

On Quantum Hamming Bound

Salah A. Aly
Department of Computer Science,
Texas A&M University,
College Station, TX 77843-3112, USA
Email: salah@cs.tamu.edu

We prove quantum Hamming bound for stabilizer codes of minimum distance $d = 5$. Also, we compute the maximum length of single and double MDS stabilizer codes over finite fields.

1 Bounds on Quantum Codes

It is desirable to study upper and lower bounds on the minimum distance and dimensions of quantum codes, so the computer search on the code parameter can be minimized and optimal codes can be known. It is a well-known fact that Singleton and Hamming bounds hold for classical codes [9].

We need some bounds on the achievable minimum distance of a quantum stabilizer code. Perhaps the simplest one is the Knill-LaFlamme bound, also called the quantum Singleton bound. The binary version of the quantum Singleton bound was first proved by Knill and Laflamme in [12], see also [1,2], and later generalized by Rains using weight enumerators in [16].

Theorem 1 (Quantum Singleton Bound). *An $((n, K, d))_q$ stabilizer code with $K > 1$ satisfies*

$$K \leq q^{n-2d+2}.$$

Codes which meet the quantum Singleton bound are called quantum MDS codes. In [11] It has been shown that these codes cannot be indefinitely long and showed that the maximal length of a q -ary quantum MDS codes is upper bounded by $2q^2 - 2$. This could probably be tightened to $q^2 + 2$. It would be interesting to find quantum MDS codes of length greater than $q^2 + 2$ since it would disprove the MDS Conjecture for classical codes [9]. A related open question is regarding the construction of codes with lengths between q and $q^2 - 1$. At the moment there are no analytical methods for constructing a quantum MDS code of arbitrary length in this range (see [8] for some numerical results).

Another important bound for quantum codes is the quantum Hamming bound. The quantum Hamming bound states (see [5,6]) that:

Theorem 2 (Quantum Hamming Bound). *Any pure $((n, K, d))_q$ stabilizer code satisfies*

$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q^2 - 1)^i \leq q^n / K.$$

So far no degenerate quantum code has been found that beats this bound. Gottesman showed that impure single and double error-correcting binary quantum codes cannot beat the quantum Hamming bound [7]. It is proved in [11] that Hamming bound holds for quantum stabilizer codes with distance $d = 3$.

In general, does Hamming bound exist for any distance d in $((n, K, d))_q$ stabilizer codes? This has been an open question for a decade. In this note we prove Hamming bound for double error-correcting stabilizer codes with distance $d = 5$.

2 Quantum Hamming Bound Holds For $d = 5$

In [1] Ashikhmin and Litsyn derived many bounds for quantum codes by extending a novel method originally introduced by Delsarte [4] for classical codes. Using this method they proved the binary versions of Theorem 3 and Theorem 1. We use this method to show that the Hamming bound holds for all double error-correcting quantum codes. See [11] for a similar result for single error-correcting codes. But first we need the Theorem 3 and the Krawtchouk polynomial of degree j in the variable x ,

$$K_j(x) = \sum_{s=0}^j (-1)^s (q^2 - 1)^{j-s} \binom{x}{s} \binom{n-x}{j-s}.$$

Theorem 3. *Let Q be an $((n, K, d))_q$ stabilizer code of dimension $K > 1$. Suppose that S is a nonempty subset of $\{0, \dots, d-1\}$ and $N = \{0, \dots, n\}$. Let*

$$f(x) = \sum_{i=0}^n f_i K_i(x)$$

be a polynomial satisfying the conditions

- i) $f_x > 0$ for all x in S , and $f_x \geq 0$ otherwise;*
- ii) $f(x) \leq 0$ for all x in $N \setminus S$.*

Then

$$K \leq \frac{1}{q^n} \max_{x \in S} \frac{f(x)}{f_x}.$$

Proof. See [11]. □

We demonstrate usefulness of the previous theorem by showing that quantum Hamming bound holds for impure codes also when $d = 5$.

Corollary 4 (Quantum Hamming Bound). *An $((n, K, 5))_q$ stabilizer code with $K > 1$ satisfies*

$$K \leq q^n / (n(n-1)(q^2-1)^2/2 + n(q^2-1) + 1).$$

Proof. Let $f(x) = \sum_{j=0}^n f_j K_j(x)$, where $f_x = (\sum_{j=0}^e K_j(x))^2$, $S = \{0, 1, \dots, 4\}$ and $N = \{0, 1, \dots, n\}$. Calculating $f(x)$ and f_x gives us

$$\begin{aligned} f_0 &= (1 + n(q^2 - 1) + n(n-1)(q^2 - 1)^2/2)^2 \\ f_1 &= \frac{1}{4}(n-1)^2(n-2)^2(q^2 - 1)^4 \\ f_2 &= \left(\frac{1}{2}(n-3)(n-2)(q^2 - 1)^2 - (n-2)(q^2 - 1)\right)^2 \\ f_3 &= (1 - 2(n-3)(q^2 - 1) + \frac{1}{2}(n-4)(n-3)(q^2 - 1)^2)^2 \\ f_4 &= (3 - 3(n-4)(q^2 - 1) + \frac{1}{2}(n-5)(n-4)(q^2 - 1)^2)^2 \end{aligned}$$

and,

$$\begin{aligned} f(0) &= q^{2n}(1 + n(q^2 - 1) + \frac{1}{2}(n-1)n(q^2 - 1)^2) \\ f(1) &= q^{2n}(q^2 + 2(n-1)(q^2 - 1) + (n-1)(q^2 - 2)(q^2 - 1)) \\ f(2) &= q^{2n}(4 + 4(q^2 - 2) + (q^2 - 2)^2 + 2(n-2)(q^2 - 1)) \\ f(3) &= q^{2n}(6 + 6(q^2 - 2)) \\ f(4) &= 6q^{2n}. \end{aligned}$$

Clearly $f_x > 0$ for all $x \in S$. Also, $f(x) \leq 0$ for all $x \in N \setminus S$ since the binomial coefficients for negative values are zero. The Hamming bound is given by

$$K \leq q^{-n} \max_{s \in S} \frac{f(x)}{f_x}$$

So, there are four different comparisons where $f(0)/f_0 \geq f(x)/f_x$, for $x = 1, 2, 3, 4$. We find a lower bound for n that holds for all values of q .

For $n \geq 7$ it follows that

$$\max\{f(0)/f_0, f(1)/f_1, f(2)/f_2, f(3)/f_3, f(4)/f_4\} = f(0)/f_0$$

□

While the above method is a general method to prove Hamming bound for impure quantum codes, the number of terms increases with a large minimum distance. It becomes difficult to find the true bound using this method. However, one can derive more consequences from Theorem 3; see, for instance, [1, 2, 13, 15].

Lemma 5. *The inequality $f(0)/f_0 \geq f(1)/f_1$ holds for $n \geq 6$ and $q \geq 2$.*

Proof. Let $f(0)/f_0 \geq f(1)/f_1$ then

$$\frac{1}{1 + n(q^2 - 1) + n(n-1)(q^2 - 1)^2/2} \geq \frac{4q^2((n-1)(q^2 - 1) + 1)}{(n-1)^2(n-2)^2(q^2 - 1)^4}$$

$$(n-1)^2(n-2)^2(q^2 - 1)^4 \geq (1 + n(q^2 - 1))$$

$$+ \frac{n(n-1)}{2}(q^2 - 1)^2(4q^2((n-1)(q^2 - 1) + 1))$$

in the left side $(n-1)$ approximates to $(n-2)$. Also, in the right side $(n-2)$ and $(n-1)$ approximate to (n) . So,

$$(n-2)^4(q^2 - 1)^4 \geq 4(1 + n(q^2 - 1)) + \frac{n^2}{2}(q^2 - 1)^2(q^2(q^2 - 1)(n-1) + 1)$$

divide both sides by $(q^2 - 1)^2(q^2 - 1)^2$ and approximate $\frac{1}{q^2-1} \leq 1$, we find that

$$(n-2)^4 \geq 8(1 + n + \frac{n^2}{2})(n-1)$$

by approximating both sides, the final result is $(n-2) \geq 4$ or

$$n \geq 6$$

□

Lemma 6. *The inequality $f(0)/f_0 \geq f(2)/f_2$ holds for $n \geq 7$ and $q \geq 2$.*

Proof. Let

$$\frac{q^{2n}}{1 + n(q^2 - 1) + n(n-1)(q^2 - 1)^2/2} \geq \frac{q^{2n}(q^4 + 2(n-2)(q^2 - 1))}{(-(n-2)(q^2 - 1) + (n-3)(n-2)(q^2 - 1)^2/2)^2}$$

by simplifying both sides

$$\frac{(-(n-2)(q^2 - 1) + (n-3)(n-2)(q^2 - 1)^2/2)^2}{(q^4 + 2(n-2)(q^2 - 1))(1 + n(q^2 - 1) + n(n-1)(q^2 - 1)^2/2)} \geq \quad (1)$$

Simplify L.H.S $(n-2)$ to $(n-3)$ then

$$(q^2 - 1)^4((n-3)^2/2 - (n-2))^2 \geq \quad (2)$$

$$(q^4 + 2(n-2)(q^2 - 1))(1 + n(q^2 - 1) + n(n-1)(q^2 - 1)^2/2) \geq \quad (3)$$

by simplifying both sides

$$((n-3)^2/2 - (n-2))^2 \geq \left(\frac{q^2}{(q^2 - 1)^2} + \frac{2(n-2)}{q^2 - 1}\right)(1 + n + n(n-1)/2)$$

$$((n-3)^2/2 - (n-2))^2 \geq 2(2n+1)(n^2 + 2n + 2)$$

$$(n-3)^2((n-3)/2 - 1)^2 \geq 2(2n+1)((n+1)^2 + 1)$$

$$(n-5)^2/4 \geq 2(2n+1)$$

$$n \geq 7$$

□

Lemma 7. *The inequality $f(0)/f_0 \geq f(3)/f_3$ holds for $n \geq 7$ and $q \geq 2$.*

Proof. We start by proposing that

$$\frac{q^{2n}}{1 + n(q^2 - 1) + n(n-1)(q^2 - 1)^2/2} \geq \frac{6q^{2n}(q^2 - 1)}{(1 - 2(n-3)(q^2 - 1) + (n-3)(n-4)(q^2 - 1)^2/2)^2}$$

by simplification

$$\begin{aligned} (1 - 2(n-3)(q^2 - 1) + (n-3)(n-4)(q^2 - 1)^2/2)^2 &\geq \\ 6(q^2 - 1)(1 + n(q^2 - 1) + n(n-1)(q^2 - 1)^2/2) & \\ \frac{((n-4)^2(q^2 - 1)^2 - 4(n-4)(q^2 - 1) + 2)^2}{4} &\geq \\ 6(q^2 - 1)(1 + n(q^2 - 1) + n(n-1)(q^2 - 1)^2/2) & \end{aligned}$$

by approximation to $(q^2 - 1)$

$$\begin{aligned} \frac{(q^2 - 1)^4}{4}((n-5)^4) &\geq 3(q^2 - 1)^3(2 + 2n + n^2) \\ (n-5)^4 &\geq 4(2 + 2n + n^2) \\ (n-5)^2 &\geq 2 \\ n &\geq 7 \end{aligned}$$

□

Lemma 8. *The inequality $f(0)/f_0 \geq f(4)/f_4$ holds for $n \geq 7$ and $q \geq 2$.*

Proof. Let

$$\begin{aligned} &\frac{q^{2n}}{1 + n(q^2 - 1) + n(n-1)(q^2 - 1)^2/2} \\ &\geq \frac{6q^{2n}}{(3 - 3(n-4)(q^2 - 1) + (n-4)(n-5)(q^2 - 1)^2/2)^2} \end{aligned}$$

divide by q^{2n} and simplifying

$$\begin{aligned} (3 - 3(n-4)(q^2 - 1) + (n-4)(n-5)(q^2 - 1)^2/2)^2 &\geq \\ 6(1 + n(q^2 - 1) + n(n-1)(q^2 - 1)^2/2) & \end{aligned}$$

then by approximating $(n-4)$ to $(n-5)$ in L.H.S and $(n-1)$ to $4n$ in R.H.S, we can find that

$$(-3(n-4)(q^2 - 1) + (n-5)^2(q^2 - 1)^2/2)^2 \geq 6(1 + n(q^2 - 1) + n^2(q^2 - 1)^2/2)$$

$$((n-5)^2(q^2 - 1) + (n-5)^2(q^2 - 1)^2/2)^2 \geq 6(1 + n(q^2 - 1) + n^2(q^2 - 1)^2/2)$$

$$(q^2 - 1)^4((n - 5)^2 + (n - 5)^2/2)^2 \geq 6(1 + n(q^2 - 1) + n^2(q^2 - 1)^2/2)$$

dividing both sides by $(q^2 - 1)^4$ and simplifying

$$(9/4)(n - 5)^4 \geq \frac{6(1 + n(q^2 - 1) + n^2(q^2 - 1)^2/2)}{(q^2 - 1)^4}$$

$$\begin{aligned} (9/4)(n - 5)^4 &\geq 6(1 + n + n^2) \\ n &\geq 7 \end{aligned}$$

□

Since it is not known if the quantum Hamming bound holds for degenerate quantum codes, it would be interesting to find degenerate quantum codes that either meet or beat the quantum Hamming bound. This is obviously a challenging open research problem.

3 Maximal length of MDS codes

In this section we derive some results on the maximal length of single error correcting and double error correcting quantum MDS codes. These bounds hold for all additive quantum codes.

3.1 Maximal length single error correcting MDS codes

Lemma 9 (Maximal length single error correcting MDS codes). *The maximal length of single error correcting additive quantum MDS codes is given by $q^2 + 1$.*

Proof. We know that the quantum Hamming bound holds for $K > 1$ for $d = 3$, so

$$K \leq \frac{q^n}{1 + n(q^2 - 1)} \quad (4)$$

If the Hamming bound is tighter than the Singleton bound for any $((n, K, 3))_q$ quantum code, then it means that MDS codes cannot exist for that set of n, K . This occurs when

$$q^{n-2d+2} = q^{n-4} \geq \frac{q^n}{1 + n(q^2 - 1)} \quad (5)$$

$$1 + n(q^2 - 1) \geq q^4 \quad (6)$$

$$n \geq q^2 + 1 \quad (7)$$

Thus there exist no single error correcting quantum MDS codes for $n > q^2 + 1$. □

3.2 Upper bound on the maximal length of double error correcting MDS codes

Lemma 10 (Upper bound on the maximal length of double error correcting MDS codes). *The maximal length of double error correcting quantum MDS codes is upperbounded by:*

$$n \leq \frac{(q^2 - 3) + \sqrt{((q^2 - 3) + 8(q^8 - 1))}}{2(q^2 - 1)} \quad (8)$$

Proof. It is known that the Hamming bound for $d = 5$ is given by:

$$K \leq \frac{q^n}{1 + n(q^2 - 1) + n(n - 1)(q^2 - 1)^2/2} \quad (9)$$

Same argument as in lemma 1, if the Hamming bound is tighter than the Singleton bound for any $((n, K, 5))_q$ quantum code, then it means that MDS codes cannot exist for that set of $[[n, K]]$. By simple computation, we find that

$$q^{n-2d+2} = q^{n-8} \geq \frac{q^n}{1 + n(q^2 - 1) + \frac{n(n-1)}{2}(q^2 - 1)^2} \quad (10)$$

$$n^2(q^2 - 1)^2 - n(q^2 - 1)(q^2 - 3) - 2(q^8 - 1) \geq 0 \quad (11)$$

So, the quadratic equation of n has two real solutions. This inequality holds for

$$n \leq \frac{(q^2 - 3) - \sqrt{((q^2 - 3)^2 + 8(q^8 - 1))}}{2(q^2 - 1)} \quad (12)$$

$$n \geq \frac{(q^2 - 3) + \sqrt{((q^2 - 3)^2 + 8(q^8 - 1))}}{2(q^2 - 1)} \quad (13)$$

Only the positive solution for n is valid. So, the maximal length of double error correcting MDS code is upper bounded by

$$n \leq \frac{(q^2 - 3) + \sqrt{((q^2 - 3)^2 + 8(q^8 - 1))}}{2(q^2 - 1)} \quad (14)$$

If $q = 2$, the Hamming bound is tighter than Singleton bound for $n \geq 8$

□

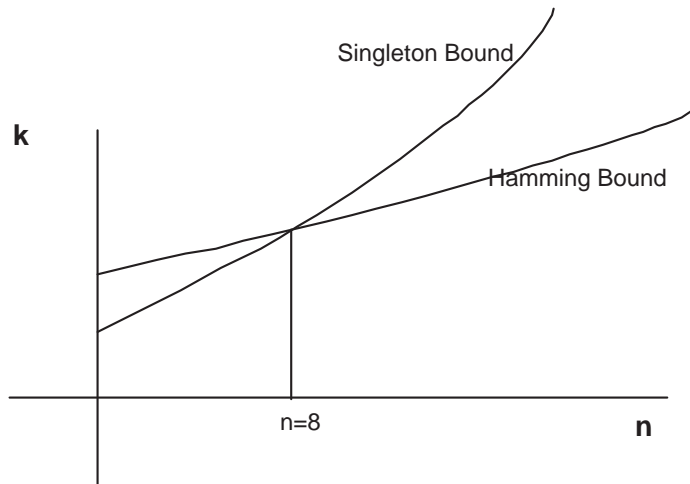


Figure 1: Comparison of Hamming and Singleton Bounds for $q=2$

References

- [1] A. Ashikhmin and S. Litsyn. Upper bounds on the size of quantum codes. *IEEE Trans. Inform. Theory*, 45(4):1206–1215, 1999.
- [2] A.E. Ashikhmin, A.M. Barg, E. Knill, and S.N. Litsyn. Quantum error detection II: Bounds. *IEEE Trans. on Information Theory*, 46(3):789–800, 2000.
- [3] P. Delsarte. Four fundamental parameters of a code and their combinatorial significance. *Information and Control*, 23(5):407–438, December 1973.
- [4] P. Delsarte. Bounds for unrestricted codes by linear programming. *Philips Res. Reports*, 27:272–289, 1972.
- [5] K. Feng and Z. Ma. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Trans. Inform. Theory*, 50(12):3323–3325, 2004.
- [6] D. Gottesman. A class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54:1862–1868, 1996.
- [7] D. Gottesman. Stabilizer codes and quantum error correction. Caltech Ph. D. Thesis, eprint: quant-ph/9705052, 1997.
- [8] M. Grassl, T. Beth, and M. Rötteler. On optimal quantum codes. *Internat. J. Quantum Information*, 2(1):757–775, 2004.
- [9] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. University Press, Cambridge, 2003.

- [10] A. Ketkar, A. Klappenecker, S. Kumar, and P. Sarvepalli. Non-binary quantum stabilizer codes. *Proc. of IEEE Infor. Trans.(in progress)*.
- [11] A. Ketkar, A. Klappenecker, S. Kumar, and P.K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, 2006.
- [12] E. Knill and R. Laflamme. A theory of quantum error-correcting codes. *Physical Review A*, 55(2):900–911, 1997.
- [13] V.I. Levenshtein. Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces. *IEEE Trans. Inform. Theory*, 41(5):1303–1321, 1995.
- [14] J.H Van Lint. Introduction to coding theory. *Third Edition, Springer-Verlag 1999*.
- [15] R.J. McEliece, E.R. Rodemich, jr. H. Rumsey, and L.R. Welch. New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities. *IEEE Trans. Inform. Theory*, 23(2):157, 1977.
- [16] E.M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45:1827–1832, 1999.

4 Appendix

This is an approach to prove quantum Hamming bound for stabilizer codes with minimum distance d .

Proof of Hamming Bound for Minimum Distance d

In this section, we proof Hamming bound for distance $d \leq (n - k + 2)/2$ in quantum stabilizer codes. We expand $f(x)/f_x$ in terms of Krawtchouk polynomials. Let $f(x) = \sum_{j=0}^n f_j K_j(x)$ and $f_x = (\sum_{i=0}^e K_i(x))^2$. The Krawtchouk polynomial of degree e in the variables x and q is

$$K_e(q, x) = \sum_{j=0}^e (-1)^j (q^2 - 1)^{e-j} \binom{x}{j} \binom{n-x}{e-j} \quad (15)$$

Before we proof Hamming bound, we refer to the following theorem [10].

Theorem 11. *Let Q be an $((n, K, d))_q$ stabilizer code of dimension $K > 1$. Suppose that S is a nonempty subset of $\{0, 1, \dots, d-1\}$ and $N = \{0, 1, \dots, n\}$. let*

$$f(x) = \sum_{i=0}^n f_i K_i(x)$$

be a polynomial satisfying the conditions:

- i) $f_x > 0$ for all $x \in S$, and $f_x \geq 0$ otherwise;
- ii) $f(x) \leq 0$ for all $x \in N \setminus S$.

Then

$$K \leq \frac{1}{q^n} \max_{x \in S} \frac{f(x)}{f_x}.$$

Notice that $f(x) = \sum_{i=0}^n f_i K_i(x)$ can be written as $f_i = q^{-2n} \sum_{x=0}^n f(x) K_x(i)$.

Lemma 12. *Let Q be an $((n, K, d))_q$ stabilizer code of dimension $k \geq 1$. Suppose that S is a non-empty subset of $\{0, 1, 2, \dots, 2e\}$, where $e = \lfloor \frac{d-1}{2} \rfloor$. The Hamming bound is given by $K \leq q^{-n} \max_{x \in S} \frac{f(x)}{f_x}$ equals to*

$$K \leq \frac{q^n}{\sum_{i=0}^e \binom{n}{i} (q^2-1)^i}$$

iff $f(0)/f_0$ is the max. value for $d \geq 3$ and $n \geq n_0$.

Proof. In this proof, we propose f_x satisfying theorem 11. Let $f_x = (\sum_{i=0}^e K_i(x))^2$ and $f(x) = \sum_{j=0}^n f_j K_j(q, x)$.

$$\frac{f(x)}{f_x} = \frac{\sum_{j=0}^n f_j K_j(q, x)}{f_x} \quad (16)$$

And our goal is to find $\max\{f(0)/f_0, f(1)/f_1, \dots, f(d-1)/f_{d-1}\}$ that may equals to $f(0)/f_0$.

Now, for $x = 0$, we find that

$$\begin{aligned} \frac{f(0)}{f_0} &= \frac{\sum_{j=0}^n f_j K_j(0)}{f_0} \\ &= K_0(q, 0) + \frac{f_1 K_1(q, 0)}{f_0} + \dots + \frac{f_n K_n(q, 0)}{f_0} \end{aligned} \quad (17)$$

or

$$\frac{f(0)}{f_0} = \frac{\sum_{j=0}^n (\sum_{i=0}^e K_i(j))^2 K_j(0)}{(\sum_{i=0}^e K_i(0))^2} \quad (18)$$

and for any other value of $y \in \{1, 2, \dots, d-1\}$, we find that

$$\begin{aligned} \frac{f(y)}{f_y} &= \frac{\sum_{j=0}^n f_j K_j(y)}{f_y} \\ &= \frac{f_0 K_0(q, y)}{f_y} + \frac{f_1 K_1(q, y)}{f_y} + \dots + \frac{f_n K_n(q, y)}{f_y} \end{aligned} \quad (19)$$

or

$$\frac{f(y)}{f_y} = \frac{\sum_{j=0}^n (\sum_{i=0}^e K_i(j))^2 K_j(y)}{(\sum_{i=0}^e K_i(y))^2} \quad (20)$$

From 17 and 19, simply if we proof that

$$\frac{f(0)}{f_0} - \frac{f(y)}{f_y} \geq 0 \quad (21)$$

It means the lemma holds and Hamming bound is true in the general case for minimum distance d .

$$\begin{aligned} \frac{f(0)}{f_0} - \frac{f(y)}{f_y} &= \frac{\sum_{j=0}^n (\sum_{i=0}^e K_i(j))^2 K_j(0)}{(\sum_{i=0}^e K_i(0))^2} - \frac{\sum_{j=0}^n (\sum_{i=0}^e K_i(j))^2 K_j(y)}{(\sum_{i=0}^e K_i(y))^2} \\ &= \sum_{j=0}^n \left(\left(\sum_{i=0}^e K_i(j) \right)^2 \left(\frac{K_j(0)}{(\sum_{i=0}^e K_i(0))^2} - \frac{K_j(y)}{(\sum_{i=0}^e K_i(y))^2} \right) \right) \\ &= \sum_{j=0}^n \left(\frac{f_j K_j(q, 0)}{f_0} - \frac{f_j K_j(q, y)}{f_y} \right) \end{aligned} \quad (22)$$

in the previous equation, $f_j > 0$ and $f_y > 0$, so, if we prove that

$$\frac{f_j K_j(q, 0)}{f_0} - \frac{f_j K_j(q, y)}{f_y} \geq 0 \quad (23)$$

then the claim holds.

As shown in [3], [14], [10], we seek a constant value for the left side in 23, So, multiply both sides by $K_e(i)$, next lemma proves $K_e(i) \geq 0$.

$$\frac{K_e(i) K_i(q, 0)}{f_0} - \frac{K_e(i) K_i(q, y)}{f_y} \geq 0 \quad (24)$$

and take $\sum_{i=0}^n$

$$\begin{aligned} \sum_{i=0}^n \left(\frac{K_e(i) K_i(q, 0)}{f_0} - \frac{K_e(i) K_i(q, y)}{f_y} \right) &\geq 0 \\ \frac{\sum_{i=0}^n K_e(i) K_i(q, 0)}{f_0} - \frac{\sum_{i=0}^n K_e(i) K_i(q, y)}{f_y} &\geq 0 \end{aligned} \quad (25)$$

from [14], given that $\sum_{i=0}^n K_e(i) K_i(q, j) = q^n \delta_{ej}$, by substitution,

$$\begin{aligned} \frac{q^n \delta_{e0}}{f_0} - \frac{q^n \delta_{ey}}{f_y} &\geq 0 \\ \frac{\delta_{e0}}{f_0} - \frac{\delta_{ey}}{f_y} &\geq 0 \end{aligned} \quad (26)$$

Now, $\delta_{e0} = 1$, and $\delta_{ey} = 1$ or 0 ; and obviously $f_y \geq f_0$.

So, if $y = e \implies \delta_{e0}/f_0 \geq 0$, and similarly, $\delta_{ey} = 1 \implies f_y - f_0 \geq 0$.

□

Lemma 13. *The Krawtchouk Polynomial $K_e(x; q, n) \geq 0$, $\forall n \geq 4$ and arbitrary values of x, n , and q and single error correction $e = 1$, and double error correction $e = 2$.*

Proof. From definition of Krawtchouk polynomial [14],

$$K_e(x; q, n) = K_e(x) = \sum_{j=0}^e (-1)^j (q^2 - 1)^{e-j} \binom{x}{j} \binom{n-x}{e-j} \quad (27)$$

Let us simplify the proof into two cases for odd and even values of e :

Case 1: Now suppose e is odd it means we have equally number of odd (negative) and even (positive) for j . we proof that each consequence two terms are

≥ 0 .

let $e = 1$, first odd,

$$\begin{aligned} K_1(x; q, n) &= \sum_{j=0}^1 (-1)^j (q^2 - 1)^{e-j} \binom{x}{j} \binom{n-x}{e-j} \\ &= (n-x)(q^2 - 1) - x \end{aligned}$$

since $e = 1 \implies x = 3$ and $K_1(x) = n(q^2 - 1) - 3q^2$, if $K_1(3) \geq 0 \implies n \geq 4$, which is a valid value.

Case 2: $e = 2$ even, So, we have two positives and one negative terms. Obviously, the final result is positive. Someone can try all other cases for e as large as possible and get the correct results.

This lemma needs to be reviewed since $n \geq 4$ valid only for $e = 1$ and we have to get new value for n and $e = 2$. \square