Quantum Inf Process (2017) 16:285
DOI 10.1007/s11128-017-1748-y

Two Gilbert–Varshamov-type existential bounds for asymmetric quantum error-correcting codes

Ryutaroh Matsumoto[1]

Received: 11 May 2017 / Accepted: 12 October 2017 / Published online: 23 October 2017

Abstract In this note, we report two versions of Gilbert–Varshamov-type existential bounds for asymmetric quantum error-correcting codes.

Keywords Asymmetric error · Quantum error correction · Gilbert-Varshamov bound

Mathematics Subject Classification 94B65

1 Introduction

Quantum error-correcting codes (QECCs) are important for construction of quantum computers, as the fault-tolerant quantum computation is based on QECC [13]. There are two kinds of errors in quantum information: One is called a bit error, and the other is called a phase error. Steane [16] first studied the asymmetry between probabilities of the bit and the phase errors, and he also considered QECC for asymmetric quantum errors, which are called asymmetric quantum error-correcting codes (AQECC). Research on AQECC has become very active recently; see [7,9,16] and the references therein.

On the other hand, in the study of error-correcting codes, it is important to know the optimal performance of codes. For classical error-correcting codes, the Gilbert–Varshamov (GV) bound [11] is a sufficient condition for existence of codes whose

✉ Ryutaroh Matsumoto
ryutaroh@rmatsumoto.org
http://www.rmatsumoto.org/research.html

1 Department of Communication and Computer Engineering, Nagoya University, Nagoya 464-8603, Japan

parameters satisfies the GV bound. By the GV bound, one can know that the optimal performance of classical codes is at least as good as the GV bound.

For QECC, Ekert and Macchiavello obtained a GV-type existential bound for general QECCs. An important subclass of general QECCs is the stabilizer codes [2,3,8], as they enable efficient encoding and decoding. Calderbank et al. [2] obtained a GV-type existential bound for the stabilizer QECCs. After that, Feng and Ma [6] and Jin and Xing [10] obtained improved versions of GV-type bounds for the stabilizer QECCs.

The Calderbank–Shor–Steane (CSS) QECCs [4,15] are an important subclass of the stabilizer QECCs, as the CSS codes enable more efficient implementation of the fault-tolerant quantum computation than the stabilizer codes.

Those existential bounds [2,4–6,10] did not consider the asymmetric quantum errors, while the asymmetry in quantum errors is important in practice [14]. As far as the author knows, nobody has reported existential bounds for the stabilizer or the CSS QECC for asymmetric quantum errors. In this note, we report such ones. Our proof arguments are similar to ones in [2,4].

2 A GV-type existential bound for the CSS codes

An $[[n, k, d_x, d_z]]_q$ QECC encodes k q-ary qudits into n q-ary qudits and detects up to d_x bit errors and up to d_z phase errors. It is known [1,3] that a nested classical code $C_2 \subset C_1 \subset \mathbf{F}_q^n$ with dimensions k_2 and k_1 can construct an $[[n, \dim C_1 - \dim C_2]]_q$ CSS code, where $\mathbf{F}_q$ is a finite field with q elements. A quantum error can be expressed as a pair $(\mathbf{e}_x, \mathbf{e}_z)$, where $\mathbf{e}_x \in \mathbf{F}_q^n$ corresponds to the bit error component of a quantum error and $\mathbf{e}_x \in \mathbf{F}_q^n$ does to the phase error component.

Let $\mathrm{GL}_n(\mathbf{F}_q)$ be the group of $n \times n$ invertible matrices over $\mathbf{F}_q$. Let $B_n = \{(C_1, C_2) \mid C_2 \subset C_1 \subset \mathbf{F}_q^n, \dim C_1 = k_1, \dim C_2 = k_2\}$. For a nonzero vector $\mathbf{e} \in \mathbf{F}_q^n$, let $B_{n,x}(\mathbf{e})$ (resp. $B_{n,z}(\mathbf{e})$) be the set of nested code pairs that cannot detect $\mathbf{e}$ as a bit error (resp. a phase error), that is, $B_{n,x}(\mathbf{e}) = \{(C_1, C_2) \in B_n \mid \mathbf{e} \in C_1 \setminus C_2\}$ (resp. $B_{n,z}(\mathbf{e}) = \{(C_1, C_2) \in B_n \mid \mathbf{e} \in C_2^\perp \setminus C_1^\perp\}$), where $C_1^\perp$ is the dual code of C_1 with respect to the standard inner product.

Lemma 1 *For nonzero* $\mathbf{e}$*, we have*

$$\sharp B_{n,x}(\mathbf{e}) = \frac{q^{k_1} - q^{k_2}}{q^n - 1} \sharp B_n,$$

$$\sharp B_{n,z}(\mathbf{e}) = \frac{q^{n-k_2} - q^{n-k_1}}{q^n - 1} \sharp B_n.$$

Proof As each pair $C_2 \subset C_1$ has $\sharp C_1 \setminus C_2 = q^{k_1} - q^{k_2}$ undetectable errors, we have

$$\frac{\sum_{\mathbf{0} \neq \mathbf{e} \in \mathbf{F}_q^n} \sharp B_{n,x}(\mathbf{e})}{\sharp B_n} = q^{k_1} - q^{k_2}.$$

For nonzero $\mathbf{e}_1, \mathbf{e}_2 \in \mathbf{F}_q^n$, we claim $\sharp B_{n,x}(\mathbf{e}_1) = \sharp B_{n,x}(\mathbf{e})_2$. Assuming the claim, we have

$$\sum_{\mathbf{0}\neq\mathbf{e}\in\mathbf{F}_q^n} \sharp B_{n,x}(\mathbf{e}) = (q^n - 1)\sharp B_{n,x}(\mathbf{e}).$$

Combining these two equalities, we have

$$\sharp B_{n,x}(\mathbf{e}) = \frac{q^{k_1} - q^{k_2}}{q^n - 1}\sharp B_n.$$

We finish the proof by proving the claim. Let $\mathbf{e}_1, \mathbf{e}_2$ be nonzero vectors. We have

$$\begin{aligned}
\sharp B_{n,x}(\mathbf{e}_1) &= \sharp\{(C_1, C_2) \in B_n \mid \mathbf{e}_1 \in C_1 \backslash C_2\} \\
&= \sharp\{(\tau C_1, \tau C_2) \mid \tau \in \mathrm{GL}_n(\mathbf{F}_q), \mathbf{e}_1 \in C_1 \backslash C_2\} \\
&= \sharp\{(\tau C_1, \tau C_2) \mid \tau \in \mathrm{GL}_n(\mathbf{F}_q), \tau'\mathbf{e}_1 \in C_1 \backslash C_2\} \\
&= \sharp\{(C_1, C_2) \in B_n \mid \tau'\mathbf{e}_1 \in C_1 \backslash C_2\} \\
&= \sharp B_{n,x}(\tau'\mathbf{e}_1),
\end{aligned}$$

where $\tau' \in \mathrm{GL}_n(\mathbf{F}_q)$ such that $\tau'\mathbf{e}_1 = \mathbf{e}_2$.

For phase errors, we can make a similar argument with $C_2^{\perp} \supset C_1^{\perp}$. □

Theorem 2 *Let n, k_1, k_2, d_x and d_z be positive integers such that*

$$\frac{q^{k_1} - q^{k_2}}{q^n - 1} \sum_{i=1}^{d_x-1} \binom{n}{i} (q-1)^i + \frac{q^{n-k_2} - q^{n-k_1}}{q^n - 1} \sum_{i=1}^{d_z-1} \binom{n}{i} (q-1)^i < 1, \quad (1)$$

then an $[[n, k_1 - k_2, d_x, d_z]]_q$ CSS QECC exists.

Proof Recall that each quantum error can be expressed by its bit error component $\mathbf{e}_x \in \mathbf{F}_q^n$ and its phase error component $\mathbf{e}_z \in \mathbf{F}_q^n$. The bit error component $\mathbf{e}_x$ cannot be detected by codes in $B_{n,x}(\mathbf{e}_x)$, and the phase error component $\mathbf{e}_z$ cannot be detected by codes in $B_{n,z}(\mathbf{e}_z)$. The detectabilities of the bit errors and the phase errors are independent of each other. Therefore, if Eq. (1) holds, then there exists at least one $(C_1, C_2) \in B_n$ that can detect all the bit errors with weight up to $d_x - 1$ and all the phase errors with weight up to $d_z - 1$, which implies it is an $[[n, k_1 - k_2, d_x, d_z]]_q$ quantum code. □

Classical coding theorists often have interest in asymptotic versions of GV-type existential bounds [11]. They are stated in terms of information rate and relative distance of classical error-correcting codes. In the classical error correction, information rate is the ratio of the number of information symbols to the code length, and relative distance is the ratio of the minimum distance to the code length.

We can also derive an asymptotic version of Theorem 2. For an $[[n, k, d_x, d_z]]_q$ AQECC, we may define the relative distance δ_x for bit errors as d_x/n and the relative distance δ_z for bit errors as d_z/n. The information rate of an $[[n, k]]_q$ QECC is defined as k/n [13].

Recall [11] that for $0 \le \delta \le 1 - 1/q$ we have

$$\sum_{i=1}^{\lfloor n\delta \rfloor} \binom{n}{i} (q-1)^i \le q^{nh_q(\delta)}, \tag{2}$$

where $h_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta)$.

Corollary 3 *Let δ_x and δ_z be real numbers such that $0 \le \delta_x \le 1-1/q$ and $0 \le \delta_z \le 1 - 1/q$. If*

$$h_q(\delta_x) < 1 - R_1, \tag{3}$$
$$h_q(\delta_z) < R_2, \text{ and}$$
$$0 \le R_1 - R_2, \tag{4}$$

then, for sufficiently large n, there exists an $[[n, \lfloor nR_1 \rfloor - \lceil nR_2 \rceil, \lfloor n\delta_x \rfloor, \lfloor n\delta_z \rfloor]]_q$ CSS QECC exists.

In Corollary 3, R_1 is the information rate of classical ECC C_1, and R_2 is the information rate of classical ECC C_2. The corresponding quantum CSS code has information rate $R_1 - R_2$, relative distance δ_x for bit errors, and relative distance δ_z for phase errors.

Proof Assume that Eq. (3) holds. Then for sufficiently large n, we have

$$\begin{aligned} & nh_q(\delta_x) < n - nR_1 \\ & \Rightarrow q^{nh_q(\delta_x)} < (1/2)\frac{q^n}{q^{nR_1}} \\ & \Rightarrow \frac{q^{nR_1}}{q^n} q^{nh_q(\delta_x)} < 1/2 \\ & \Rightarrow \frac{q^{\lfloor nR_1 \rfloor} - q^{\lceil nR_2 \rceil}}{q^n - 1} \sum_{i=1}^{\lfloor n\delta_x \rfloor - 1} \binom{n}{i} (q-1)^i < 1/2. \end{aligned} \tag{5}$$

Similarly, for sufficiently large n Eq. (4) implies

$$\begin{aligned} & nh_q(\delta_z) < nR_2 \\ & \Rightarrow q^{nh_q(\delta_z)} < (1/2)\frac{q^n}{q^{n(1-R_2)}} \\ & \Rightarrow \frac{q^{n(1-R_2)}}{q^n} q^{nh_q(\delta_z)} < 1/2 \\ & \Rightarrow \frac{q^{n-\lceil nR_2 \rceil} - q^{n-\lfloor nR_1 \rfloor}}{q^n - 1} \sum_{i=1}^{\lfloor n\delta_z \rfloor - 1} \binom{n}{i} (q-1)^i < 1/2. \end{aligned} \tag{6}$$

Equations (5) and (6) imply that the assumption of Theorem 2 becomes true for sufficiently large n, which shows Corollary 3. □

3 A GV-type existential bound for the stabilizer codes

Let $C \subset \mathbf{F}_q^{2n}$ be a $\mathbf{F}_q$-linear space of dimension $n-k$ self-orthogonal with respect to the standard symplectic inner product in $\mathbf{F}_q^{2n}$. C can be viewed as an $[[n,k]]_q$ stabilizer QECC. Let A_n be the set of all such C's. A nonzero $\mathbf{e} \in \mathbf{F}_q^{2n}$ can be viewed as a quantum error on n qudits. Let $A_n(\mathbf{e})$ be the set of stabilizer codes that cannot detect $\mathbf{e}$ as an error, that is, $A_n(\mathbf{e}) = \{C \in A_n \mid \mathbf{e} \in C^{\perp \mathrm{s}} \setminus C\}$, where $C^{\perp \mathrm{s}}$ is the dual of C with respect to the symplectic inner product. Then $\sharp A_n(\mathbf{e}) \le \frac{1-q^{-2k}}{1-q^{-2n}} \cdot \frac{1}{q^{n-k}} \sharp A_n$ [12, Lemma 9].

Recall that, for C to be $[[n,k,d_x,d_z]]_q$, C must be able to detect all d_x or less bit errors and all d_z or less phase errors. The number of such errors is

$$\sum_{i=1}^{d_x-1} \binom{n}{i}(q-1)^i \times \sum_{i=1}^{d_z-1} \binom{n}{i}(q-1)^i.$$

By the same argument as [12, Remark 10] (or as the last section), we have the following theorem:

Theorem 4 *Let n, k_1, k_2, d_x and d_z be positive integers such that*

$$\frac{1-q^{-2k}}{1-q^{-2n}} \cdot \frac{1}{q^{n-k}} \sum_{i=1}^{d_x-1} \binom{n}{i}(q-1)^i \times \sum_{i=1}^{d_z-1} \binom{n}{i}(q-1)^i < 1$$

then there exists an $[[n,k,d_x,d_z]]_q$ stabilizer QECC. □

By almost the same argument as Corollary 3, we can derive the following asymptotic version of Theorem 4.

Corollary 5 *Let δ_x and δ_z be real numbers such that $0 \le \delta_x \le 1-1/q$ and $0 \le \delta_z \le 1-1/q$. If*

$$h_q(\delta_x) + h_q(\delta_z) < 1 - R \le 1, \tag{7}$$

then, for sufficiently large n, there exists an $[[n, \lfloor nR \rfloor, \lfloor n\delta_x \rfloor, \lfloor n\delta_z \rfloor]]_q$ stabilizer QECC. □

The quantum stabilizer code in Corollary 5 has information rate R, relative distance δ_x for bit errors, and relative distance δ_z for phase errors.

By the relation between the CSS and the stabilizer QECCs [3], we see that the assumption in Corollary 3 is less demanding than that in Corollary 5 for the same n, $R = R_1 - R_2$, δ_x and δ_z, which means that Corollary 5 is a stronger existential bound than Corollary 3.

Remark 6 Theorems 2 and 4 and Corollaries 3 and 5 do not admit direct comparisons against previously known GV-type bounds even when $d_x = d_z$. The reason is as follows: For a binary QECC to be $[[n, k, 2, 2]]_2$, it must detect at least n^2 different errors. On the other hand, for a binary $[[n, k]]_2$ QECC to detect all single symmetric errors, it only has to detect $3n$ errors, which is generally much fewer than n^2. The above example shows that the number of asymmetric quantum errors is much different from that of corresponding symmetric quantum errors, even if we assume the same number of bit errors and phase errors in asymmetric quantum errors.

In addition, the famous $[[5, 1, 3]]_2$ binary stabilizer code in [3,8] can detect up to four bit errors if there is no phase error, and can detect up to four phase errors if there is no bit error. Thus, it is simultaneously both $[[5, 1, 1, 5]]_2$ AQECC and $[[5, 1, 5, 1]]_2$ AQECC. This phenomenon makes the direct comparison even more difficult.

Acknowledgements The author would like to thank an anonymous reviewer for careful reading and the helpful report that improved this note, and Prof. Fernando Hernando for drawing his attention to the asymmetric quantum error correction.

References

1. Ashikhmin, A., Knill, E.: Nonbinary quantum stabilizer codes. IEEE Trans. Inform. Theory **47**(7), 3065–3072 (2001)
2. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction and orthogonal geometry. Phys. Rev. Lett. **78**(3), 405–408 (1997)
3. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inform. Theory **44**(4), 1369–1387 (1998)
4. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. Phys. Rev. A **54**(2), 1098–1105 (1996)
5. Ekert, A., Macchiavello, C.: Quantum error correction for communication. Phys. Rev. Lett. **77**(12), 2585–2588 (1996)
6. Feng, K., Ma, Z.: A finite Gilbert–Varshamov bound for pure stabilizer quantum codes. IEEE Trans. Inform. Theory **50**(12), 3323–3325 (2004). doi:10.1109/TIT.2004.838088
7. Galindo, C., Geil, O., Hernando, F., Ruano, D.: Improved constructions of nested code pairs. IEEE Trans. Inform. Theory (2017). doi:10.1109/TIT.2017.2755682
8. Gottesman, D.: Class of quantum error-correcting codes saturating the quantum Hamming bound. Phys. Rev. A **54**(3), 1862–1868 (1996)
9. Ioffe, L., Mézard, M.: Asymmetric quantum error-correcting codes. Phys. Rev. A **75**, 032345 (2007). doi:10.1103/PhysRevA.75.032345
10. Jin, L., Xing, C.: Quantum Gilbert–Varshamov bound through symplectic self-orthogonal codes. In: Proceedings 2011 IEEE International Symposium on Information Theory, pp. 455–458. Sait Petersburg, Russia (2011). doi:10.1109/ISIT.2011.6034167
11. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. Elsevier, Amsterdam (1977)
12. Matsumoto, R., Uyematsu, T.: Lower bound for the quantum capacity of a discrete memoryless quantum channel. Jo. Math. Phys. **43**(9), 4391–4403 (2002). doi:10.1063/1.1497999
13. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
14. Sarvepalli, P.K., Klappenecker, A., Rötteler, M.: Asymmetric quantum codes: constructions, bounds and performance. Proc. R. Soc. A Math. Phys. Eng. Sci. **465**(2105), 1645–1672 (2009). doi:10.1098/rspa.2008.0439

15. Steane, A.M.: Multiple particle interference and quantum error correction. Proc. R. Soc. Lond. Ser. A **452**(1954), 2551–2577 (1996)
16. Steane, A.M.: Simple quantum error-correcting codes. Phys. Rev. A **54**(6), 4741–4751 (1996). doi:10.1103/PhysRevA.54.4741