Degenerate Quantum Codes and the Quantum Hamming Bound

Pradeep Sarvepalli[1,*] and Andreas Klappenecker[2,†]

[1]*Department of Physics and Astronomy, University of British Columbia, Vancouver V6T 1Z1, Canada*

[2]*Department of Computer Science, Texas A&M University, College Station, TX 77843*

(Dated: November 21, 2009)

The parameters of a nondegenerate quantum code must obey the Hamming bound. An important open problem in quantum coding theory is whether or not the parameters of a degenerate quantum code can violate this bound for nondegenerate quantum codes. In this paper we show that Calderbank-Shor-Steane (CSS) codes with alphabet $q \geq 5$ cannot beat the quantum Hamming bound. We prove a quantum version of the Griesmer bound for the CSS codes which allows us to strengthen the Rains' bound that an $[[n, k, d]]_2$ code cannot correct more than $\lfloor (n + 1)/6 \rfloor$ errors to $\lfloor (n - k + 1)/6 \rfloor$. Additionally, we also show that the general quantum codes $[[n, k, d]]_q$ with $k + d \leq (1 - 2eq^{-2})n$ cannot beat the quantum Hamming bound.

Keywords: quantum Hamming bound, quantum codes, degenerate codes, CSS codes

I. INTRODUCTION

Quantum information can be protected by encoding it into a quantum error-correcting code. An $((n, K, d))_q$ quantum code is a K-dimensional subspace of the state space $\mathcal{H} = (\mathbb{C}^q)^{\otimes n}$ of n quantum systems with q levels that can detect all errors affecting less than d quantum systems, but cannot detect some errors affecting d quantum systems. An $((n, K, d))_q$ quantum code with $k = \log_q K$ is also said to be an $[[n, k, d]]_q$ quantum code. The parameter k is not necessarily integral.

A measure of the performance of the quantum code is its ability to correct errors on the encoded information. Let $\mathcal{B}(\mathcal{H})$ denote the algebra of bounded operators on $\mathcal{H}$. We denote by $P_\mathcal{Q}$ the orthogonal projector in $\mathcal{B}(\mathcal{H})$ that projects onto the quantum code $\mathcal{Q}$. Let $\mathcal{E}$ denote a subspace of $\mathcal{B}(\mathcal{H})$ with basis B. The quantum code $\mathcal{Q}$ is able to correct all errors in $\mathcal{E}$ if and only if there exists a hermitian matrix C such that

$$(P_\mathcal{Q} E^\dagger F P_\mathcal{Q})_{E,F \in B} = C \otimes P_\mathcal{Q}. \tag{1}$$

In other words, $\mathcal{Q}$ can correct all errors in $\mathcal{E}$ if and only if it can detect all errors in the set $\{E^\dagger F \mid E, F \in B\}$.

Of particular interest are localized errors that affect few quantum systems. Let $\mathcal{E}_t$ denote the vector space spanned by all elements in $\mathcal{B}(\mathcal{H})$ affecting at most t quantum systems. A quantum code $\mathcal{Q}$ is called t-error correcting if and only if it can correct all errors in $\mathcal{E}_t$. An $((n, K, d))_q$ quantum code is t-error correcting for $t = \lfloor (d-1)/2 \rfloor$.

The pair $(\mathcal{Q}, \mathcal{E})$ consisting of a quantum code $\mathcal{Q}$ and a vector space of errors $\mathcal{E}$ is called degenerate if and only if the hermitian matrix C in equation (1) is singular; otherwise, $(\mathcal{Q}, \mathcal{E})$ is called nondegenerate. An $((n, K, d))_q$ quantum code $\mathcal{Q}$ is said to be nondegenerate if and only if $(\mathcal{Q}, \mathcal{E}_t)$ is nondegenerate for $t = \lfloor (d-1)/2 \rfloor$.

In the construction of quantum codes, one would like to have both large dimension K and large minimum distance d, but these are two conflicting requirements on the quantum code. The trade off between the number of correctable errors and the size of the quantum code is usually quantified by various bounds. For example, a nondegenerate $((n, K, d))_q$ quantum code satisfies the Hamming bound

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

The term 'degenerate quantum code' was introduced a decade ago. Since the term was coined, researchers raised the question whether a degenerate $[[n, k, d]]_q$ quantum code violating the Hamming bound (2) might exist, [3]. The standard proof of (2) by a simple counting argument can fail for degenerate quantum codes in a spectacular fashion, fueling the interest in this problem. To date this problem remains to be fully settled.

We review briefly some previous work to put our result in context. Gottesman reported the first analytical result as to the generality of the quantum Hamming bound in [4] by proving that single and double error-correcting binary stabilizer codes cannot beat the quantum Hamming bound. Subsequently, Ashikhmin and Litsyn [1] showed a stronger result that asymptotically binary quantum codes obey the quantum Hamming bound; their result is applicable to general codes not just binary stabilizer codes. In [8] Gottesman's result was generalized for nonbinary codes with distance three [8], suggesting that even with the freedom of increased alphabet it may not be possible to beat the quantum Hamming bound.

In this paper we prove some new results on the applicability of quantum Hamming bound to quantum codes. We show that all CSS codes with alphabet size $q \geq 5$ must obey the Hamming bound. In the process, we also show a weaker result that holds for general quantum codes, namely we prove that if one bounds $k + d$ by a fraction of the length n, then an arbitrary $[[n, k, d]]_q$ quantum code must also obey the quantum Hamming bound. Furthermore, we prove a quantum version of the

*pradeep@phas.ubc.ca

†klappi@cse.tamu.edu

Griesmer bound for the CSS codes. As a consequence of this bound we can tighten Rains' bound when applied to CSS codes.

Since one-dimensional quantum codes are by definition nondegenerate, hence obey the Hamming bound, we may assume throughout that the quantum code is of dimension $K > 1$.

II. QUANTUM HAMMING BOUND AND ARBITRARY QUANTUM CODES

One of the long standing open questions in quantum coding theory is whether the Hamming bound (2) holds for degenerate quantum codes. In this section, we show that this question has an affirmative answer for a large class of general quantum codes.

We denote by $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ the binary entropy function.

Theorem 1. *If $2eq^{-2} \leq \delta \leq 1$ and $q \geq 3$, then an $((n,K,d))_q$ code with $\log_q K + d \leq (1-\delta)n$ satisfies the quantum Hamming bound (2).*

Proof. We have $K \leq q^{(1-\delta)n-d} = q^n/q^{\delta n+d}$. Let

$$T = q^{\delta n+d}\Big/\sum_{j=0}^{t}\binom{n}{j}(q^2-1)^j. \quad (3)$$

It suffices to show that $T \geq 1$, since this implies that

$$K \leq \frac{q^n}{q^{\delta n+d}} \leq \frac{q^n}{\sum_{j=0}^{t}\binom{n}{j}(q^2-1)^j}.$$

As $2t+1 \leq d \leq 2t+2$ we can bound T from below by

$$T \;\geq\; \frac{q^{\delta n+2t+1}}{(q^2-1)^t\sum_{j=0}^{t}\binom{n}{j}} = \frac{q^{\delta n+1}}{(1-q^{-2})^t\sum_{j=0}^{t}\binom{n}{j}}.$$

By [7, Corollary 23.6] we have $\sum_{j=0}^{t}\binom{n}{j} \leq 2^{nh(t/n)}$. Hence, we obtain

$$T \geq \frac{q^{\delta n+1}2^{-nh(t/n)}}{(1-q^{-2})^t} = \frac{q^{\delta n+1-nh(t/n)\log_q 2}}{q^{t\log_q(1-q^{-2})}} \geq 1.$$

In other words, we need to show that

$$\delta n + 1 - nh(t/n)\log_q 2 - t\log_q(1-q^{-2}) \geq 0,$$

that is

$$h(t/n)\log_q 2 + (t/n)\log_q(1-q^{-2}) - 1/n \leq \delta \leq 1. \quad (4)$$

Next, we will show the above inequality holds for $\delta \geq 2eq^{-2}$.

Without loss of generality let us assume that $k+d = (1-\delta)n$ where $2eq^{-2} \leq \delta \leq 1$ and $k = \log_q K$. By the quantum Singleton bound, $k+d \leq n-d+2$; so $d \leq \delta n + 2$ and $t = \lfloor (d-1)/2 \rfloor \leq \lfloor (\delta n+1)/2 \rfloor$, hence, $t/n \leq \delta/2 + 1/2n$.

Let $f(x) = x - h(x/2)\log_q 2 = x + (x/2)\log_q(x/2) + (1-x/2)\log_q(1-x/2)$, for $x \in (0,2)$. The derivative of $f(x)$ is given by

$$f'(x) = 1 + \frac{1}{2}\log_q\frac{x}{2-x} = \frac{1}{2}\log_q\frac{q^2x}{2-x},$$

which can be seen to satisfy $f'(x) > 0$ for $x > 2/(q^2+1)$. Since $\delta \geq 2eq^{-2} = 2e(1+q^{-2})/(q^2+1) > 2/(q^2+1)$, the function $f(x)$ is increasing for $x \geq 2eq^{-2}$. We claim that $f(x) \geq 0$ for $x \geq 2eq^{-2}$ and $q \geq 3$. Indeed, we have

$$\begin{aligned} f(x) &= x - h(x/2)\log_q 2 \\ &= x + (x/2)\log_q(x/2) + (1-x/2)\log_q(1-x/2) \\ &= \log_q(q^2x/2)^{x/2}(1-x/2)^{1-x/2} \geq f(2eq^{-2}) \\ &= \log_q e^{eq^{-2}}(1-eq^{-2})^{1-eq^{-2}}. \end{aligned}$$

Since $(1+z) \leq e^z$ holds for all z, we have $(1-z) = 1/(1+z/(1-z)) \geq e^{-z/(1-z)}$; and as $eq^{-2} < 1$ for $q \geq 3$ we obtain

$$f(x) \;\geq\; \log_q e^{eq^{-2}}e^{-eq^{-2}} = 0,$$

as claimed. In particular, we have $\delta + 1/n \geq h(\delta/2 + 1/2n)\log_q 2$ for $2eq^{-2} \leq \delta \leq 1$. The entropy function $h(x)$ is monotonically increasing in x for $x \in [0,1/2]$. Since $t/n \leq \delta/2 + 1/2n$, for $2eq^{-2} \leq \delta \leq 1-1/n$, the monotonicity of $h(x)$ implies that $h(t/n) \leq h(\delta/2+1/2n)$. If $1-1/n < \delta \leq 1$, then we observe that $1/2 < \delta/2 + 1/2n \leq 3/4$, for $n \geq 2$. As $h(x) = h(1-x)$, we have $h(1/4) \leq h(\delta/2+1/2n) < h(1/2)$. But $t/n \leq 1/4$, by the Singleton bound, therefore again we have $h(t/n) \leq h(\delta/2+1/2n)$. In either case we have $h(t/n)\log_q 2 \leq h(\delta/2+1/2n)\log_q 2 \leq \delta + 1/n$. Thus, δ satisfies the inequality (4); note that $(t/n)\log_q(1-q^{-2}) < 0$. If $n = 1$, then $t = 0$ and equation (4) holds trivially for all $0 \leq \delta \leq 1$. Hence, the quantum code obeys quantum Hamming bound (2). □

It follows from Theorem 1 that for any $\delta > 0$, an $[[n,k,d]]_q$ code with $k+d \leq (1-\delta)n$ obeys the quantum Hamming bound for any alphabet size $q \geq \sqrt{2e/\delta}$. This suggests that it is less likely that one can find a degenerate quantum code beating the quantum Hamming bound for larger alphabet sizes. Indeed, if we choose a larger alphabet size q, then we can choose a smaller parameter δ, so the previous theorem rules out an even larger fraction of quantum codes.

The following table list for a given alphabet size q the fraction $1-\delta$ of the length that bounds the sum of minimum distance d and dimension parameter k.

The thresholds on δ given in Theorem 1 are monotonically decreasing in q. Therefore, if we conclude from Theorem 1 that all $[[n,k,d]]_\alpha$ codes with $k+d \leq (1-\delta)n$ obey the Hamming bound, then this implies that the same claim holds for all alphabet sizes $q \geq \alpha$. In particular, we can conclude from Table I that if $q \geq 4$ and $k+d \leq n/2$, then an $[[n,k,d]]_q$ quantum code cannot

q	3	4	5	6	7	8	9	10	11
δ	0.605	0.340	0.218	0.152	0.111	0.085	0.068	0.055	0.045
$1-\delta$	0.395	0.660	0.782	0.848	0.889	0.915	0.932	0.945	0.955

TABLE I: Threshold values of δ for $[[n,k,d]]_q$ codes as computed by Theorem 1

beat the quantum Hamming bound. Similarly, we can conclude from Table I that if $q \geq 5$ and $k+d \leq 3n/4$, then an $[[n,k,d]]_q$ cannot beat the quantum Hamming bound.

Notice that these results are not a restatement of the asymptotic versions of the quantum Hamming bound. The asymptotic forms usually claim that for large n, the quantum Hamming bound holds. In contrast, the present result specifies the restriction of K and d when the quantum Hamming bound holds exactly, irrespective of the size of n.

III. QUANTUM HAMMING BOUND AND CSS CODES

In this section, we focus on a subset of the stabilizer codes known as CSS codes. These quantum codes have desirable properties especially in the context of fault tolerant quantum computation. Even though some better bounds are known for CSS codes, such as tighter linear programming bounds, it remained unclear whether they obey the quantum Hamming bound.

In this section, we will additionally assume that the alphabet size q is power of a prime. We show that all CSS codes obey the quantum Hamming bound when the alphabet size $q \geq 5$. In particular, we can partially complement the results of Theorem 1 by including the range $k+d > (1-\delta)n$, where $\delta = 2eq^{-2}$.

For the background, we mention that the CSS construction used here can be found in [2, Theorem 9] and q-ary versions in [5] or [8]. Our proof takes advantage of an idea that has been introduced in [1, Theorem 8].

Lemma 2. *Let Q be an $[[n,k,d]]_q$ CSS code derived from a pair of classical codes $C_1 \subset C_2 \subset \mathbb{F}_q^n$, where C_i is an $[n,k_1]_q$ code. Then Q implies the existence of $[n-k_1,k,\geq d]_q$ and $[k+k_1,k,\geq d]_q$ codes.*

Proof. Since $C_1 \subset C_2$, the generator matrices of C_1 and C_2 can be put in the form

$$G_{C_1} = \left[\begin{array}{cc} I_{k_1} & P \end{array}\right] \quad G_{C_2} = \left[\begin{array}{cc} I_{k_1} & P \\ 0_{k\times k_1} & A \end{array}\right].$$

Since C_2 is an $[n,k_1+k]_q$ code we can further transform G_{C_2} to

$$G_{C_2} = \left[\begin{array}{ccc} I_{k_1} & P' & P'' \\ 0_{k\times k_1} & I_k & A' \end{array}\right] = \left[\begin{array}{ccc} I_{k_1} & & P \\ 0_{k\times k_1} & I_k & A' \end{array}\right].$$

The code generated by $\left[\begin{array}{ccc} 0_{k\times(n-k)/2} & I_k & A' \end{array}\right]$ is in $C_2 \setminus C_1$ and has a distance d. Because the first k_1 coordinates are zero we can also view it as an $[n-k_1,k,d]_q$ code. The codes $C_2^\perp \subset C_1^\perp$ have the parameters $[n,n-k_1-k]_q$ and $[n,n-k_1]_q$ respectively. Reasoning similarly with $C_2^\perp$ and $C_1^\perp$ we can show that there exists a $[k_1+k,k,d]_q$ code. ☐

Proposition 3. *Let $\mathcal{Q}$ be an $[[n,k,d]]_q$ CSS code with $k+d > (1-\delta)n$ such that $\delta = 2eq^{-2}$ and q a prime power ≥ 5. Then $\mathcal{Q}$ obeys the quantum Hamming bound.*

Proof. Suppose that $\mathcal{Q}$ is derived from a pair of nested codes $C_1 \subset C_2 \subset \mathbb{F}_q^n$ with the parameters $[n,k_1]_q$ and $[n,k+k_1]_q$, respectively. These codes must satisfy $\min\{\mathrm{wt}(C_2 \setminus C_1), \mathrm{wt}(C_1^\perp \setminus C_2^\perp)\} = d$.

If $k+d = n-d+2$, then $\mathcal{Q}$ is an MDS code. Rains has shown that every quantum MDS code is nondegenerate, see [9, Theorem 2]; hence, the Hamming bound holds. Thus, we can assume that $k+d \leq n-d+1$. The integrality of $k+d$ implies that $k+d \geq \lfloor (1-\delta)n \rfloor + 1$. By assumption, we also have $\lfloor (1-\delta)n \rfloor + 1 \leq k+d \leq n-d+1$, which implies $d \leq n - \lfloor (1-\delta)n \rfloor = \lceil \delta n \rceil$ and

$$t = \lfloor (d-1)/2 \rfloor \leq \delta n/2. \tag{5}$$

By Lemma 2, there exist classical codes D and D' with the parameters $[n-k_1,k,d]_q$ and $[k+k_1,k,d]_q$ respectively. Since D obeys the classical Singleton bound, cf. [6, pg. 71], we have

$$n-k_1 \ \geq \ k+d-1. \tag{6}$$

In particular, if $k_1 > n-k-d+1$, then $\mathcal{Q}$ cannot have a distance d and no $[[n,k,d]]_q$ code can be derived from such a C_1 and C_2. Further, D obeys the classical Hamming bound, see [6, pg. 48]; hence,

$$q^k \ \leq \ \frac{q^{n-k_1}}{\sum_{j=0}^{t}\binom{n-k_1}{j}(q-1)^j}. \tag{7}$$

Similarly, applying the classical Singleton and Hamming bounds to D', we respectively obtain

$$k_1+k \ \geq \ k+d-1, \tag{8}$$

$$q^k \ \leq \ \frac{q^{k_1+k}}{\sum_{j=0}^{t}\binom{k_1+k}{j}(q-1)^j}. \tag{9}$$

In particular, if $k_1 < d-1$, there cannot exist an $[[n,k,d]]_q$ code. From equations (7) and (9) we obtain

$$q^{2k} \ \leq \ \frac{q^{n-k_1+k_1+k}}{\sum_{j=0}^{t}\binom{n-k_1}{j}(q-1)^j \sum_{j=0}^{t}\binom{k_1+k}{j}(q-1)^j}.$$

which yields

$$q^k \ \leq \ \frac{q^n}{\sum_{i,j=0}^{t}\binom{n-k_1}{i}\binom{k_1+k}{j}(q-1)^{i+j}}. \tag{10}$$

To prove that $\mathcal{Q}$ obeys the Hamming bound, it suffices to show that the right hand side of (10) is less than the right hand side of (2); put differently, it suffices to show that

$$\sum_{j=0}^{t}\binom{n}{j}(q^2-1)^j \le \sum_{i,j=0}^{t}\binom{n-k_1}{i}\binom{k_1+k}{j}(q-1)^{i+j}.$$

If $n\le 4$ and $k>0$, the quantum Singleton bound implies that $d\le 2$, i.e., $t=0$ and the inequality holds. For $n\ge 5$ we shall prove an even stronger inequality, namely that

$$\sum_{j=0}^{t}\binom{n}{j}(q^2-1)^j \le \sum_{j=0}^{t}\binom{n-k_1}{j}\binom{k+k_1}{j}(q-1)^{2j} \quad (11)$$

holds term by term, $\binom{n}{j}(q^2-1)^j \le \binom{n-k_1}{j}\binom{k+k_1}{j}(q-1)^{2j}$. It clearly holds for $j=0$. For $j>0$ we use the fact that $(n/j)^j \le \binom{n}{j} \le (ne/j)^j$; hence, it suffices to show that

$$\left(\frac{ne}{j}\right)^j (q^2-1)^j \;\le\; \left(\frac{n-k_1}{j}\frac{k+k_1}{j}\right)^j (q-1)^{2j}.$$

This is equivalent to showing that

$$\frac{ne}{j}(q+1) \le \frac{n-k_1}{j}\frac{k+k_1}{j}(q-1). \quad (12)$$

Notice that equality cannot hold in both (6) and (8). Indeed, if we have $k_1=n-k-d+1$ in (6), then it follows that $k_1+k=n-d+1\ge k+d$ as $\mathcal{Q}$ is not MDS, tightening the inequality (8). If $k_1+k=k+d-1$ in (8), then this implies $n-k_1=n-d+1\ge k+d$, tightening the inequality (6). It follows that $(n-k_1)(k+k_1)\ge (k+d)(k+d-1)\ge(1-\delta)n\left((1-\delta)n-1\right)$. Hence, to prove that (12) holds it is enough to show

$$ej(q+1)\le n(1-\delta)(1-\delta-1/n)(q-1).$$

By assumption $\delta=2eq^{-2}$. By equation (5), we have $j\le t\le \delta n/2$; thus, it remains to show that

$$e^2q^{-2}(q+1)\le(1-2eq^{-2})(1-2eq^{-2}-1/n)(q-1).$$

This inequality holds for $q=5$ and $n=5$. The left side of this inequality is monotonically decreasing in q while the right hand side is monotonically increasing in q and n; hence, the inequality holds for all $q\ge 5$ and $n\ge 5$. Consequently, we have shown that inequality (11) holds for all n, and it follows that $\mathcal{Q}$ obeys the quantum Hamming bound. □

Theorem 4. *For $q\ge 5$ all $[[n,k,d]]_q$ CSS codes obey the quantum Hamming bound.*

Proof. Set $\delta=2eq^{-2}$. A CSS code obeys the quantum Hamming bound by Theorem 1 if $k+d\le(1-\delta)n$, and by Proposition 3 if $k+d>(1-\delta)n$. □

Other interesting bounds can be derived as a consequence of Lemma 2. For instance, an analogue of the Griesmer bound is possible.

Theorem 5 (Quantum Griesmer Bound for CSS Codes)**.** *An $[[n,k,d]]_q$ CSS code satisfies the following bound:*

$$\frac{n+k}{2} \;\ge\; \sum_{i=0}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil. \quad (13)$$

Proof. By Lemma 2 there exist $[n-k_1,k,d]_q$ and $[k+k_1,k,d]_q$ codes. These codes obey the classical Griesmer bound, see [6, Theorem 2.7.4], hence we obtain

$$n-k_1\ge\sum_{i=0}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil \text{ and } k+k_1\ge\sum_{i=0}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil.$$

Combining the two inequalities proves the statement of the theorem. □

We can also show that a similar bound (though not exactly the same) is applicable for linear quantum codes. Since $\lceil d/q^i\rceil\ge 1$ for $i>0$, we have $(n+k)/2\ge d+k-1$ and we recover the quantum Singleton bound as $n-k\ge 2d-2$. A very natural question would be if there are quantum codes that meet the quantum Griesmer bound. If $k=1$ (and $n-k$ even), then this essentially reduces to the quantum Singleton bound and all $[[n,1,(n+1)/2]]_q$ quantum MDS codes meet this bound. The interesting case is when $k\ge 2$. The $[[4,2,2]]_2$ code for instance meets this bound, it also meets the quantum Singleton bound. At this time we are not aware of other codes that meet the quantum Griesmer bound.

Corollary 6. *An $[[n,k,d]]_q$ CSS code with $d\ge q$ satisfies*

$$\frac{n-k}{2} \;\ge\; d(1+1/q)-2. \quad (14)$$

Proof. This is an easy consequence of Theorem 5. Since $d\ge q$ we have

$$\frac{n+k}{2} \;\ge\; d+d/q+\sum_{i=2}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil \ge d+d/q+k-2.$$

Simplifying the above inequality yields the claim. □

Note that Corollary 6 is tighter than the quantum Singleton bound. Rains had shown that the binary quantum codes cannot correct more than $\lfloor (n+1)/6\rfloor$ errors [10]. A slightly stronger result can be easily derived for CSS codes.

Corollary 7. *An $[[n,k,d]]_2$ CSS code cannot correct more than $\lfloor(n-k+1)/6\rfloor$ errors.*

Proof. By Corollary 6, we have $(n-k)/2\ge 3d/2-2$, which implies the claim. □

IV. CONCLUSIONS

In this paper we have shown that the quantum Hamming bound holds for all CSS codes with alphabet greater than 5. We also have shown a slightly weaker result for general quantum codes. Our results give ample evidence for the conjecture that the quantum Hamming bound holds for all quantum codes. However, there still remain some gaps. The major remaining open question is the status of $((n, K, d))_q$ quantum codes which do not satisfy the conditions in Theorem 1. Some special cases of interest are linear stabilizer codes and CSS codes of small alphabet $q \leq 4$.

Acknowledgment

We thank Alexei Ashikhmin for correcting an erroneous remark in a previous version of this manuscript and an anonymous reader for pointing out a subtle issue with the original formulation of Theorem 1 for arbitrary quantum codes. This research is supported by NSF Career Award CCF 0347310 and NSF grant CCF 0622201. P.S. is also supported by grants from NSERC, MITACS and CIFAR.

[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.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*, 44:1369–1387, 1998.

[3] D. Gottesman. A class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54:1862–1868, 1996.

[4] D. Gottesman. Stabilizer codes and quantum error correction. Caltech Ph. D. Thesis, eprint: quant-ph/9705052, 1997.

[5] M. Grassl, T. Beth, and M. Rötteler. On optimal quantum codes. *Internat. J. Quantum Information*, 2(1):757–775, 2004.

[6] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. University Press, Cambridge, 2003.

[7] S. Jukna. *Extremal Combinatorics*. Springer, 2001.

[8] 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.

[9] E.M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45:1827–1832, 1999.

[10] E.M. Rains. Quantum shadow enumerators. *IEEE Trans. Inform. Theory*, 45(7):2361–2366, 1999.