Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound

Chen, Hao; Ling, San; Xing, Chaoping

2001

Chen, H., Ling, S., & Xing, C. (2001). Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound. IEEE Transactions on Information Theory, 47(5), 2055-2058.

https://hdl.handle.net/10356/95782

https://doi.org/10.1109/18.930941

Asymptotically Good Quantum Codes Exceeding the Ashikhmin–Litsyn–Tsfasman Bound

Hao Chen, San Ling, and Chaoping Xing

***Abstract*—It is known that quantum error correction can be achieved using classical binary codes or additive codes over $\boldsymbol{F}_4$ (see [2], [3], [9]). In [1] and [4], asymptotically good quantum codes from algebraic-geometry codes were constructed and, in [1], a bound on (δ, R) was computed from the Tsfasman–Vlăduţ–Zink bound of the theory of classical algebraic-geometry codes. In this correspondence, by the use of a concatenation technique we construct a family of asymptotically good quantum codes exceeding the bound in [1] in a small interval.**

***Index Terms*—Algebraic-geometry codes, concatenated codes, Calderbank–Shor–Steane (CSS) construction, quantum codes.**

I. Introduction

Since the pioneering works reported in [3], [8], [9], the theory of quantum error-correcting codes has been rapidly developing. A thorough discussion of the principles of quantum coding theory was given in [2], and many examples and tables on various bounds were given there. Many kinds of interesting good quantum codes were also constructed using classical binary codes, see, e.g., [5], [7], [10]. It is natural to consider using the theory of algebraic-geometry codes to construct good quantum codes. In [1] and [4], a family of asymptotically good quantum codes (i.e., $R = \lim_{i\to\infty} \frac{k_i}{n_i} > 0$ and $\delta = \lim_{i\to\infty} \frac{d_i}{n_i} > 0$ for the family of quantum $[[n_i, k_i, d_i]]$ codes) was constructed from the algebraic-geometry codes arising from the well-known asymptotically good family of curves over $\boldsymbol{F}_{2^{2t}}$ attaining the Drinfeld–Vlăduţ bound [6], [11]. The binary expansions of a pair of the asymptotically good algebraic-geometry codes were used to produce the asymptotically good quantum codes with $R + \delta \geq \frac{1}{12}$ in [4] from the Calderbank–Shor–Steane (CSS) construction (see [2], [3], [9], or Theorem 1.4 at the end of this Introduction). In [1], the binary expansions of asymptotically good algebraic-geometry codes were inserted into Steane's enlargement of the CSS construction [10] to produce asymptotically good quantum codes as in the following theorem.

Theorem 1.1 (Ashikhmin, Litsyn, and Tsfasman [1], [12]): For any $\delta \in (0, \frac{1}{18})$ and R lying on the broken line given by the piecewise-linear function

$$R(\delta) = 1 - \frac{1}{2^{m-1} - 1} - \frac{10}{3} m\delta, \qquad \text{when } \delta \in [\delta_m, \delta_{m-1}] \quad (1)$$

for $m = 3, 4, 5, \ldots$ and where $\delta_2 = \frac{1}{18}$, $\delta_3 = \frac{3}{56}$, and

$$\delta_m = \frac{3}{5} \frac{2^{m-2}}{(2^{m-1} - 1)(2^m - 1)}, \qquad \text{for } m = 4, 5, 6, \ldots$$

Manuscript received August 14, 2000; revised December 6, 2000. The work of H. Chen was supported in part by NNSF. The work of S. Ling and C. Xing was supported in part by MOE-ARF under Research Grant R146-000-018-112. This work was also supported in part by NSTB-MOE under Research Grant R252-000-015-203.

H. Chen is with the Department of Mathematics, Zhongshan University, Guangzhou, Guangdong 510275, People's Republic of China, and also with the Department of Computer Science, National University of Singapore, Singapore 117543, Republic of Singapore (e-mail: dcschenh@nus.edu.sg).

S. Ling and C. Xing are with the Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore (e-mail: matlings@nus.edu.sg; matxcp@nus.edu.sg).

Communicated by A. Barg, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(01)04668-5.

there exist polynomially constructible families of quantum codes with $n \to \infty$ and asymptotic parameters greater than or equal to (δ, R).

The main result of the present correspondence is the following.

Theorem 1.2: Let

$$\delta_t = \frac{2}{3} \frac{2^t - 3}{(2t+1)(2^t - 1)}.$$

For $t \geq 3$ and $\delta \in (0, \delta_t)$, there exist polynomially constructible families of quantum codes with $n \to \infty$ and asymptotic parameters $(\delta, R_1(\delta))$, where

$$R_1(\delta) = 3t(\delta_t - \delta).$$

Corollary 1.3: Using $t = 3$ and the equation $R + 9\delta = \frac{30}{49}$, the bound in Theorem 1.2 is defined in $(0, \frac{10}{147})$ (bigger than $(0, \frac{1}{18})$ in the Ashikhmin–Litsyn–Tsfasman bound) and exceeds the Ashikhmin–Litsyn–Tsfasman bound in the interval $(\frac{8}{147}, \frac{1}{18})$.

Proof: The first part of the statement is clear from Theorem 1.2. For the second part, it is clear that, in the interval $(8/147, 1/18)$, the Ashikhmin–Litsyn–Tsfasman bound is defined by $R(\delta) = 2/3 - 10\delta$ and the bound in Theorem 1.2 is given by $R_1(\delta) = 30/49 - 9\delta$. These equations define two straight lines and it is easy to check that $R_1(1/18) > R(1/18)$ and $R_1(8/147) = R(8/147)$. Thus, the second part of the statement is proved.

The outline of our proof of Theorem 1.2 is as follows. We begin with an asymptotically good family of curves over $\boldsymbol{F}_{2^{2t}}$ satisfying the Drinfeld-Vlăduţ bound. From each of these curves, we construct a pair of algebraic–geometry codes over $\boldsymbol{F}_{2^{2t}}$, which are then used to yield, via concatenation, a pair of binary codes $\mathcal{C}_1$ and $\mathcal{C}_2$ such that $\mathcal{C}_1 \subset \mathcal{C}_2$. The CSS construction (see Theorem 1.4 below) is then applied to these pairs of codes to yield the desired family of quantum codes with good asymptotic parameters.

We recall now the CSS construction (cf. [2], [3], or [9]). For a classical code C (C can be a nonlinear code), we denote by $\mathrm{wt}(C)$ the minimal Hamming weight of all codewords of C.

Theorem 1.4 (Calderbank–Shor–Steane): Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two binary codes with parameters $[n, k_1]$ and $[n, k_2]$, respectively. Suppose that $\mathcal{C}_1 \subset \mathcal{C}_2$. Then a quantum $[[n, k_2 - k_1, d]]$ code can be constructed, where

$$d = \min\{\mathrm{wt}(\mathcal{C}_2 \backslash \mathcal{C}_1), \mathrm{wt}(\mathcal{C}_1^{\perp} \backslash \mathcal{C}_2^{\perp})\}.$$

The correspondence is organized as follows. As concatenation is used to construct the codes desired in Theorem 1.2, we give in Section II the concatenation code and a description of its dual code. The description of the dual code is interesting in its own right. In Section III, we construct the asymptotically good quantum codes as claimed in our main result Theorem 1.2.

II. The Dual Code of a Concatenated Code

Let C be an $[s, t, d]$ code over $\boldsymbol{F}_{q^k}$ and, for $i = 1, 2, \ldots, s$, let $\pi_i: \boldsymbol{F}_{q^k} \to \boldsymbol{F}_q^{n_i}$ be an $\boldsymbol{F}_q$-linear injective map whose image $C_i = im(\pi_i)$ is an $[n_i, k, d_i]$ code over $\boldsymbol{F}_q$. The image $\pi(C)$ of the following $\boldsymbol{F}_q$-linear injective map:

$$\begin{array}{rcl} \pi : C & \longrightarrow & \boldsymbol{F}_q^{n_1 + \cdots + n_s} \\ (c_1, \ldots, c_s) & \longmapsto & (\pi_1(c_1), \ldots, \pi_s(c_s)) \end{array} \qquad (2)$$

is an $[n_1 + \cdots + n_s, tk]$ linear (concatenated) code over $\boldsymbol{F}_q$. The following observation can be easily verified.

Lemma 2.1: Suppose the images $im(\pi_i)(1 \le i \le s)$ are identical and have parameters $[n, k, w]$. Then $\pi(C)$ is an $[ns, tk]$ linear code over $\boldsymbol{F}_q$ with the minimum distance at least wd.

Next we describe the dual code of $\pi(C)$. We show in Theorem 2.3 that it is the direct sum $D \oplus \pi'(C^\perp)$, where D and $\pi'(C^\perp)$ are two codes to be described.

Let $C_i^\perp \subset \boldsymbol{F}_q^{n_i}$ be the dual code of C_i and let D be the direct sum $C_1^\perp \oplus \cdots \oplus C_s^\perp$. It is clear that $D \subset \boldsymbol{F}_q^{n_1+\cdots+n_s}$ is an

$$[n_1 + \cdots + n_s, n_1 + \cdots + n_s - sk]$$

linear code over $\boldsymbol{F}_q$.

To describe $\pi'(C^\perp)$, we need to first define $\boldsymbol{F}_q$-linear injective maps $\pi_i' : \boldsymbol{F}_{q^k} \to \boldsymbol{F}_q^{n_i}$, for $1 \le i \le s$.

Let $\{e_1, \ldots, e_k\}$ be an $\boldsymbol{F}_q$-basis of $\boldsymbol{F}_{q^k}$. A set $\{e_1', \ldots, e_k'\}$ of $\boldsymbol{F}_{q^k}$ is called the dual basis of $\{e_1, \ldots, e_k\}$ if we have $\mathrm{Tr}_{\boldsymbol{F}_{q^k}/\boldsymbol{F}_q}(e_i e_j') = \delta_{ij}$ (Kronecker symbol). It is well known that the dual basis always exists. We say that a basis is self-dual if it is its own dual.

Now we choose an $\boldsymbol{F}_q$-basis $\{e_1, \ldots, e_k\}$ for $\boldsymbol{F}_{q^k}$ and let $\{e_1', \ldots, e_k'\}$ be its dual basis. For each $1 \le i \le s$, we define the $\boldsymbol{F}_q$-linear injective map $\pi_i' : \boldsymbol{F}_{q^k} \to \boldsymbol{F}_q^{n_i}$ by first defining the images $\pi_i'(e_j')$ for $1 \le j \le k$, and then extending the map $\boldsymbol{F}_q$-linearly. For each $1 \le j \le k$ and $1 \le \ell \le k$, we want $\pi_i'(e_j')$ to satisfy

$$\pi_i(e_\ell) \cdot \pi_i'(e_j') = \delta_{\ell j} \tag{3}$$

where $\delta_{\ell j}$ is the Kronecker symbol. As ℓ runs through all values from 1 to k, (3) gives a linearly independent system of k equations in n_i variables. As $k \le n_i$, the system admits a solution, which shall be defined as our $\pi_i'(e_j')$. In general, this choice of $\pi_i'(e_j')$ is not unique, but is unique up to addition by a vector in $C_i^\perp$.

It is clear that π_i' is an $\boldsymbol{F}_q$-linear injective map whose image is an $[n_i, k]$ linear code over $\boldsymbol{F}_q$.

Let $C^\perp \subset \boldsymbol{F}_{q^k}^s$ be the dual code of C. This is an $[s, s-t]$ linear code over $\boldsymbol{F}_{q^k}$. We define $\pi'(C^\perp)$ to be the concatenated code defined through $C^\perp$ and $\pi_1', \ldots, \pi_s'$, similar to the way $\pi(C)$ was defined through C and $\pi_1, \ldots, \pi_s$. This is an $[n_1 + \cdots + n_s, (s-t)k]$ linear code over $\boldsymbol{F}_q$.

Lemma 2.2: For each $1 \le i \le s$, we have $C_i^\perp \cap im(\pi_i') = 0$. Therefore, $D \cap \pi'(C^\perp) = 0$.

Proof: The second statement follows directly from the first. The first statement follows directly from (3).

Theorem 2.3: The dual code $\pi(C)^\perp$ of $\pi(C)$ is the direct sum $D \oplus \pi'(C^\perp)$.

Proof: Since

$$\dim_{\boldsymbol{F}_q}(D) + \dim_{\boldsymbol{F}_q}(\pi'(C^\perp)) = n_1 + \cdots + n_s - tk$$

and it is clear that $D \subset \pi(C)^\perp$, we only need to prove $\pi'(C^\perp) \subset \pi(C)^\perp$.

Let

$$a = (a_1, \ldots, a_s) \in C$$

and

$$b = (b_1, \ldots, b_s) \in C^\perp$$

so that

$$\pi(a) = (\pi_1(a_1), \ldots, \pi_s(a_s)) \in \pi(C)$$

and

$$\pi'(b) = (\pi_1'(b_1), \ldots, \pi_s'(b_s)) \in \pi'(C^\perp).$$

Using (3) and the expansions

$$a_i = a_i^1 e_1 + \cdots + a_i^k e_k$$

and

$$b_i = b_i^1 e_1' + \cdots + b_i^k e_k'$$

where $a_i^j, b_i^j \in \boldsymbol{F}_q$ for all $1 \le i \le s$ and $1 \le j \le k$, we have

$$\begin{aligned}\pi(a) \cdot \pi'(b) &= \sum_{i=1}^{s} \pi_i(a_i) \cdot \pi_i'(b_i) \\ &= \sum_{i=1}^{s} \left(\sum_{\ell=1}^{k} a_i^\ell \pi_i(e_\ell) \right) \cdot \left(\sum_{j=1}^{k} b_i^j \pi_i'(e_j') \right) \\ &= \sum_{i=1}^{s} \sum_{j=1}^{k} a_i^j b_i^j.\end{aligned} \tag{4}$$

On the other hand, since $a \in C$ and $b \in C^\perp$, we have $\sum_{i=1}^{s} a_i b_i = 0$. Hence

$$\begin{aligned}0 &= \sum_{i=1}^{s} (a_i^1 e_1 + \cdots + a_i^k e_k)(b_i^1 e_1' + \cdots + b_i^k e_k') \\ &= \sum_{i=1}^{s} \sum_{\ell, j=1}^{k} a_i^\ell b_i^j e_\ell e_j'.\end{aligned} \tag{5}$$

By taking the trace of (5) and using the property of the dual basis, we have

$$\sum_{i=1}^{s} \sum_{j=1}^{k} a_i^j b_i^j = 0.$$

Thus, $\pi(a) \cdot \pi'(b) = 0$, so $\pi'(C^\perp) \subset \pi(C)^\perp$.

Remark: Although the choice of the maps π_i' (and hence π') is not unique, we have noted that it is unique up to addition by a vector in $C_i^\perp$. Therefore, the direct sum $D \oplus \pi'(C^\perp)$ is uniquely defined.

Corollary 2.4: Suppose $n_1 = \cdots = n_s = k$ and, for each $1 \le i \le s$, π_i is the expansion with respect to some $\boldsymbol{F}_q$-basis T of $\boldsymbol{F}_{q^k}$, so that $\pi(C)$ is the expansion of C with respect to the basis T. Then the dual of $\pi(C)$ is the expansion of $C^\perp$ with respect to the dual basis $T^\perp$.

Corollary 2.4 follows directly from Theorem 2.3. The result of Kasami and Lin used in [1, Theorem 3] is a direct consequence of Corollary 2.4.

III. Proof of Theorem 1.2

Let X be a smooth, projective, absolutely irreducible curve of genus g defined over $\boldsymbol{F}_q$, let D be a set of N $\boldsymbol{F}_q$-rational points of X and let G be an $\boldsymbol{F}_q$-rational divisor of X such that $\mathrm{supp}(G) \cap D = \emptyset$ and $2g - 2 < \deg(G) < N$, where $\mathrm{supp}(G)$ and $\deg(G)$ denote the support and the degree of G, respectively. Then the functional algebraic-geometry code $C_L(G, D)$ and the residue algebraic-geometry code $C_\Omega(G, D)$ can be defined. It is well known that the dual of $C_L(G, D)$ is $C_\Omega(G, D)$ (e.g., see [11]). Their parameters are as follows.

Theorem 3.1 (cf. [11]): The functional code $C_L(G, D)$ is an $[N, \deg(G)-g+1, N-\deg(G)]$ linear code over $\boldsymbol{F}_q$ and the residue code $C_\Omega(G, D)$ is an $[N, N-\deg(G)+g-1, \deg(G)-2g+2]$ linear code over $\boldsymbol{F}_q$.

We assume $q = 2^{2t}$ from now on.

It is known [6], [11] that there exists a family of algebraic curves $\{X_n\}$ over $\boldsymbol{F}_q$ with $g(n) \to \infty$ attaining the Drinfeld–Vlăduţ bound, i.e.,

$$\limsup_{n\to\infty}(N(X_n/\boldsymbol{F}_q)/g(n)) = \sqrt{q}-1$$

where $N(X_n/\boldsymbol{F}_q)$ and $g(n)$ are the number of $\boldsymbol{F}_q$-rational points and the genus of X_n, respectively.

We choose a rational point $P^{(n)}$ on each X_n and put

$$D_n = \sum_{P\in X_n(\boldsymbol{F}_q)\setminus\{P^{(n)}\}} P,$$

where $X_n(\boldsymbol{F}_q)$ is the set of $\boldsymbol{F}_q$-rational points of X_n. Then

$$N(n) := |\mathrm{supp}(D_n)| = N(X_n/\boldsymbol{F}_q) - 1$$

satisfies

$$\limsup_{n\to\infty}(N(n)/g(n)) = \sqrt{q}-1.$$

For each n, let $G_1(n), G_2(n)$ be two divisors of X_n supported at the point $P^{(n)}$ and, for $i = 1, 2$, let $m_i(n)$ denote the degree of $G_i(n)$. Suppose that

$$2g(n)-2 < m_2(n) < m_1(n) < N(n).$$

Consider the algebraic-geometry functional codes

$$T_i = C_L(G_i(n), D_n)(i = 1, 2).$$

Note that $T_2 \subset T_1$ and that T_i is an

$$[N(n), m_i(n)-g(n)+1, N(n)-m_i(n)]$$

linear code over $\boldsymbol{F}_q$. The dual of T_i is the algebraic-geometry residue code $T_i^\perp = C_\Omega(G_i(n), D_n)$, which is an

$$[N(n), N(n)-m_i(n)+g(n)-1, m_i(n)-2g(n)+2]$$

linear code over $\boldsymbol{F}_q$ (see Theorem 3.1).

Proof of Theorem 1.2: For any $t \in \{3, 4, 5, \ldots\}$, let π_* be an $\boldsymbol{F}_2$-linear injective map from $\boldsymbol{F}_{2^{2t}}$ into $\boldsymbol{F}_2^{2t+1}$ whose image C_* is the trivial binary maximum-distance separable (MDS) $[2t+1, 2t, 2]$ code. Then, using the notation of Section II with $\pi_1 = \cdots = \pi_{N(n)} = \pi_*$, we have the concatenated codes $\mathcal{C}_2 = \pi(T_2) \subset \mathcal{C}_1 = \pi(T_1)$ as described in Section II. From Lemma 2.1, $\mathcal{C}_i (i = 1, 2)$ is a binary

$$[(2t+1)N(n), 2t(m_i(n)-g(n)+1), 2(N(n)-m_i(n))]$$

code. The dual of $\mathcal{C}_i$ is $\mathcal{C}_i^\perp = D \oplus (\pi'(C_\Omega(G_i(n), D_n)))$ from Theorem 2.3.

We claim that, for any vector $\boldsymbol{x} \in (\mathcal{C}_2^\perp \setminus \mathcal{C}_1^\perp)$, the weight $\mathrm{wt}(\boldsymbol{x})$ satisfies $\mathrm{wt}(\boldsymbol{x}) \ge m_2(n)-2g(n)+2$. Indeed, let

$$\boldsymbol{x} = \pi'(\boldsymbol{x}') + \boldsymbol{b} = (\pi_*'(x_1)+b_1, \ldots, \pi_*'(x_{N(n)})+b_{N(n)})$$

with

$$\boldsymbol{x}' = (x_1, \ldots, x_{N(n)}) \in T_2^\perp$$

and

$$\boldsymbol{b} = (b_1, \ldots, b_{N(n)}) \in D.$$

It is clear that $\boldsymbol{x}'$ is a nonzero vector since $\boldsymbol{x}$ is not in $\mathcal{C}_1^\perp$, thus $\mathrm{wt}(\boldsymbol{x}') \ge m_2(n)-2g(n)+2$. At each position j with x_j nonzero, we know that $\pi_*'(x_j)+b_j$ is nonzero from the fact $b_j \in C_*^\perp$ and $C_*^\perp \cap im(\pi_*') = 0$. Thus, the claim is proved.

Using the CSS construction (see Theorem 1.4 in Section I), we have, for each n, a

$$\begin{aligned}[[(2t+1)N(n),\ & 2t(m_1(n)-m_2(n)),\\ & \ge \min\{2(N(n)-m_1(n)), m_2(n)-2g(n)+2\}]]\end{aligned}$$

quantum code $\mathcal{A}_n$. Let $k(n) = m_1(n)-m_2(n)$. It is clear that $k(n)$ can take any integer in $(0, N(n)-2g(n)]$. For any such $k(n)$, taking

$$m_1(n) = \lfloor(2N(n)+2g(n)+k(n)-2)/3\rfloor$$

where $\lfloor u\rfloor$ means the greatest integer less than or equal to the real number u, we have

$$\begin{aligned}2(N(n)-m_1(n)) &\ge m_2(n)-2g(n)+2\\ &\ge \frac{2}{3}(N(n)-2g(n)-k(n)+1).\end{aligned}$$

Thus, $\mathcal{A}_n$ has parameters

$$\left[\left[(2t+1)N(n), 2tk(n), \ge \tfrac{2}{3}(N(n)-2g(n)-k(n)+1)\right]\right].$$

For a fixed $\lambda \in (0, 1-2/(\sqrt{q}-1))$, we let $k(n)/N(n) \to \lambda$ as n tends to ∞. Put

$$R := \lim_{n\to\infty}\frac{2tk(n)}{(2t+1)N(n)} = \frac{2t}{2t+1}\lambda$$

and

$$\begin{aligned}\delta &:= \limsup_{n\to\infty}\frac{2(N(n)-2g(n)-k(n)+1)}{3(2t+1)N(n)}\\ &= \frac{2}{3(2t+1)}\left(1-\frac{2}{2^t-1}-\lambda\right).\end{aligned}$$

Then (δ, R) lies on the line defined by

$$R_1(\delta) = \frac{2t}{2t+1}\left(1-\frac{2}{2^t-1}\right)-3t\delta.$$

Hence, we have found the family of quantum codes with the desired asymptotic parameters. Moreover, since the algebraic-geometry codes used here and concatenation are polynomially computable (see, for example, [11]), our conclusion of Theorem 1.2 is proved.

Acknowledgment

The authors wish to thank Prof. M. A. Tsfasman for the discussion on the result in [1] and to Prof. A. M. Steane for his encouragement. They also thank the anonymous referee for his/her very helpful suggestions and comments which led to improvement in the exposition of this correspondence.

References

[1] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, "Asymptotically good quantum codes," paper, quant-ph/0006061.
[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*, vol. 44, pp. 1369–1387, July 1998.
[3] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, 1996.
[4] H. Chen, "Some good quantum error-correcting codes from algebraic geometry codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2059–2061, July 2001.
[5] G. Cohen, S. Encheva, and S. Litsyn, "On binary construction of quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2495–2498, Nov. 1999.
[6] A. Garcia and H. Stichtenoth, "On the asymptotic behavior of some towers of function fields over finite fields," *J. Number Theory*, vol. 61, pp. 248–273, 1996.
[7] M. Grassl, W. Geiselmann, and T. Beth, "Quantum Reed–Solomon codes," in *Proc. AAECC-13 (Lecture Notes in Computer Science)*, M. Fossorier, H. Imai, S. Lin, and A. Poli, Eds. New York: Springer-Verlag, 1999, vol. 1719, pp. 231–244.
[8] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, pp. R2493–R2496, 1995.
[9] A. M. Steane, "Multiple particle interference and quantum error correction," in *Proc. Roy. Soc. London A*, vol. 452, 1996, pp. 2551–2577.
[10] ——, "Enlargement of Calderbank–Shor–Steane quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2492–2495, Nov. 1999.
[11] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic Geometric Codes*. Dordrecht/Boston/London: Kluwer, 1991.
[12] M. A. Tsfasman, private communication, July 18, 2000.
[13] 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.