $C_1=\{0,1\}$.

Now from [12], the weight enumerator of the resulting classical code will be

$$A^{'}(x)=\left(1+3x^{n-1}\right)(1+x).$$

Hence, the weight enumerator of the quantum $[\left[n,n-3,2\right]$ code will be

$$B^{'}(x) = A^{'}(x)$$

and

$$B^{'\perp}(x) = \frac{dimQ}{2^n}(1+3x)^n B^{'}\left(\frac{1-x}{1+3x}\right)$$

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

$$P_{ue}(Q,p) = \sum_{i=0}^{n}(B_i^{\perp}-B_i)\left(\frac{p}{3}\right)^i(1-p)^{n-i}$$

$$= \begin{bmatrix} \frac{1}{8}\left\{1+\frac{3-4p}{3}+3\left(\frac{3-4p}{3}\right)^{n-1}+3\left(\frac{3-4p}{3}\right)^n\right\} \\ -(1-p)^n-\frac{p(1-p)^{n-1}}{3} \\ -3\left(\frac{p}{3}\right)^{n-1}(1-p)-3\left(\frac{p}{3}\right)^n \end{bmatrix}$$

$$\frac{dP_{ue}}{dp} = -\frac{1}{6}-\frac{(n-1)}{2}\left(\frac{3-4p}{3}\right)^{n-2}$$
$$-\frac{n}{2}\left(\frac{3-4p}{3}\right)^{n-1}+n(1-p)^{n-1}$$
$$-\frac{1}{3}(1-p)^{n-1}+(n-1)\frac{p}{3}(1-p)^{n-2}$$
$$-(n-1)\left(\frac{p}{3}\right)^{n-2}(1-p)+3\left(\frac{p}{3}\right)^{n-1}-n\left(\frac{p}{3}\right)^{n-1}$$

We shall prove that

$$\frac{dP_{ue}}{dp} \geq 0, \text{ for } 0 \leq p \leq \frac{3}{4}.$$

Now

$$\frac{dP_{ue}}{dp} \geq 0$$

if

$$Z = -\frac{1}{6}-\frac{(n-1)}{2}\left(\frac{3-4p}{3}\right)^{n-2}$$
$$-\frac{n}{2}\left(\frac{3-4p}{3}\right)^{n-1}+n(1-p)^{n-1}$$
$$-\frac{1}{3}(1-p)^{n-1}-n\left(\frac{p}{3}\right)^{n-1} \geq 0$$

When $p = 0, Z = 0$.

Let us assume $Z \geq 0$, for $n = k$.

That is

$$\frac{1}{6}-\frac{(k-1)}{2}\left(\frac{3-4p}{3}\right)^{k-2}$$
$$-\frac{k}{2}\left(\frac{3-4p}{3}\right)^{k-1}+k(1-p)^{k-1}$$
$$-k\left(\frac{p}{3}\right)^{k-1}-\frac{1}{3}(1-p)^{k-1} \geq 0$$

We shall prove that $Z \geq 0$ for $n = k+1$.

Now

$$-\frac{1}{6}-\frac{k}{2}\left(\frac{3-4p}{3}\right)^{k-1}-\frac{k+1}{2}\left(\frac{3-4p}{3}\right)^k$$
$$+(k+1)(1-p)^k-(k+1)\left(\frac{p}{3}\right)^k-\frac{1}{3}(1-p)^k$$
$$\geq \frac{(k-1)}{2}\left(\frac{3-4p}{3}\right)^{k-2}-\frac{k+1}{2}\left(\frac{3-4p}{3}\right)^k$$
$$+(k+1)(1-p)^k-k(1-p)^{k-1}-(k+1)\left(\frac{p}{3}\right)^k$$
$$+k\left(\frac{p}{3}\right)^{k-1}-\frac{1}{3}(1-p)^k+\frac{1}{3}(1-p)^{k-1}$$
$$\geq \frac{(k-1)}{2}\left(\frac{3-4p}{3}\right)^k-\frac{k+1}{2}\left(\frac{3-4p}{3}\right)^k$$
$$+(k+1)(1-p)^k-k(1-p)^{k-1}$$
$$-(k+1)\left(\frac{p}{3}\right)^k+k\left(\frac{p}{3}\right)^{k-1}$$
$$-\frac{1}{3}(1-p)^k+\frac{1}{3}(1-p)^{k-1}$$
$$\geq k(1-p)^k-k(1-p)^{k-1}-k\left(\frac{p}{3}\right)^k$$
$$+k\left(\frac{p}{3}\right)^{k-1}-\frac{1}{3}(1-p)^k+\frac{1}{3}(1-p)^{k-1}$$
$$\geq k\begin{bmatrix}\left((1-p)^k-\left(\frac{p}{3}\right)^k\right) \\ -\left((1-p)^{k-1}-\left(\frac{p}{3}\right)^{k-1}\right)\end{bmatrix} \geq 0$$

Thus

$$\frac{dP_{ue}}{dp} \geq 0 \text{ for } 0 \leq p \leq \frac{3}{4}$$

and hence $P_{ue}(Q,p)$ is an increasing function in this interval.

Now for $0 \leq p \leq \frac{3}{4}$

$$P_{ue}(Q,p) \leq \frac{1}{8}, \ \forall n \geq 3.$$

Thus the $P_{ue}(Q,p)$ is upper bounded by $2^{(-(n-k))}$.

Thus we have proved that quantum $[[n, n-2, 2]]$ and $[[n, n-3, 2]]$ codes obeys the 2^{-p} bound, *where* $p = n-k$. This result is similar to the general rule for the classical linear block codes as given in [13].

2.2.1. Remark

We have also verified that this bound is satisfied by the quantum Hamming codes

$$\left[\left[\frac{2^{2m}-1}{3},\frac{2^{2m}-1}{3}-2m,3\right]\right] \text{ where } m \geq 2.$$

The probability of undetected error of these codes is

$$P_{ue}(Q,p)=\frac{1}{3n+1}\left[1+3n\left(\frac{3-4p}{3}\right)^{\frac{3n+1}{4}}\right]$$
$$-(1-p)^n-3n\left(\frac{p}{3}\right)^{\frac{3n+1}{4}}(1-p)^{\frac{n-1}{4}}.$$

This is a monotonic increasing function of p giving an upper bound $2^{-(n-k)}$. Many more quantum codes satisfy this bound.

In classical codes there are certain codes [13], in which this bound is not satisfied so such violation in quantum additive codes would be the topic of further investigation

3. Conclusion

The probability of undetected error for optimal distance 2 codes was found to be increasing functions and satisfies the upper bound $2^{-(n-k)}$ which is same as the classical bound.

Acknowledgement

This research work is supported by National Board for Higher Mathematics (NBHM), Mumbai with Ref. No. 2/48(1)/2012/NBHM/R&D11/10924.

One of the author, Divya Taneja also acknowledges Punjab Technical University, Jalandhar, Punjab for providing the research facilities.

References

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

[2] Cross, A., Smith, G., Smolin, J.A. and Zeng, B., "Codeword Stabilized Quantum Codes." *IEEE Trans. Inf. Theory*,vol.55, pp. 433-438, 2009.

[3] Ashikhmin, A. E., Barg, A. M., Knill, E.and Litsyn, S. N., "Quantum Error Detection I: Statement of the Problem", *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 778-788, 2000.

[4] Gottesman, D., "Stabilizer Codes and Quantum Error Correction," Caltech Ph.D. dissertation, California Institute of Technology, Psadena, CA, 1997.

[5] Rains, E. M., "Quantum codes of minimum distance two," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 266-271, 1999.

[6] Rains, E. M., "Quantum shadow enumerators", *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2361- 2366, 1999.

[7] Rains, E. M., Hardin, R. H., Shor, P. W. and Sloane, N. J. A.,"A nonadditive quantum code," *Phys. Rev. Lett.*, vol. 79, pp. 953-954,1997.

[8] Smolin, J. A., Smith, G., and Wehner, S., "A simple family of nonadditive quantum codes" arXiv: quant-ph/0701065v2, 2007.

[9] Feng, K. and Xing, C. P., "A new construction on quantum error-correcting codes," *Trans. Amer. Math. Soc.*, vol. 360, pp. 2007-2019, 2008.

[10] Shor, P. W. and Laflamme, R., "Quantum analog of the MacWilliams identities in classical coding theory," *Phys. Rev. Lett.*, vol. 78, pp. 1600-1602, 1997.

[11] Aggarwal, V. and Calderbank, R., "Boolean Functions, Projection Operators and Quantum Error Correcting Codes."*IEEE Trans. Inf. Theory*, vol.54, pp. 1700-1707, 2008.

[12] Cary Huffman, W. and Vera Pless, "Fundamentals of Error-Correcting Codes." Cambridge University Press, 2003.

[13] Leung-Yan-Cheong, S. K. and Hellman, M.E. "Concerning a bound on undetected error probability," *IEEE Trans. Inf. Theory*, vol. IT- 22. pp. 235-231, 1976.

[14] Gupta, M., Narula, R. K and Taneja, D., "On the Construction of Odd Length Quantum Codes,"British Journal of Mathematics & Computer Science 6(5), pp. 444-450, 2015.