B. Proof of Lemma 5.3

It is clear that for any given S, M_I is positive definite, and hence M_I^{-1} is also positive definite. It then follows that for every S

$$0 < \frac{\sqrt{P_1}}{1 + P_1 s_1^H M_I^{-1} s_1} < \sqrt{P_1}. \tag{21}$$

Combining (11) and (12) with (21), we have that

$$W_1^{(N)}(\boldsymbol{X}, \boldsymbol{Z}) \xrightarrow{P} \frac{1}{2} a_g^2 \int_0^\infty \frac{\lambda}{(\lambda+\eta)^2} \, dG^*(\lambda) \tag{22}$$

$$W_2^{(N)}(\boldsymbol{X}, \boldsymbol{Z}) \xrightarrow{P} \frac{1}{2} a_g^2 \int_0^\infty \frac{\lambda}{(\lambda+\eta)^2} \, dG^*(\lambda). \tag{23}$$

Then, for every subsequence $\{N'\}$ of $\{N\}$, combining (21) with (10) yields that

$$\left| U^{(N')}(\boldsymbol{X}, \boldsymbol{Z}) \right| \xrightarrow{P} 0.$$

Appealing to Lemma 5.2, we conclude that there exists a subsequence $\{J'\}$ of $\{N'\}$ such that

$$P\left\{\omega\colon \left| U^{(J')}(\boldsymbol{X}(\omega), \boldsymbol{Z}) \right| \xrightarrow{P} 0 \right\} = 1.$$

Based on (22) and (23), for the subsequence $\{J'\}$, we resort to Lemma 5.2 again and conclude that there exists a further subsequence $\{N''\}$ of $\{J'\}$ such that

$$P\left\{\omega\colon W_1^{(N'')}(\boldsymbol{X}(\omega), \boldsymbol{Z}) \xrightarrow{P} \frac{1}{2} a_g^2 \int_0^\infty \frac{\lambda}{(\lambda+\eta)^2} \, dG^*(\lambda) \right\} = 1$$

$$P\left\{\omega\colon W_2^{(N'')}(\boldsymbol{X}(\omega), \boldsymbol{Z}) \xrightarrow{P} \frac{1}{2} a_g^2 \int_0^\infty \frac{\lambda}{(\lambda+\eta)^2} \, dG^*(\lambda) \right\} = 1.$$

Furthermore, it is clear that

$$P\left\{\omega\colon \left| U^{(N'')}(\boldsymbol{X}(\omega), \boldsymbol{Z}) \right| \xrightarrow{P} 0 \right\} = 1$$

thereby concluding the proof.

ACKNOWLEDGMENT

The authors would like to thank David N. C. Tse for helpful discussions. The authors would also like to thank the anonymous reviewers for their helpful comments that improved the presentation of the correspondence.

REFERENCES

[1] P. Billingsley, *Probability and Measure*, 3rd ed. New York: Wiley, 1995.
[2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.
[3] M. L. Honig, U. Madhow, and S. Verdú, "Blind adaptive multiuser detection," *IEEE Trans. Inform. Theory*, vol. 41, pp. 944–960, July 1995.
[4] E. A. Lee and D. G. Messerschmitt, *Digital Communication*, 2nd ed. Boston, MA: Kluwer Academic, 1994.
[5] U. Madhow and M. L. Honig, "MMSE interference suppression for directed-sequence spread-spectrum CDMA," *IEEE Trans. Commun.*, vol. 42, pp. 3178–3188, Dec. 1994.
[6] ——, "On the average near–far resistance for MMSE detection of directed-sequence CDMA signals with random spreading," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2039–2045, Sept. 1999.
[7] T. L. Marzetta and B. M. Hochwald, "Capacity of a mobile multiple-antenna communication link in Rayleigh flat fading," *IEEE Trans. Inform. Theory*, vol. 45, pp. 139–157, Jan. 1999.
[8] D. L. McLeish, "Dependent central limit theorems and invariance principles," *Ann. Probab.*, vol. 2, no. 4, pp. 620–628, 1974.
[9] K. S. Miller, *Complex Stochastic Processes: An Introduction to Theory and Application*, 1st ed. Reading, MA: Addison-Wesley, 1974.
[10] D. Mitra and J. A. Morrison, "A distributed power control algorithm for bursty transmissions on cellular, spread spectrum wireless networks," in *Proc. 5th WINLAB Workshop on Third Generation Wireless Information Networks*, J. M. Holtzman, Ed. Boston, MA: Kluwer Academic, 1996, pp. 201–212.
[11] F. D. Nesser and J. L. Massey, "Proper complex random processes with applications to information theory," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1293–1302, July 1993.
[12] H. V. Poor and S. Verdú, "Probability of error in MMSE multiuser detection," *IEEE Trans. Inform. Theory*, vol. 43, pp. 858–871, May 1997.
[13] J. W. Silverstein and Z. D. Bai, "On the empirical distribution of eigenvalues of a class of large dimensional random matrices," *J. Multivariate Anal.*, vol. 54, no. 2, pp. 175–192, 1995.
[14] T. J. Sweeting, "On conditional weak convergence," *J. Theor. Probab.*, vol. 2, no. 4, pp. 461–474, 1989.
[15] D. N. C. Tse and S. V. Hanly, "Linear multiuser receivers: Effective interference, effective bandwidth and user capacity," *IEEE Trans. Inform. Theory*, vol. 45, pp. 641–657, Mar. 1999.
[16] S. Verdú, *Multiuser Detection*. Cambridge, U.K.: Cambridge Univ. Press, 1998.
[17] S. Verdú and S. Shamai (Shitz), "Spectral efficiency of CDMA with random spreading," *IEEE Trans. Inform. Theory*, vol. 45, pp. 622–640, Mar. 1999.
[18] J. Zhang, "Design and performance analysis of power-controlled CDMA wireless networks with linear receivers and antenna arrays," Ph.D. dissertation, Purdue Univ., West Lafayette, IN, May 2000.
[19] J. Zhang and E. K. P. Chong, "CDMA systems in fading channels: Admissibility, network capacity, and power control," *IEEE Trans. Inform. Theory*, vol. 46, pp. 962–981, May 2000.
[20] J. Zhang, E. K. P. Chong, and D. N. C. Tse, "Output MAI distributions of linear MMSE multiuser receivers in DS-CDMA systems," *IEEE Trans. Inform. Theory*, pp. 1128–1144, Mar. 2001.

Improvement of Ashikhmin–Litsyn–Tsfasman Bound for Quantum Codes

Ryutaroh Matsumoto, *Member, IEEE*

***Abstract*—We improve performance of the asymptotically good quantum codes constructed by Ashikhmin, Litsyn, and Tsfasman, by using more rational points on algebraic curves.**

***Index Terms*—Algebraic-geometry code, Ashikhmin–Litsyn–Tsfasman bound, quantum code.**

I. Introduction

Recently, quantum computation and quantum communication have attracted much attention, because the use of quantum-mechanical phenomena can offer unusual efficiency in computation and com-

Manuscript received October 14, 2001; revised January 15, 2002. The material in this correspondence was submitted for consideration of presentation at the 2002 IEEE International Symposium on Information Theory, Lausanne, Switzerland.

The author is with the Department of Communications and Integrated Systems, Tokyo Institute of Technology, Tokyo 152-8552, Japan (e-mail: ryutaroh@rmatsumoto.org).

Communicated by P. W. Shor, Associate Editor for Quantum Information Theory.
Publisher Item Identifier S 0018-9448(02)05176-3.

munication. We have to protect quantum states from environmental noise in quantum computation and some methods in quantum communication, such as the quantum superdense coding [2], [3]. The quantum error-correcting codes (or quantum codes) independently proposed by Shor [12] and Steane [13] constitute one of the techniques for protecting quantum states.

Let us explain quantum codes. We begin with the notion of t-error correction. Let $\mathcal{H}$ be a q-dimensional complex linear space, where q is a prime power, and suppose that $\mathcal{H}$ represents a physical system of interest. A quantum code Q is a q^k-dimensional subspace of $\mathcal{H}^{\otimes n}$. When we want to protect a quantum state $|\varphi\rangle \in \mathcal{H}^{\otimes k}$, we encode $|\varphi\rangle$ into a state in Q. So we encode a quantum state of k particles into that of n particles. Such a code Q is said to be an $[[n, k]]$ quantum code. Suppose that we send $|\varphi\rangle \in Q$ and receive $|\psi\rangle \in \mathcal{H}^{\otimes n}$. A quantum code Q is said to be *t-error-correcting* if we can decode $|\varphi\rangle$ from $|\psi\rangle$ provided that at least the states of $n - t$ particles in $|\psi\rangle$ are left unchanged from $|\varphi\rangle$.

Since a change of a quantum state is continuous, the notion of t-error correction seems irrational at first glance [8]. This notion can be justified as follows. In general, the decoding process of a quantum code does not decode perfectly the transmitted quantum state from a received one. However, the decoded state and a transmitted state become closer as t increases provided that the quantum channel used is memoryless as a q-ary channel [11, Sec. 7.4], [9]. A quantitative relation between the closeness of states, the noisiness of a channel, and t can be found in [9].

In [9], it is shown that one can make the decoded state arbitrarily close to the transmitted state by increasing the code length provided that the ratio t/n is fixed and is sufficiently large compared with the noisiness of the channel. This is a major motivation for studying long codes as in the classical coding theory [10, Sec. 4.3].

A sequence of t_i-error-correcting $[[n_i, k_i]]$ quantum codes is said to be asymptotically good if

$$\lim_{i\to\infty} n_i = \infty$$
$$\liminf_{i\to\infty} k_i/n_i > 0$$
$$\liminf_{i\to\infty} t_i/n_i > 0.$$

Ashikhmin, Litsyn, and Tsfasman [1] constructed the first asymptotically good sequence of quantum codes. After that, Chen, Ling, and Xing [5] also constructed an asymptotically good sequence of binary quantum codes from algebraic curves based on the idea in [16] better than those in [1] in certain range of parameters. Note that Chen [4] also proposed the same construction of quantum codes as that in [1].

The construction of Ashikhmin *et al.* used a sequence of algebraic curves having many rational points over a finite field. In their construction, they do not use at least g rational points on the curve (see [1, remark below Theorem 4]), where g is the genus of the curve. We can easily see that the use of more rational points improves the performance of the constructed sequence of quantum codes.

Garcia and Stichtenoth [7] showed the first sequence of algebraic curves with many rational points defined by explicit equations. By using their explicit sequence of curves we shall construct an asymptotically good sequence of quantum codes using asymptotically all the rational points on algebraic curves.

II. Construction

Ashikhmin *et al.* used the following fact in their construction of quantum codes. The minimum distance of a quantum code is the maximum number of detectable quantum errors that can be written as a tensor product of the Pauli spin operators.

Proposition 1: Suppose that we have a chain of classical linear codes $C^\perp \subset C \subset C'$ in $\boldsymbol{F}_{2^{2m}}^n$, where $C^\perp$ denotes the dual codes of C with respect to the standard inner product. Suppose also that C is an $[n, k, d]$ code and C' is $[n, k', d']$ one with $k' \geq k + 2$. From this chain we can construct a $[[2nm, 2m(k + k' - n), \min\{d, \frac{3}{2}d'\}]]$ binary quantum code. Proposition 1 is based on the construction of quantum codes proposed in [6], [14].

Hereafter, we shall use the formalism of algebraic function fields instead of algebraic curves. Notations used are exactly the same as those in Stichtenoth's textbook [15]. We construct an asymptotically good sequence of binary quantum codes from the Garcia–Stichtenoth function field [7]. Let $F_i = \boldsymbol{F}_{q^2}(x_1, z_2, \ldots, z_i)$ with

$$z_i^q + z_i - x_{i-1}^{q+1} = 0,$$
$$x_i = z_i/x_{i-1}.$$

Proposition 2: For an integer $m \geq 2$ there exists a sequence of $[[2mn_i, 2mk_i, d_i]]$ binary quantum codes such that

$$\lim_{i\to\infty} n_i = \infty$$
$$\liminf_{i\to\infty} k_i/n_i \geq R_m(\delta)$$
$$\liminf_{i\to\infty} d_i/2mn_i \geq \delta$$

for

$$0 < \delta \leq \frac{1}{2m}\left(\frac{1}{2} - \frac{1}{2^m - 1}\right) \tag{1}$$

where

$$R_m(\delta) = 1 - \frac{10}{3}m\delta - \frac{2}{2^m - 1}. \tag{2}$$

Remark 3: For those who read [1], we highlight the difference between the construction in [1] and ours. The problem of constructing a family of classical self-orthogonal algebraic geometry codes suitable for Proposition 1 is to find a set of rational places $\{P_1, \ldots, P_n\}$ and a divisor G with $\operatorname{supp} G \cap \{P_1, \ldots, P_n\} = \emptyset$ such that there exists a differential η whose divisor is

$$2G - (P_1 + \cdots + P_n).$$

For the general algebraic function field used in [1], it seems difficult to use asymptotically all the rational places as $\{P_1, \ldots, P_n\}$ and find G and η. From the Garcia–Stichtenoth function fields, we shall explicitly construct G and η in the following proof while using asymptotically all the rational places, namely,

$$\eta = \frac{x_1^{q^2-2}\,dx_1}{x_1^{q^2-1} - 1}$$
$$G = ((\eta) + P_1 + \cdots + P_n)/2$$

where $P_1 + \cdots + P_n$ is the zero divisor of $x_1^{q^2-1} - 1$.

Proof of Proposition 2: We shall consider the Garcia–Stichtenoth function field F_i over $\boldsymbol{F}_{2^{2m}}$ with $i \geq 2$. Let $q = 2^m$.

Let $n_i = (q^2 - 1)q^{i-1}$ and $y = x_1^{q^2-1} - 1$. The zero divisor of y consists of n_i places of degree one [7, Sec. 3]. Therefore, we can write the zero divisor of y as $P_1 + \cdots + P_{n_i}$ such that $P_j \neq P_l$ for all j, l. For a divisor D of $F_i/\boldsymbol{F}_{q^2}$ with $\operatorname{supp} D \cap \{P_1, \ldots, P_{n_i}\} = \emptyset$, we shall consider a classical linear code $C(D)$ defined by

$$C(D) = \{(f(P_1), \ldots, f(P_{n_i})) \mid f \in \mathcal{L}(D)\}.$$

Let $\eta = dy/y = x_1^{q^2-2}\,dx_1/y$, $G_0' = (\eta) + P_1 + \cdots + P_{n_i}$, and P_∞ be the unique pole of x_1 in F_i. We have

$$G_0' = (q^2-2)(x_1) - (q^2-1)v_{P_\infty}(x_1)P_\infty + (dx_1).$$

The different exponent of F_i/F_1 is even at every place of F_i (see [7, text below Lemma 2.9]). Hence, the discrete valuation of (dx_1) is even at every place of F_i by [15, Remark IV.3.7]. Observe that $v_{P_\infty}(x_1) = -q^{i-1}$ [7]. Therefore, the valuation of the divisor G_0' is an even integer at every place of F_i. Define $G_0 = G_0'/2$. We have

$$\begin{aligned}\deg\, G_0 &= \frac{n_i + \deg(dx_1)}{2}\\ &= \frac{n_i + 2g_i - 2}{2}\\ &= n_i/2 + g_i - 1\end{aligned}$$

where g_i is the genus of $F_i/\boldsymbol{F}_{q^2}$.

Let j be a nonnegative integer. Let

$$H = (P_1 + \cdots + P_{n_i}) - (G_0 + jP_\infty) + (\eta) = G_0 - jP_\infty.$$

By [15, Proposition VII.1.2], we have $C(G_0 + jP_\infty)^\perp = C(H)$. Since $G_0 + jP_\infty \geq H$

$$C(G_0 + jP_\infty)^\perp \subseteq C(G_0 + jP_\infty).$$

Observe that $C(G_0 + jP_\infty)$ is an $[n_i, j + n_i/2, \geq n_i/2 - g_i + 1 - j]$ classical linear code if $j \leq n_i/2 - g_i$.

There is the inclusion of classical codes

$$\begin{aligned}&C\left(G_0 + \left(\left\lfloor\left(\frac{1}{2} - \delta'\right)n_i\right\rfloor - g_i + 1\right)P_\infty\right)^\perp\\ &\quad\subset C\left(G_0 + \left(\left\lfloor\left(\frac{1}{2} - \delta'\right)n_i\right\rfloor - g_i + 1\right)P_\infty\right)\\ &\quad\subset C\left(G_0 + \left(\left\lfloor\left(\frac{1}{2} - \frac{2}{3}\delta'\right)n_i\right\rfloor - g_i + 1\right)P_\infty\right)\end{aligned}$$

for $0 \leq \delta' \leq 1/2 - g_i/n_i$, and the condition $9/n_i \leq \delta' \leq 1/2 - g_i/n_i$ implies

$$\begin{aligned}&\dim C\left(G_0 + \left(\left\lfloor\left(\frac{1}{2} - \delta'\right)n_i\right\rfloor - g_i + 1\right)P_\infty\right) + 2\\ &\qquad\leq \dim C\left(G_0 + \left(\left\lfloor\left(\frac{1}{2} - \frac{2}{3}\delta'\right)n_i\right\rfloor - g_i + 1\right)P_\infty\right).\end{aligned}$$

Hence, by applying Proposition 1 to the inclusion above, for $9/n_i \leq \delta' \leq 1/2 - g_i/n_i$ we can construct $[[2mn_i, 2mk_i, d_i]]$ binary quantum codes with

$$k_i \geq \left(1 - \frac{5}{3}\delta'\right)n_i - 2g_i, \qquad d_i \geq \delta' n_i.$$

Since $\lim_{i\to\infty} n_i/g_i = 2^m - 1$ [7], by setting $\delta = \delta'/2m$ we have

$$\liminf_{i\to\infty} \frac{k_i}{n_i} \geq R_m(\delta), \qquad \liminf_{i\to\infty} \frac{d_i}{2mn_i} \geq \delta$$

for the range of δ specified in (1). □

By choosing an appropriate value m for every δ, we can construct a sequence of $[[2mn_i, 2mk_i, d_i]]$ binary quantum codes with

$$\liminf_{i\to\infty} \frac{k_i}{n_i} \geq R(\delta), \qquad \liminf_{i\to\infty} \frac{d_i}{2mn_i} \geq \delta$$

where $R(\delta) = R_m(\delta)$ for

$$\frac{3\cdot 2^m}{5(2^m-1)(2^{m+1}-1)} \leq \delta \leq \min\left\{\frac{5}{84},\, \frac{3\cdot 2^{m-1}}{5(2^{m-1}-1)(2^m-1)}\right\}.$$

The sequences in [1], [5] and the sequences in this correspondence are compared in Fig. 1. Since (2) is larger than [1, eq. (21)], the information rate of our sequence is always larger than that of [1] at every relative minimum distance.

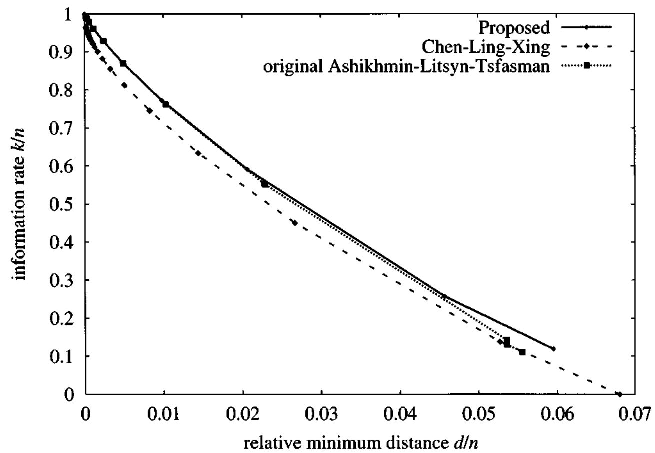

Fig. 1. Asymptotically good sequences of quantum codes.

ACKNOWLEDGMENT

The author wishes to thank the anonymous referees for providing detailed comments on the initial manuscript, which identified several errors.

REFERENCES

[1] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, "Asymptotically good quantum codes," *Phys. Rev. A*, vol. 63, no. 3, p. 032311, Mar. 2001.

[2] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem," arXiv:quant-ph/0106052, June 2001.

[3] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operations on Einstein–Podolsky–Rosen states," *Phys. Rev. Lett.*, vol. 69, no. 20, pp. 2881–2884, Nov. 1992.

[4] H. Chen, "Some good quantum error-correcting codes from algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2059–2061, July 2001.

[5] H. Chen, S. Ling, and C. Xing, "Asymptotically good quantum codes exceeding the Ashikhmin–Litsyn–Tsfasman bound," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2055–2058, July 2001.

[6] G. Cohen, S. Encheva, and S. Litsyn, "On binary constructions of quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2495–2498, Nov. 1999.

[7] A. Garcia and H. Stichtenoth, "A tower of Artin–Schreier extensions of function fields, attaining the Drinfeld–Vladut bound," *Invent. Math.*, vol. 121, no. 1, pp. 211–222, July 1995.

[8] S. Kak, "The initialization problem in quantum computing," *Found. Phys.*, vol. 29, no. 2, pp. 267–279, Feb. 1999. arXiv:quant-ph/9811005.

[9] R. Matsumoto, "Fidelity of a $\boldsymbol{t}$-error correcting quantum code with more than $\boldsymbol{t}$ errors," *Phys. Rev. A*, vol. 64, no. 2, p. 022314, Aug. 2001.

[10] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA: MIT Press, 1972.

[11] J. Preskill. (1998) Lecture Notes for Physics 229: Quantum Information and Computation. [Online]. Available: http://www.theory.caltech.edu/people/preskill/ph229

[12] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, pp. 2493–2496, Oct. 1995.

[13] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, pp. 793–797, July 1996.

[14] A. M. Steane, "Enlargement of Calderbank–Shor–Steane quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2492–2495, Nov. 1999.

[15] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 1993.

[16] C. Xing, H. Niederreiter, and K. Y. Lam, "A generalization of algebraic-geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2498–2501, Nov. 1999.