On The Undetected Error Probability for Quantum Hamming Codes Quantum Coding

Divya Taneja
Assistant Professor
Yadavindra College of Engineering
Talwandi Sabo, Punjab
Email: dtaneja25@yahoo.co.in

Manish Gupta
Associate Professor
Baba Farid College of Engineering & Technology
Bathinda, Punjab.

R.K. Narula
Assistant Professor
PIT
Mansa, Punjab.

Abstract-*We give a construction of quantum Hamming code using classical self orthogonal code over GF(4). The Undetected Error Probability, used for error detection on depolarization channel, of this code is calculated and it has been proved that this probability function is monotonic increasing function satisfying the upper bound* $\mathbf{2}^{-(n-k)}$ *which is analogous to the classical bound.*

Keywords-*additive codes; quantum Hamming codes; undetected error; weight enumerators; undetected error probability.*

I. Introduction

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 selforthogonal with respect to a certain symplectic inner product. An [[n, k, d]] code is an additive quantum code of minimum distance d and length n encoding k quantum bits. The construction of additive quantum codes using additive classical codes C over GF(4) is given in [1].

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

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

where A_i is the number of code words of weight i in code. It was shown in [3] 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 [2] 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 [4].

In this paper we have constructed quantum Hamming codes giving its weight enumerators and then calculated the undetected error probability of these codes. We have proved that this probability function is monotonic increasing and attains the upper bound which is equivalent to the classical case.

II. Quantum Hamming Codes and Undetected Error Probability

A. Quantum Hamming Codes

The classical Hamming codes over GF(4) as defined in [5], are of length $\frac{2^{2m}-1}{3}$, with dimension $\frac{2^{2m}-1}{3} - m$ and minimum distance 3, where $m \ge 2$. The dual of this code is a self orthogonal code $\left[\frac{2^{2m}-1}{3}, m, 2^{2(m-1)}\right]$ with codes of constant weight $2^{2(m-1)}$. Thus, by the construction of additive quantum codes given in Calderbank *et.al.*[1], we have the existence of the

quantum code $\left[\left[\frac{2^{2m}-1}{3}, \frac{2^{2m}-1}{3}-2m, 3\right]\right]$. These codes are equivalent to the codes $[[n, n-m-2, 3]]$, where $n = \sum_{i=0}^{m/2} 2^{2i}$ and even $m \geq 2$ discovered by [1] and [6].

A. *Undetected Error Probability*

The weight enumerators of quantum Hamming code are

$$B(x) = 1 + (2^{2m} - 1)x^{2^{2(m-1)}}$$

Also by MacWilliams Identity [7]

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

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

$$= \frac{1}{2^{2m}}\Bigg[(1+3x)^{n} + (2^{2m} - 1)(1-x)^{2^{2(m-1)}}(1+3x)^{\frac{2^{2(m-1)}-1}{3}}\Bigg]$$

Now

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

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

$$= \frac{1}{2^{2m}}\left[1 + (2^{2m}-1)\left(\frac{3-4p}{3}\right)^{2^{2(m-1)}}\right] - (1-p)^{n} - (2^{2m} - 1)\left(\frac{p}{3}\right)^{2^{2(m-1)}}(1-p)^{n-2^{2(m-1)}}$$

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

$$\frac{dP_{ue}}{dp} = -n\left(\frac{3-4p}{3}\right)^{\frac{3(n-1)}{4}} + n(1-p)^{n-1} - n\left(\frac{3n+1}{4}\right)\left(\frac{p}{3}\right)^{3\left(\frac{n-1}{4}\right)}(1-p)^{\frac{n-1}{4}} + 3n\left(\frac{n-1}{4}\right)\left(\frac{p}{3}\right)^{\frac{3n+1}{4}}(1-p)^{\frac{n-5}{4}}$$

Now

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

if

$$(1-p)^{n-1} + 3\left(\frac{n-1}{4}\right)\left(\frac{p}{3}\right)^{\frac{3n+1}{4}}(1-p)^{\frac{n-5}{4}} - \left(\frac{3-4p}{3}\right)^{\frac{3(n-1)}{4}} - \left(\frac{3n+1}{4}\right)\left(\frac{p}{3}\right)^{3\left(\frac{n-1}{4}\right)}(1-p)^{\frac{n-1}{4}} \geq 0$$

We shall prove this by induction

For $n = 5$, we have

$$(1-p)^{4} + 3\left(\frac{p}{3}\right)^{4} - \left(\frac{3-4p}{3}\right)^{3} - \left(\frac{p}{3}\right)^{3}(1-p) = \frac{32}{27}p^{4} - \frac{48}{27}p^{3} + \frac{2}{3}p^{2} = \frac{2p^{2}}{3}\left(\frac{4}{3}p - 1\right)^{2} \geq 0$$

Thus the result is true for $n = 5$.

Let us assume the result is true for $n = k$

$$(1-p)^{k-1} + 3\left(\frac{k-1}{4}\right)\left(\frac{p}{3}\right)^{\frac{3k+1}{4}}(1-p)^{\frac{k-5}{4}} - \left(\frac{3-4p}{3}\right)^{\frac{3(k-1)}{4}} - \left(\frac{3k+1}{4}\right)\left(\frac{p}{3}\right)^{3\left(\frac{k-1}{4}\right)}(1-p)^{\frac{k-1}{4}} \geq 0$$

We shall prove it for $n = k+1$

Now

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

$$\geq (1-p)\left\{-3\left(\frac{k-1}{4}\right)\left(\frac{p}{3}\right)^{\frac{3k+1}{4}}(1-p)^{\frac{k-5}{4}} + \left(\frac{3-4p}{3}\right)^{\frac{3(k-1)}{4}} + \left(\frac{3k+1}{4}\right)\left(\frac{p}{3}\right)^{3\left(\frac{k-1}{4}\right)}(1-p)^{\frac{k-1}{4}}\right\}$$

$$\geq (1-p)\left\{-3\left(\frac{k-1}{4}\right)\left(\frac{p}{3}\right)^{\frac{3k+1}{4}}(1-p)^{\frac{k-5}{4}} + \left(\frac{3k+1}{4}\right)\left(\frac{p}{3}\right)^{3\left(\frac{k-1}{4}\right)}(1-p)^{\frac{k-1}{4}}\right\} + \left(\frac{3-4p}{3}\right)^{\frac{3k}{4}}$$

since $(1-p) \geq \left(\frac{3-4p}{3}\right)^{\frac{3}{4}}$ $for\ 0 \leq p \leq \frac{3}{4}$

$$= (1-p)\left\{\left(\frac{k(3-4p)+1}{4}\right)\left(\frac{p}{3}\right)^{\frac{3(k-1)}{4}}(1-p)^{\frac{k-5}{4}}\right\} + \left(\frac{3-4p}{3}\right)^{\frac{3k}{4}}$$

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

$$(1-p)\left(\frac{k(3-4p)+1}{4}\right)\left(\frac{p}{3}\right)^{\frac{3(k-1)}{4}}(1-p)^{\frac{k-5}{4}} \geq \left(\frac{(k+1)(3-4p)+1}{4}\right)\left(\frac{p}{3}\right)^{\frac{3k}{4}}(1-p)^{\frac{k-1}{4}}$$

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

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

Which is true for $k = 5$ and for$k > 5$, the right hand side decreases and hence this is true for all $k \geq 5$.

Thus we have

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

Thus

$$\frac{dP_{ue}}{dp} \geq 0 \text{ for all } n \geq 5 \text{ and } 0 \leq p \leq \frac{3}{4}$$

Hence $P_{ue}(Q,p)$ is an increasing function for $0 \leq p \leq \frac{3}{4}$ and

$$P_{ue}(Q,p) \leq \frac{1}{2^{2m}} = 2^{-(n-k)}$$

$$\text{for } 0 \leq p \leq \frac{3}{4} \text{ and } m \geq 2.$$

This gives an upper bound on the undetected error probability of quantum Hamming codes which is same as the classical bound given in [3].

III. Conclusion

We have constructed Hamming quantum codes using classical codes over GF(4). The probability of undetected error for these codes was increasing functions and satisfies the upper bound $2^{-(n-k)}$which is same as the classical bound.

References

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

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

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

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

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

[6] D. Gottesman, "Pasting quantum codes," LANL e-print quant-ph/9607027.

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