# This document is downloaded from DR-NTU (https://dr.ntu.edu.sg) Nanyang Technological University, Singapore. 

## Quantum codes from concatenated algebraic-geometric codes

Chen, Hao; Ling, San; Xing, Chaoping

2005

Chen, H., Ling, S., \& Xing, C. (2005). Quantum Codes From Concatenated Algebraic-Geometric Codes. IEEE Transactions on Information Theory, 51(8), 2915-2920.
https://hdl.handle.net/10356/96320
https://doi.org/10.1109/TIT.2005.851760

[^0]
# Quantum Codes From Concatenated Algebraic-Geometric Codes 

Hao Chen, San Ling, and Chaoping Xing


#### Abstract

We apply Steane's enlargement of the Calderbank-ShorSteane (CSS) codes and additive codes over $\boldsymbol{F}_{4}$ to concatenated alge-braic-geometric codes to construct many good quantum codes with fewer restrictions on the parameters compared to some known quantum codes. Some of the quantum codes we have constructed are either optimal or have parameters as good as the best known codes, while some have parameters better than those obtained from other known constructions.


Index Terms-Algebraic-geometric codes, concatenated codes, enlargement of the Calderbank-Shor-Steane (CSS) codes, quantum error-correcting codes.

## I. Introduction and Preliminaries

Since the pioneering works in [4], [11], [10], the theory of quantum error-correcting codes has been rapidly developing. A thorough discussion of the principles of quantum coding theory is given in [3], where it is shown that quantum error correction can be achieved from additive codes over $\boldsymbol{F}_{4}$. Many techniques for constructing good quantum codes, such as the Calderbank-Shor-Steane (CSS) codes or Steane's enlargement of the CSS codes, etc., have been developed (see [4], [11], [10], [3], [13], [7]), and good quantum codes have been given by applying these constructions to Reed-Muller codes, Bose-Chaudhuri-Hocquenghem $(\mathrm{BCH})$ codes, and quadratic-resudue (QR) codes ([2], [3], [7]), Reed-Solomon codes ([8]) and algebraic-geometric codes ([5], [1], [6]). In [1], [5], the family of asymptotically good quantum codes is constructed and a bound (the Ashkhmin-Litsyn-Tsfasman bound) on the asymptotic parameters is given in [1]. We improved this bound in some parameter interval by concatenation technique in our earlier paper [6].

In this correspondence, the concatenated algebraic-geometric codes are inserted into the construction of Steane's enlargement of the CSS codes in [13] to provide several families of good quantum codes (Constructions A, B, C in Section III). We also apply the construction of quantum codes from additive codes over $F_{4}$ ([3]) to concatenated alge-braic-geometric codes to provide good quantum codes (Construction D in Section III). Compared with known quantum codes, some of the

The work of S. Ling and C. Xing was supported in part by MOE-ARF Research Grant R-146-000-029-112, DSTA Research Grant R-394-000-011-422, and NSTB-MOE Research Grant R252-000-015-203.
H. Chen is with the Department of Computing and Information Technology, Fudan University, Shanghai 200433, China (e-mail: chenhao1964cn@ yahoo.com.cn).
S. Ling was with the Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore. He is now with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637616, Republic of Singapore (e-mail: lingsan@ntu.edu.sg).
C. Xing is with the Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore and the Department of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, China (e-mail: xingcp@ math.nus.edu.sg).

Communicated by E. H. Knill, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2005.851760
quantum codes from our construction are either optimal or as good as the best known ones, while some have parameters better than those obtained from other constructions.

From the theory of algebraic curves over the finite field $\boldsymbol{F}_{q}$ there are quite complete results about the existence of the algebraic curves with special values of the genus and the number of $\boldsymbol{F}_{q}$ rational points. For a very useful table of such curves we refer to [15]. Thus, it is easy to apply our main results (Theorems 3.1,3.4,3.7,3.10) to the algebraic curves in the table [15] to get many good quantum codes from algebraic curves over finite fields. We give many examples of such quantum codes in this correspondence.

This correspondence is organized as follows. We recall first the basic results of Steane's enlargement of the CSS codes ([13]), quantum codes from additive codes over $\boldsymbol{F}_{4}$ ([3]), and some well-known facts about algebraic-geometric codes. The description of the dual of a concatenated code under both the ordinary inner product and the symplectic inner product is given in Section II. In Section III, new examples of quantum codes are constructed and compared with previous results.

We recall the following results in [13] and [3].
Theorem 1.1 (Steane's Enlargement of the CSS Codes [13]): Given a classical $[n, k, d]$ binary code $C$ which contains its dual, $C^{\perp} \subseteq C$, and which can be enlarged to an $\left[n, k^{\prime}>k+1, d^{\prime}\right]$ code $C^{\prime}$, a pure quantum code of parameters $\left[\left[n, k+k^{\prime}-n, \min \left(d,\left\lceil 3 d^{\prime} / 2\right\rceil\right)\right]\right]$ can be constructed.

We define the symplectic inner product on $\boldsymbol{F}_{2}^{2 n}$ as follows. For any two vectors

$$
\boldsymbol{a}=\left(a_{1}, \ldots, a_{n}, a_{n+1}, \ldots, a_{2 n}\right)
$$

and

$$
\begin{gather*}
\boldsymbol{b}=\left(b_{1}, \ldots, b_{n}, b_{n+1}, \ldots, b_{2 n}\right) \\
\langle\boldsymbol{a}, \boldsymbol{b}\rangle_{s}=\sum_{i=1}^{n} a_{i} b_{n+i}+\sum_{i=1}^{n} a_{n+i} b_{i}=\boldsymbol{a} S_{2 n} \boldsymbol{b}^{\tau} \tag{1}
\end{gather*}
$$

where $\tau$ denotes the transpose and $S_{2 n}$ is the symplectic matrix of size $2 n$

$$
\left(\begin{array}{cc}
0 & I_{n}  \tag{2}\\
I_{n} & 0
\end{array}\right)
$$

with $I_{n}$ the $n \times n$ identity matrix.
For a vector $\boldsymbol{a}=\left(a_{1}, \ldots, a_{n}, a_{n+1}, \ldots, a_{2 n}\right) \in \boldsymbol{F}_{2}^{2 n}$, where $\boldsymbol{F}_{2}^{2 n}$ is equipped with the symplectic inner product, we define its weight as

$$
\mathrm{wt}_{s}(\boldsymbol{a})=\#\left\{i \mid 1 \leq i \leq n, a_{i} \neq 0 \text { or } a_{n+i} \neq 0\right\}
$$

The notation $\mathrm{wt}(\boldsymbol{a})$ is reserved to denote the usual Hamming weight of $\boldsymbol{a}$.

Theorem 1.2 ([3]): Suppose that $C$ is a self-orthogonal $[2 n, n-k]$ code in $\boldsymbol{F}_{2}^{2 n}$ under the symplectic inner product (1), that $C^{\perp(s)}$ is its dual under (1), and that there are no vectors $\boldsymbol{v} \in C^{\perp(s)} \backslash C$ with $\mathrm{wt}_{s}(\boldsymbol{v})<d$. Then there is a quantum code with parameters $[[n, k, d]]$.

This is just equivalent to the main result in [3, Theorem 2] (see also [3, Theorem 1]).

We also need to recall the following facts on algebraic-geometric codes in [14] and [1]. Let $\mathcal{X} / \boldsymbol{F}_{q}$ be a smooth, projective curve of genus $g$, let $P_{1}, \ldots, P_{n}$ be $n$ rational points on $\mathcal{X}$ and let $G$ be a rational divisor with $2 g-2<\operatorname{deg}(G)<n$ and $\operatorname{supp}(G) \cap\left\{P_{1}, \ldots, P_{n}\right\}=\emptyset$. Let $D=P_{1}+\cdots+P_{n}$. The functional algebraic-geometric code and residual algebraic-geometric code can be defined as in [14] and denoted
by $C_{L}(G, D)$ and $C_{\Omega}(G, D)$. It is well known that $C_{L}(G, D)$ is an $[n, \operatorname{deg}(G)-g+1, n-\operatorname{deg}(G)]$ code and $C_{\Omega}(G, D)$ is an $[n, n-$ $\operatorname{deg}(G)+g-1, \operatorname{deg}(G)-2 g+2]$ code (over $\left.\boldsymbol{F}_{q}\right)$. Moreover, the dual of $C_{L}(G, D)$ is $C_{\Omega}(G, D)$ (see [14]). The codes in the following result of [1] are constructed from equivalent codes of algebraic-geometric codes (two codes $C_{1}, C_{2} \subset \boldsymbol{F}_{q}^{n}$ are said to be equivalent if and only if there exists nonzero $u_{1}, \ldots, u_{n} \in \boldsymbol{F}_{q}$ such that $\left.C_{1}=\left(u_{1}, \ldots, u_{n}\right) C_{2}\right)$.

Theorem 1.3 (see [1, Theorem 4]): Let $\boldsymbol{F}_{q}$ be a finite field of characteristic 2 , let $\mathcal{X} / \boldsymbol{F}_{q}$ be a curve of genus $g$ with at least $n^{\prime} \geq 4 g \boldsymbol{F}_{q}$-points. Then for any $2 g \leq n \leq n^{\prime}-g$ and any $a=2 g-1, \ldots,(n / 2)+g-1$, there is an $[n, n-a+g-1, a-2 g+2$ ] code $C_{a}$ over $\boldsymbol{F}_{q}$ with $C_{a}^{\perp} \subseteq C_{a}$.

Remark 1.1: Actually, the code $C_{a}$ in Theorem 1.3 is equivalent to the dual of the functional code corresponding to a divisor of degree $a$ (see [1, p. 4]). When the condition that there are at least $n^{\prime}+1 \boldsymbol{F}_{q}$-points on $\mathcal{X}$ is satisfied, the codes $C_{a}$ 's, for $a=2 g-1, \ldots,(n / 2)+g-1$, can be chosen in such a way that they satisfy $C_{a^{\prime}} \subseteq C_{a}$ whenever $a \leq a^{\prime}$. In fact, we can choose the $D$ and $E$ in the proof of Theorem 1.3 (see $[1, \mathrm{p} .4]$ ) to be the divisors supported at the $\boldsymbol{F}_{q}$-point outside the special set $P^{\prime}$ of $\boldsymbol{F}_{q}$-points in [1]. In this way, we can choose the same corresponding $E+2 D=E^{\prime}+2 D^{\prime}$ for different $a$ and $a^{\prime}$. Thus we have the same $\omega \in \Omega\left(P^{\prime}-2 D-E\right)=\Omega\left(P^{\prime}-2 D^{\prime}-E^{\prime}\right)$. Hence, we can take $P=P_{1}+\cdots+P_{n}$ consisting of the pole points of $\omega$, which is the same for both $C_{a}$ and $C_{a^{\prime}}$.

From Theorem 1.3 and the Remark 1.1 we have the following results. It is clear that under the assumption of the Corollaries 1.4 and 1.5 , the codes can be chosen in such a way that they satisfy $C_{a^{\prime}} \subseteq C_{a}$ whenever $a \leq a^{\prime}$.

Corollary 1.4 (Generalized Reed-Solomon Codes): Let $\boldsymbol{F}_{q}$ be as above. For any $1 \leq n \leq q$ and $0<m \leq(n-2) / 2$, there exists a code $C$ over $\boldsymbol{F}_{q}$ such that $C^{\perp} \subseteq C$ and with parameters $[n, n-m-$ $1, m+2]$.

Proof: We just take $\mathcal{X}$ to be the projective line with its $q+1 \boldsymbol{F}_{q}$-rational points in Theorem 1.3 and the conclusion follows directly.

Corollary 1.5 (Algebraic-Geometric Codes From Elliptic Curves):
Let $\boldsymbol{F}_{q}$ be as above. Suppose there is an elliptic curve (i.e., of genus $g=1$ ) with $N \geq 4 \boldsymbol{F}_{q}$-rational points. Then for any $2 \leq n \leq N-1$ and $1 \leq m \leq n / 2$, there exists a code $C$ over $\boldsymbol{F}_{q}$ such that $C^{\perp} \subseteq C$ and with parameters $[n, n-m, m]$.

Proof: We just take $\mathcal{X}$ in Theorem 1.3 to be this elliptic curve and the conclusion follows directly.

## II. The Dual of a Concatenated Code

In this section, we give a description of the dual of a concatenated code under both the ordinary and symplectic inner products.

## A. The Dual of a Concatenated Code Under the Ordinary Inner Product

We first recall the results in [6] on the dual of a concatenated code under the ordinary inner product.

Let $C$ be an $[s, t]$ code over $\boldsymbol{F}_{q^{k}}$ and, for $i=1,2, \ldots, s$, let $\pi_{i}: \boldsymbol{F}_{q^{k}} \rightarrow \boldsymbol{F}_{q}^{n_{i}}$ be an $\boldsymbol{F}_{q}$-linear injective map whose image $C_{i}=i m\left(\pi_{i}\right)$ is an $\left[n_{i}, k, d_{i}\right]$ code over $\boldsymbol{F}_{q}$. The image $\pi_{\left(C_{1}, \ldots, C_{s}\right)}(C)$ of the following $\boldsymbol{F}_{q}$-linear injective map:

$$
\begin{align*}
\pi_{\left(C_{1}, \ldots, C_{s}\right)}: C & \longrightarrow \boldsymbol{F}_{q}^{n_{1}+\cdots+n_{s}} \\
\left(\boldsymbol{c}_{1}, \ldots, \boldsymbol{c}_{s}\right) & \longmapsto\left(\pi_{1}\left(\boldsymbol{c}_{1}\right), \ldots, \pi_{s}\left(\boldsymbol{c}_{s}\right)\right) \tag{3}
\end{align*}
$$

is an $\left[n_{1}+\cdots+n_{s}, t k\right]$ linear (concatenated) code over $\boldsymbol{F}_{q}$.

Next, we describe the dual code of $\pi_{\left(C_{1}, \ldots, C_{s}\right)}(C)$ under the ordinary inner product. Let $C_{i}^{\perp} \subseteq \boldsymbol{F}_{q}^{n_{i}}$ be the dual code of $C_{i}$ under the ordinary inner product and let $D$ be the direct sum $C_{1}^{\perp} \oplus \cdots \oplus C_{s}^{\perp}$. It is clear that $D \subseteq \boldsymbol{F}_{q}^{n_{1}+\cdots+n_{s}}$ is an $\left[n_{1}+\cdots+n_{s}, n_{1}+\cdots+n_{s}-s k\right]$ linear code over $\boldsymbol{F}_{q}$.

On the other hand, let $\left\{e_{1}, \ldots, e_{k}\right\}$ be an $\boldsymbol{F}_{q}$-basis of $\boldsymbol{F}_{q^{k}}$. A set $\left\{e_{1}^{\prime}, \ldots, e_{k}^{\prime}\right\}$ of $\boldsymbol{F}_{q^{k}}$ is called the dual basis of $\left\{e_{1}, \ldots, e_{k}\right\}$ if we have $\operatorname{Tr}_{\boldsymbol{F}_{q^{k}} / \boldsymbol{F}_{q}}\left(e_{i} e_{j}^{\prime}\right)=\delta_{i j}$ (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. When $q=2$, it is well known that a self-dual basis of $\boldsymbol{F}_{2^{k}}$ over $\boldsymbol{F}_{2}$ always exists.

Now we choose an $\boldsymbol{F}_{q}$-basis $\left\{e_{1}, \ldots, e_{k}\right\}$ for $\boldsymbol{F}_{q^{k}}$ and let $\left\{e_{1}^{\prime}, \ldots, e_{k}^{\prime}\right\}$ be its dual basis. For each $1 \leq i \leq s$, we define the $\boldsymbol{F}_{q}$-linear injective map $\pi_{i}^{\prime}: \boldsymbol{F}_{q^{k}} \rightarrow \boldsymbol{F}_{q}^{n_{i}}$ by first defining the images $\pi_{i}^{\prime}\left(e_{j}^{\prime}\right)$ for $1 \leq j \leq k$, and then extending the map $\boldsymbol{F}_{q}$-linearly. For each $1 \leq j \leq k$ and $1 \leq \ell \leq k$, we want $\pi_{i}^{\prime}\left(e_{j}^{\prime}\right)$ to satisfy

$$
\begin{equation*}
\pi_{i}\left(e_{\ell}\right) \pi_{i}^{\prime}\left(e_{j}^{\prime}\right)^{\tau}=\delta_{\ell j} \tag{4}
\end{equation*}
$$

where $\tau$ denotes the transpose of a matrix and $\delta_{\ell j}$ is the Kronecker symbol. As $\ell$ runs through all values from 1 to $k$, (4) gives a linearly independent system of $k$ equations in $n_{i}$ variables. As $k \leq n_{i}$, the system admits a solution, we define as our $\pi_{i}^{\prime}\left(e_{j}^{\prime}\right)$. In general, this choice of $\pi_{i}^{\prime}\left(e_{j}^{\prime}\right)$ is not unique, but is unique up to addition by a vector in $C_{i}^{\perp}$.

It is clear that $\pi_{i}^{\prime}$ is an $\boldsymbol{F}_{q}$-linear injective map whose image $C_{i}^{\prime}$ is an $\left[n_{i}, k\right]$ linear code over $\boldsymbol{F}_{q}$. It is proved in [6] that $C_{i}^{\perp} \cap C_{i}^{\prime}=0$.

Let $C^{\perp} \subseteq \boldsymbol{F}_{q^{k}}^{s}$ be the dual code of $C$ under the ordinary inner product. This is an $[s, s-t]$ linear code over $\boldsymbol{F}_{q^{k}}$. We define $\pi_{\left(C_{1}^{\prime}, \ldots, C_{s}^{\prime}\right)}\left(C^{\perp}\right)$ to be the concatenated code defined through $C^{\perp}$ and $\pi_{1}^{\prime}, \ldots, \pi_{s}^{\prime}$, similar to the way $\pi_{\left(C_{1}, \ldots, C_{s}\right)}(C)$ was defined through $C$ and $\pi_{1}, \ldots, \pi_{s}$. This is an $\left[n_{1}+\cdots+n_{s},(s-t) k\right]$ linear code over $\boldsymbol{F}_{q}$. We know that $D \cap \pi_{\left(C_{1}^{\prime}, \ldots, C_{s}^{\prime}\right)}\left(C^{\perp}\right)=0$.

Theorem 2.1 (see [6]): The dual code $\pi_{\left(C_{1}, \ldots, C_{s}\right)}(C)^{\perp}$ of $\pi_{\left(C_{1}, \ldots, C_{s}\right)}(C)$ is the direct sum $\pi_{\left(C_{1}^{\prime}, \ldots, C_{s}^{\prime}\right)}\left(C^{\perp}\right) \oplus D$.

Corollary 2.2 (see [8], [1], [6]): Let $\left\{e_{1}, \ldots, e_{k}\right\}$ be a self-dual basis of $\boldsymbol{F}_{2^{k}}$ over $\boldsymbol{F}_{2}$ and let $C$ be a linear code over $\boldsymbol{F}_{2^{k}}$. Then the dual of the binary image of $C$ with respect to the above basis is the binary image of the dual code $C^{\perp}$ with respect to the same basis.

Proof: Note the fact that the binary image is just the concatenation of $C$ under the trivial $\pi_{\left(C_{1}, \ldots, C_{s}\right)}$, where, for each $1 \leq i \leq s$, $\pi_{i}: \boldsymbol{F}_{2^{k}} \rightarrow \boldsymbol{F}_{2}^{k}$ is the trivial map that sends each element of $\boldsymbol{F}_{2^{k}}$ to the coefficients of its binary expansion with respect to $\left\{e_{1}, \ldots, e_{k}\right\}$, thus, the conclusion follows from Theorem 2.1.

We also need the following result on the minimum distance of the dual of a concatenated code.

Lemma 2.3: Let $D$ be a code over $\boldsymbol{F}_{2 k}$ with parameters $\left[s, t, d^{\prime}\right]$ and let $\pi: \boldsymbol{F}_{2^{k}} \rightarrow \boldsymbol{F}_{2}^{n}$ be a linear map such that its image $C$ is a binary code with parameters $[n, k, d]$. Let $C^{\prime}$ be an $\left[n, k^{\prime}, d^{\prime}\right]$ binary code satisfying $C \cap C^{\prime}=0$ and let $\pi_{(C, \ldots, C)}(D)$ be the binary concatenated code defined as in (3). Then $\pi_{(C, \ldots, C)}(D) \oplus\left(C^{\prime} \oplus \cdots \oplus C^{\prime}\right)$ has minimum distance $d^{\prime}$.

Proof: For any nonzero

$$
\boldsymbol{y}=\boldsymbol{y}_{1}+\boldsymbol{y}_{2} \in \pi_{(C, \ldots, C)}(D) \oplus\left(C^{\prime} \oplus \cdots \oplus C^{\prime}\right)
$$

where $\boldsymbol{y}_{1} \in \pi_{(C, \ldots, C)}(D), \boldsymbol{y}_{2} \in C^{\prime} \oplus \cdots \oplus C^{\prime}$, it is clear that $\mathrm{wt}(\boldsymbol{y}) \geq$ $d^{\prime}$ if $\boldsymbol{y}_{1}=0$. If $\boldsymbol{y}_{1}$ is not zero, write $\boldsymbol{y}_{1}=\pi_{(C, \ldots, C)}(\boldsymbol{x})$, where $\boldsymbol{x}=$
$\left(\boldsymbol{x}_{1}, \ldots, \boldsymbol{x}_{s}\right) \in D$. Since $D$ has minimum weight $d^{\prime}$, there are $i_{1}<$ $\cdots<i_{d^{\prime}}$ such that $\boldsymbol{x}_{i_{1}}, \ldots, \boldsymbol{x}_{i_{d^{\prime}}}$ are nonzero. Since

$$
\boldsymbol{y}_{1}=\left(\ldots, \pi\left(\boldsymbol{x}_{i_{1}}\right), \ldots, \pi\left(\boldsymbol{x}_{i_{d^{\prime}}}\right), \ldots\right)
$$

with each $\pi\left(\boldsymbol{x}_{j}\right) \in C$ while each corresponding component of the second part $\boldsymbol{y}_{2}$ is in $C^{\prime}$, the assumption that $C \cap C^{\prime}=0$ shows that the components of $\boldsymbol{y}=\boldsymbol{y}_{1}+\boldsymbol{y}_{2}$ at the positions corresponding to $\boldsymbol{x}_{i_{1}}, \ldots, \boldsymbol{x}_{i_{d^{\prime}}}$ are nonzero, thus wt $(\boldsymbol{y}) \geq d^{\prime}$.

## B. The Dual of a Concatenated Code Under the Symplectic Inner Product

Let $C$ be an $[s, t]$ code over $\boldsymbol{F}_{2^{k}}$ and, for $i=1,2, \ldots, s$, let $\pi_{i}$ : $\boldsymbol{F}_{2^{k}} \rightarrow \boldsymbol{F}_{2}^{2 n_{i}}$ be an $\boldsymbol{F}_{2}$-linear injective map whose image $C_{i}=$ $\operatorname{im}\left(\pi_{i}\right)$ is a $\left[2 n_{i}, k, d_{i}\right]$ code over $\boldsymbol{F}_{2}$. The image $\pi_{\left(C_{1}, \ldots, C_{s}\right)}(C)$ of the following $\boldsymbol{F}_{2}$-linear injective map

$$
\begin{align*}
\pi_{\left(C_{1}, \ldots, C_{s}\right)}: C & \longrightarrow \boldsymbol{F}_{2}^{2 n_{1}+\cdots+2 n_{s}} \\
\left(\boldsymbol{c}_{1}, \ldots, \boldsymbol{c}_{s}\right) & \longmapsto\left(\pi_{1}\left(\boldsymbol{c}_{1}\right), \ldots, \pi_{s}\left(\boldsymbol{c}_{s}\right)\right) \tag{5}
\end{align*}
$$

is a $\left[2 n_{1}+\cdots+2 n_{s}, t k\right]$ linear (concatenated) code over $\boldsymbol{F}_{2}$.
Here $C_{i} \subseteq \boldsymbol{F}_{2}^{2 n_{i}}$ is equipped with the symplectic inner product as in (1) and let $C_{i}^{\perp \text { (s) }}$ be its dual under the symplectic inner product. Let $D^{(s)}$ be the direct sum of $C_{1}^{\perp(s)}, \ldots, C_{s}^{\perp(s)}$. This is a

$$
\left[2 n_{1}+\cdots+2 n_{s}, 2 n_{1}+\cdots+2 n_{s}-s k\right]
$$

linear code over $\boldsymbol{F}_{2}$.
We extend the notion of the weight $\mathrm{wt}_{s}$ to the concatenated code $\pi_{\left(C_{1}, \ldots, C_{s}\right)}(C)$ by

$$
\mathrm{wt}_{s}\left(\pi_{1}\left(\boldsymbol{c}_{1}\right), \ldots, \pi_{s}\left(\boldsymbol{c}_{s}\right)\right)=\mathrm{wt}_{s}\left(\pi_{1}\left(c_{1}\right)\right)+\cdots+\mathrm{wt}_{s}\left(\pi_{s}\left(\boldsymbol{c}_{s}\right)\right) .
$$

Let $\left\{e_{1}, \ldots, e_{k}\right\}$ be a basis of $\boldsymbol{F}_{2^{k}} / \boldsymbol{F}_{2}$ as above and let $\left\{e_{1}^{\prime}, \ldots, e_{k}^{\prime}\right\}$ be its dual basis. Consider the generator matrix $G_{i}$ of $C_{i}$ of size $k \times 2 n_{i}$ consisting of $k$ rows $\pi_{i}\left(e_{1}\right), \ldots, \pi_{i}\left(e_{k}\right)$. It is easy to verify that there exists a matrix (not unique) $G_{i}^{\prime}$ of size $k \times 2 n_{i}$ and rank $k$ such that $G_{i} S_{2 n_{i}} G_{i}^{\prime \tau}=I_{k}$, where $\tau$ denotes the transpose. Let $C_{i}^{\prime}$ be the $\left[2 n_{i}, k\right]$ code over $\boldsymbol{F}_{2}$ with generator matrix $G_{i}^{\prime}$. Let $\pi^{\prime}: \boldsymbol{F}_{2 k} \rightarrow \boldsymbol{F}_{2}^{2 n_{i}}$ be the $\boldsymbol{F}_{2}$-linear map that sends $e_{j}^{\prime}$ to the $j$ th row of the matrix $G_{i}^{\prime}$. As in [6], it can be proved that $C_{i}^{\prime} \cap C_{i}^{\perp(s)}=0$. In fact, if $x=r G_{i}^{\prime} \in C_{i}^{\prime} \cap C_{i}^{\perp(s)}$, where $r \in \boldsymbol{F}_{2}^{k}$ is a length- $k$ row vector. We know that $x$ is orthogonal to each row of $G_{i}$ under the symplectic inner product and thus, $G_{i} S_{2 n_{i}} G_{i}^{\prime \tau} r^{\tau}=0$. This implies $r=0$ since $G_{i} S_{2 n_{i}} G_{i}^{\prime \tau}=I_{k}$. Similarly, we can define the concatenated code $\pi_{\left(C_{1}^{\prime}, \ldots, C_{s}^{\prime}\right)}\left(C^{\perp}\right)$, where $C^{\perp}$ is the dual of $C$ under the ordinary inner product ( $\mathrm{an}[s, s-t]$ linear code over $\boldsymbol{F}_{2^{k}}$ ). This is a $\left[2 n_{1}+\cdots+2 n_{s},(s-t) k\right]$ code over $\boldsymbol{F}_{2}$. We have the following result, whose proof is similar to the proof of Theorem 2.3 in [6], so we omit it.

Theorem 2.4: Under the following symplectic inner product on $\boldsymbol{F}_{2}^{2 n_{1}+\cdots+2 n_{s}}$ :

$$
\begin{equation*}
\left\langle\left(\boldsymbol{a}_{1}, \ldots, \boldsymbol{a}_{s}\right),\left(\boldsymbol{b}_{1}, \ldots, \boldsymbol{b}_{s}\right)\right\rangle_{S}=\boldsymbol{a}_{1} S_{2 n_{1}} \boldsymbol{b}_{1}^{\tau}+\cdots+\boldsymbol{a}_{s} S_{2 n_{s}} \boldsymbol{b}_{s}^{\tau} \tag{6}
\end{equation*}
$$

where $\boldsymbol{a}_{i}, \boldsymbol{b}_{i}$ are vectors in $\boldsymbol{F}_{2}^{2 n_{i}}$ for $i=1, \ldots, s$, the dual of $\pi_{\left(C_{1}, \ldots, C_{s}\right)}(C)$ is the direct sum $\pi_{\left(C_{1}^{\prime}, \ldots, C_{s}^{\prime}\right)}\left(C^{\perp}\right) \oplus D^{(s)}$.

Remark 2.1: There is an analog of Lemma 2.3 where the minimum distance (or Hamming weight) wt is replaced by the minimum weight $\mathrm{wt}_{s}$. The proof is similar.

TABLE I

$$
\begin{aligned}
& {\left[\left[3 n, 3\left(n-m-m^{\prime}-2\right), \min \left\{m+2,\left[3\left(m^{\prime}+2\right) / 2\right\rceil\right\}\right]\right]} \\
& \text { QUANTUM Codes }
\end{aligned} \qquad \begin{array}{|c|c|}
\hline \text { Our QC's } & n, m, m^{\prime} \\
\hline[[24,9,4]] & 8,2,1 \\
\hline[[24,15,3]] & 8,1,0 \\
\hline[[21,12,3]] & 7,1,0 \\
\hline
\end{array}
$$

## III. Quantum Codes From Concatenated Algebraic-Geometric Codes

In this section, we give several constructions of quantum codes using Theorems 1.1, 1.2, and concatenated algebraic-geometric codes.

## A. Construction A

In this subsection, we present quantum codes constructed by applying Theorem 1.1 to the trivial concatenation (binary image) of alge-braic-geometric codes. We note that even in this case some best known quantum codes are obtained.

Theorem 3.1: Let $\mathcal{X} / \boldsymbol{F}_{2^{k}}(k \geq 2)$ be an algebraic curve of genus $g$ with $n^{\prime}+1 \geq 4 g \boldsymbol{F}_{2 k}$-rational points. Then for any $2 g \leq n \leq n^{\prime}-g$ and $2 g-1 \leq m^{\prime}<m \leq(n / 2)+g-1$, there exists a
$\left[\left[k n, k\left(n-m-m^{\prime}+2 g-2\right), \min \left\{m-2 g+2,\left\lceil 3\left(m^{\prime}-2 g+2\right) / 2\right\rceil\right\}\right]\right]$

## quantum code.

Proof: Take two codes $C_{m} \subset C_{m^{\prime}}$ with parameters
$[n, n-m+g-1, m-2 g+2]$ and $\left[n, n-m^{\prime}+g-1, m^{\prime}-2 g+2\right]$
respectively, as in Theorem 1.3 and Remark 1.1. Let $\left\{e_{1}, \ldots, e_{k}\right\}$ be a self-dual basis of $\boldsymbol{F}_{2^{k}} / \boldsymbol{F}_{2}$, and let $C, C^{\prime}$ be the binary images of $C_{m}$, $C_{m^{\prime}}$, respectively. Applying Theorem 1.1 to $C$ and $C^{\prime}$, the conclusion follows.

The next two results follows directly from Theorem 3.1 and Corollaries 1.4 and 1.5 .

Corollary 3.2: Suppose $k, n$ and $m, m^{\prime}$ are integers satisfying $k>$ $1,1 \leq n \leq 2^{k}$, and $0 \leq m^{\prime}<m \leq(n-2) / 2$. Then there exists a

$$
\left[\left[k n, k\left(n-m-m^{\prime}-2\right), \min \left\{m+2,\left\lceil 3\left(m^{\prime}+2\right) / 2\right\rceil\right\}\right]\right]
$$

quantum code.
Example 3.1: Let $k=3$, so $\boldsymbol{F}_{2^{k}}=\boldsymbol{F}_{8}$. In this case we have quantum codes with the parameters shown in Table I.

Comparing with [3, Table III], the above quantum codes have the same parameters as the best known ones.

Corollary 3.3: Suppose there exists an elliptic curve over $\boldsymbol{F}_{2^{k}}(k>$ 1) with $N \geq 4$ points, then there exist quantum codes with parameters

$$
\left[\left[k n, k\left(n-m-m^{\prime}\right), \min \left\{m,\left\lceil 3 m^{\prime} / 2\right\rceil\right\}\right]\right]
$$

where $2 \leq n \leq N-1$ and $1 \leq m^{\prime}<m \leq n / 2$.
Example 3.2: Let $k=3$, so $\boldsymbol{F}_{2^{k}}=\boldsymbol{F}_{8}$. There exists an elliptic curve with $N=14 \boldsymbol{F}_{8}$-rational points ([15]). In this case we have quantum codes with parameters shown in Table II.

We note that these quantum codes are not as good as the quantum twisted codes constructed in [2].

TABLE II

$$
\begin{gathered}
{\left[\left[3 n, 3\left(n-m-m^{\prime}\right), \min \left\{m,\left\lceil 3 m^{\prime} / 2\right\rceil\right\}\right]\right]} \\
\text { QUANTUM CODES } \\
\qquad \begin{array}{|c|c|}
\hline \text { Our QC's } & n, m, m^{\prime} \\
\hline[[39,9,6]] & 13,6,4 \\
\hline[[39,15,5]] & 13,5,3 \\
\hline[[39,18,4]] & 13,4,3 \\
\hline[[36,12,5]] & 12,5,3 \\
\hline[[36,21,3]] & 12,3,2 \\
\hline
\end{array}
\end{gathered}
$$

## B. Construction B

Theorem 3.4: Let $C$ be an $[n, k]$ self-orthogonal binary code with its dual $C^{\perp}$ an $\left[n, n-k, d^{\perp}\right]$ code, let $\mathcal{X} / \boldsymbol{F}_{2^{k}}$ be an algebraic curve of genus $g$ with $n^{\prime} \boldsymbol{F}_{2^{k}}$-rational points, and let $m^{\prime}$ be the smallest integer such that $3\left(m^{\prime}-2 g+2\right) / 2 \geq d^{\perp}$. Then for any $d^{\perp}+2 g-1 \leq N \leq$ $n^{\prime}-1$, there exists a

$$
\left[\left[n N, n N-k\left(m^{\prime}+d^{\perp}\right), d^{\perp}\right]\right]
$$

quantum code.
Proof: For $2 g-2<m<N$, let $D_{m}$ denote a functional al-gebraic-geometric code of parameters $[N, m-g+1]$ over $\boldsymbol{F}_{2 k}$, constructed using $\mathcal{X}$ and a divisor $G$ of degree $m$ supported at one rational point (evaluated at other rational points), in such a way that $D_{\ell} \subseteq D_{m}$ whenever $\ell \leq m$. The concatenated code $\pi_{(C, \ldots, C)}\left(D_{m}\right)$ (as in Section II-A) is an $[n N, k(m-g+1)]$ binary code. From Theorem 2.1, its dual is

$$
\left(\pi_{(C, \ldots, C)}\left(D_{m}\right)\right)^{\perp}=\pi_{\left(C^{\prime}, \ldots, C^{\prime}\right)}\left(D_{m}^{\perp}\right) \oplus\left(C^{\perp} \oplus \cdots \oplus C^{\perp}\right)
$$

where $C^{\prime}$ is as described in Section II-A and there are $N$ copies of $C^{\perp}$ in the direct sum. It is clear that

$$
\pi_{(C, \ldots, C)}\left(D_{m}\right) \subseteq C \oplus \cdots \oplus C \subseteq C^{\perp} \oplus \cdots \oplus C^{\perp}
$$

Hence, $\pi_{(C, \ldots, C)}\left(D_{m}\right)$ is self-orthogonal. Its dual is an $[n N, n N-$ $k(m-g+1)$ ] binary code.

Set $m_{1}=d^{\perp}+2 g-2$ and consider the dual code

$$
\pi_{\left(C^{\prime}, \ldots, C^{\prime}\right)}\left(D_{m_{1}}^{\perp}\right) \oplus\left(C^{\perp} \oplus \cdots \oplus C^{\perp}\right)
$$

of $\pi_{(C, \ldots, C)}\left(D_{m_{1}}\right)$. It follows from Lemma 2.3 and the fact that $D_{m_{1}}^{\perp}$ has minimum distance at least $m_{1}-2 g+2=d^{\perp}$ (see [14]) that $\left(\pi_{(C, \ldots, C)}\left(D_{m_{1}}\right)\right)^{\perp}$ has minimum distance $d^{\perp}$.

Let $t$ be the minimum weight of the $\left[n N, n N-k\left(m^{\prime}-g+1\right)\right]$ binary code

$$
\left(\pi_{(C, \ldots, C)}\left(D_{m^{\prime}}\right)\right)^{\perp}=\pi_{\left(C^{\prime}, \ldots, C^{\prime}\right)}\left(D_{m^{\prime}}^{\perp}\right) \oplus\left(C^{\perp} \oplus \cdots \oplus C^{\perp}\right)
$$

An argument similar to that in the proof of Lemma 2.3 shows that $3 t / 2 \geq d^{\perp}$.

Applying Steane's enlargement of the CSS codes (Theorem 1.1) to $\left(\pi_{(C, \ldots, C)}\left(D_{m_{1}}\right)\right)^{\perp}$ and its enlargement $\left(\pi_{(C, \ldots, C)}\left(D_{m^{\prime}}\right)\right)^{\perp}$, the conclusion follows.

We can apply Theorem 3.4 to genus 0 and 1 curves and thus have the following results.

Corollary 3.5: Let $C$ be an $[n, k]$ self-orthogonal binary code with its dual $C^{\perp}$ an $\left[n, n-k, d^{\perp}\right]$ code. Let $m^{\prime}$ be the smallest integer such

TABLE III
[[7N, $7 N-9,3]]$ QUANTUM CODES

| Our QC's | Previously known |
| :---: | :---: |
| $[[21,12,3]]$ | $[[21,12,3]]$ |
| $[[28,19,3]]$ | $[[28,19,3]]$ |
| $[[35,26,3]]$ | $[[32,25,3]]$ |
| $[[42,33,3]]$ | $[[46,32,3]]$ |
| $[[49,40,3]]$ | $[[52,42,3]]$ |
| $[[56,47,3]]$ | $[[52,42,3]]$ |

that $\left\lfloor 3\left(m^{\prime}+2\right) / 2\right\rfloor \geq d^{\perp}$. Then for each $N$ satisfying $d^{\perp}-1 \leq N \leq$ $2^{k}$, there exists an $\left[\left[n N, n N-k\left(m^{\prime}+d^{\perp}\right), d^{\perp}\right]\right]$ quantum code.

Corollary 3.6: Let $C$ be an $[n, k]$ self-orthogonal binary code with its dual $C^{\perp}$ an $\left[n, n-k, d^{\perp}\right]$ code and let $m^{\prime}$ be the smallest integer such that $\left\lfloor 3 m^{\prime} / 2\right\rfloor \geq d^{\perp}$. Suppose there exists an elliptic curve $\mathcal{X} / \boldsymbol{F}_{2^{k}}$ with $n^{\prime} \boldsymbol{F}_{2^{k}}$-rational points. Then for each $N$ satisfying $d^{\perp}+$ $1 \leq N \leq n^{\prime}-1$, there exists an $\left[\left[n N, n N-k\left(m^{\prime}+d^{\perp}\right), d^{\perp}\right]\right]$ quantum code.

Example 3.3: Let $C$ be the [7,3] binary code with the following generator matrix:

$$
\left(\begin{array}{lllllll}
1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 1
\end{array}\right)
$$

It is clear that $C$ is a self-orthogonal code with its dual $C^{\perp} \mathrm{a}[7,4,3]$ code. Thus, we have $d^{\perp}=3$ and $m^{\prime}=0$ in Corollary 3.5. From Corollary 3.5 , [[ $7 N, 7 N-9,3]$ ] quantum codes with $2 \leq N \leq 8$ can be constructed (see Table III).

Remark 3.1: Quantum codes with parameters [[21, 12, 3]], $[[28,19,3]]$ are found in [3, Table III]. From loc. cit., the upper bound of $d$ in these cases is 4 . In Table III, the other entries of previously known codes, among which [[32, 25, 3]] is an optimal one, are from [13]. It is clear that our quantum code of parameters [[42, 33, 3]] is better than the previously known [[46,32,3]] quantum code. Other quantum codes in this new family are good when compared with previously known quantum codes.

Example 3.4: Let $C$ be the [7,3] binary code as in Example 3.3. Since there exists an elliptic curve $\mathcal{X} / \boldsymbol{F}_{8}$ with 14 rational points ([15]), we can take $n^{\prime}=14, d^{\perp}=3$, and $m^{\prime}=2$ in Corollary 3.6. Thus, quantum codes of parameters $[[7 N, 7 N-15,3]]$ with $4 \leq N \leq 13$ can be constructed.

Example 3.5: Let $C$ be the [8, 4, 4] binary Hamming code with the following generator matrix:

$$
\left(\begin{array}{llllllll}
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0
\end{array}\right)
$$

It is clear that $C=C^{\perp}$, i.e., $C$ is a self-dual code. Thus, we have $d^{\perp}=4$. From Theorem 3.4, with $\mathcal{X}$ the projective line over $\boldsymbol{F}_{16}$, we have $m^{\prime}=1$ and hence $[[8 N, 8 N-20,4]]$ quantum codes with $3 \leq$ $N \leq 16$ are constructed. We note that the $[[72,52,4]]$ quantum code in our family is much better than Steane's [[74, 45, 4]] in [13]. When the length of the quantum code is $2^{m}$, there is a family of quantum codes with parameters [[ $\left.2^{m}, 2^{m}-2 m-1,4\right]$ ] from [7, Theorem 3]. For these special lengths, the quantum codes from [7] are better than ours for $n=$

64,128 . The quantum $[[88,68,4]],[[128,108,4]]$ codes when $n=$ 11,16 are not as good as the quantum $[[85,69,4]]$ code constructed in [3] and the quantum [[128, 112, 4]] code constructed in [2].

Example 3.6: Let $C=C^{\perp}$ be the $[32,16,8]$ self-dual binary code as in [9]. Then from Corollary 3.5, we have [[32N, $32 N-192,8]$ ] quantum codes for $7 \leq N \leq 2^{16}$. Our quantum codes with parameters $\left[\left[2^{19}, 2^{19}-192,8\right]\right],\left[\left[2^{20}, 2^{20}-192,8\right]\right],\left[\left[2^{21}, 2^{21}-192,8\right]\right]$ are not as good as the quantum BCH codes of parameters [[ $\left.\left.2^{r}, 2^{r}-5 r-2,8\right]\right]$ with $r>4$ constructed in [13].

Remark 3.2: As in Example 3.5, we can obtain quantum codes of parameters $[[8 N, 8 N-28,4]]$, for $5 \leq N \leq 24$, when the maximal elliptic curve $\mathcal{X} / \boldsymbol{F}_{16}$ (see [15]) is used in Corollary 3.6. We can even use curves of higher genus in Theorem 3.4. The advantage is more choices for the length and dimension of the quantum codes, although the minimum distance is generally not good.

## C. Construction C

Let $n>1$. Suppose that $A$ is a binary $n \times n$ matrix such that $A=A^{\tau}$ and $I_{n}+A$ is nonsingular. We consider the binary $[2 n, n]$ code $C$ with generator matrix $\left(I_{n}, A\right)$. It is clear that its dual $C^{\perp}$ is the binary code with generator matrix $\left(A, I_{n}\right)$. Thus, $C$ and $C^{\perp}$ have the same minimum distance $d=d^{\perp}$.

Now let $\left\{e_{1}, \ldots, e_{n}\right\}$ be a self-dual basis of $\boldsymbol{F}_{2^{n}} / \boldsymbol{F}_{2}$. Since $I_{n}+A$ is nonsingular, the $n$ rows of the matrix $\left(I_{n}+A\right)^{-1}\left(I_{n}, A\right)$ are linearly independent vectors in $C$. We define $\pi: \boldsymbol{F}_{2^{n}} \rightarrow \boldsymbol{F}_{2}^{2 n}$ by sending $e_{i}$ to the $i$ th row of this latter matrix, so the image of $\pi$ is $C$. Thus, for any code $T$ over $\boldsymbol{F}_{2^{n}}$, we obtain the concatenated code $\pi_{(C, \ldots, C)}(T)$.

On the other hand, we have

$$
\left(I_{n}+A\right)^{-1}\left(I_{n}, A\right)\left(I_{n}, A\right)^{\tau}\left(I_{n}+A\right)^{-1}=I_{n}
$$

thus, $\pi\left(e_{i}\right) \pi\left(e_{j}\right)^{\tau}=\delta_{i j}$. In the notation of Section II-A, we may take $\pi_{i}^{\prime}$ to be $\pi$ and $C_{i}^{\prime}$ to be $C$. Therefore, the dual $\left(\pi_{(C, \ldots, C)}(T)\right)^{\perp}$ of $\pi_{(C, \ldots, C)}(T)$ is

$$
\pi_{(C, \ldots, C)}\left(T^{\perp}\right) \oplus\left(C^{\perp} \oplus \cdots \oplus C^{\perp}\right)
$$

In the case where $T$ is a self-orthogonal code over $\boldsymbol{F}_{2^{n}}, \pi_{(C, \ldots, C)}(T)$ is a self-orthogonal binary code.

Theorem 3.7: Let $C, C^{\perp}$ be as above, let $\mathcal{X} / \boldsymbol{F}_{2^{n}}$ be an algebraic curve of genus $g$ with $n^{\prime}+1 \geq 4 g \boldsymbol{F}_{2 n}$-rational points and let $m^{\prime}$ be the smallest integer such that $\left\lceil 3\left(m^{\prime}-2 g+2\right) / 2\right\rceil \geq d$. Then for $2(d+g-1) \leq N \leq n^{\prime}-g$, there exist $\left[\left[2 n N, 2 n N-n\left(d+m^{\prime}\right), d\right]\right]$ quantum codes.

Proof: As in Theorem 1.3, take $D_{m_{1}}$ to be the (equivalent) al-gebraic-geometric code over $\boldsymbol{F}_{2^{n}}$ with parameters [ $\left.N, m_{1}-g+1\right]$ satisfying $D_{m_{1}} \subseteq D_{m_{1}}^{\perp}$ (i.e., $D_{m_{1}}=C_{m_{1}}^{\perp}$ ), where

$$
2\left(m_{1}-g+1\right) \leq N \leq n^{\prime}-g .
$$

For our purpose, we take $m_{1}=d+2 g-2$, thus, $\pi_{(C, \ldots, C)}\left(D_{m_{1}}\right)$ is a self-orthogonal binary code with dual

$$
\left(\pi_{(C, \ldots, C)}\left(D_{m_{1}}\right)\right)^{\perp}=\pi_{(C, \ldots, C)}\left(D_{m_{1}}^{\perp}\right) \oplus\left(C^{\perp} \cdots \oplus C^{\perp}\right)
$$

a $[2 n N, 2 n N-n(d+g-1), d]$ binary code (cf. Lemma 2.3). With $m^{\prime}$ as in the statement of the theorem, $D_{m^{\prime}}$ may be chosen in such a way that $\pi_{(C, \ldots, C)}\left(D_{m^{\prime}}^{\perp}\right) \oplus\left(C^{\perp} \oplus \cdots \oplus C^{\perp}\right)$, with parameters $\left[2 n N, 2 n N-n\left(m^{\prime}-g+1\right), m^{\prime}-2 g+2\right]$, is an enlargement of $\left(\pi_{(C, \ldots, C)}\left(D_{m_{1}}\right)\right)^{\perp}$. Applying Steane's enlargement of the CSS codes

TABLE IV
[[8N, $8 N-12,3]]$ QUANTUM CODES

| Our QC's | Previously known |
| :---: | :---: |
| $[[48,36,3]]$ | $[[46,32,3]]$ |
| $[[72,60,3]]$ | $[[74,63,3]]$ |
| $[[96,84,3]]$ | $[[94,82,3]]$ |
| $[[104,92,3]]$ | $[[106,92,3]]$ |
| $[[112,100,3]]$ | $[[118,104,3]]$ |

(Theorem 1.1) to this pair of codes, we obtain a $[[2 n N, 2 n N-n(d+$ $m^{\prime}$ ), d]] quantum code.

The following two results are immediate consequences of Theorem 3.7 when $\mathcal{X} / \boldsymbol{F}_{2^{n}}$ is taken to be the projective line or an elliptic curve.

Corollary 3.8: Let $C, C^{\perp}$ be as above and let $m^{\prime}$ be the smallest integer such that $\left\lceil 3\left(m^{\prime}+2\right) / 2\right\rceil \geq d$. Then for $2(d-1) \leq N \leq 2^{n}$, $\left[\left[2 n N, 2 n N-n\left(d+m^{\prime}\right), d\right]\right]$ quantum codes exist.

Corollary 3.9: Let $C, C^{\perp}$ be as above, let $\mathcal{X} / \boldsymbol{F}_{2 n}$ be an elliptic curve with $n^{\prime} \geq 4 \boldsymbol{F}_{2 n}$-rational points and let $m^{\prime}$ be the smallest integer such that $\left\lceil 3 m^{\prime} / 2\right\rceil \geq d$. Then, for $2 d \leq N \leq n^{\prime}-2$, $\left[\left[2 n N, 2 n N-n\left(d+m^{\prime}\right), d\right]\right]$ quantum codes exist.

Example 3.7: We take $A$ to be the following binary matrix:

$$
\left(\begin{array}{llll}
0 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1
\end{array}\right)
$$

Then $C$ and $C^{\perp}$ are $[8,4,3]$ codes and we have $[[8 N, 8 N-12,3]]$ quantum codes, for $4 \leq N \leq 16$, from Corollary 3.8. We compare our quantum codes with some of the best previously known quantum codes in Table IV. All the previously known codes there are taken from [13]. Our quantum code with parameters [[104, 92, 3]] is better than Steane's [[106, 92, 3]]. Other examples are also good when compared with the best previously known quantum codes.

Example 3.8: Let $C, C^{\perp}$ be $[8,4,3]$ binary codes as in Example 3.7. Over $\boldsymbol{F}_{16}$, there exists an elliptic curve with 25 rational points (see [15]). Thus, from Corollary 3.9, we have quantum codes with parameters $[[8 N, 8 N-20,3]]$ codes with $6 \leq N \leq 23$.

## D. Construction D

Let $C$ be a $[2 n, k]$ binary code. Suppose that its dual $C^{\perp(s)}$ under the symplectic inner product (1) is a $\left[2 n, 2 n-k, d^{\perp}\right]$ code, where $d^{\perp}$ is the minimum weight $\mathrm{wt}_{s}$ as in Section I. Suppose that $C \subseteq C^{\perp(s)}$.

Theorem 3.10: Let $C, C^{\perp(s)}$ be as above and let $\mathcal{X} / \boldsymbol{F}_{2 k}$ be an algebraic curve of genus $g$ with $n^{\prime} \boldsymbol{F}_{2^{k}}$-rational points. Then for any $d^{\perp}+2 g-1 \leq N \leq n^{\prime}$, there exists an $\left[\left[n N, n N-k\left(d^{\perp}+g-1\right), d^{\perp}\right]\right]$ quantum code.

Proof: Take $D$ to be the algebraic-geometric code (over $\boldsymbol{F}_{2^{k}}$ ) of parameters $\left[N, d^{\perp}+g-1\right]$ (the degree of the divisor is $d^{\perp}+2 g-2$ ). We now consider the concatenated code $\pi_{(C, \ldots, C)}(D)$. From Theorem 2.4, its dual $\left(\pi_{(C, \ldots, C)}(D)\right)^{\perp(s)}$ under the symplectic inner product (6) is

$$
\pi_{\left(C^{\prime}, \ldots, C^{\prime}\right)}\left(D^{\perp}\right) \oplus\left(C^{\perp(s)} \oplus \cdots \oplus C^{\perp(s)}\right)
$$

Since

$$
\pi_{(C, \ldots, C)}(D) \subseteq C \oplus \cdots \oplus C \subseteq C^{\perp(s)} \oplus \cdots \oplus C^{\perp(s)}
$$

TABLE V
[[8N, $8 N-10,3]]$ QUANTUM CODES

| Our QC's | Previously known |
| :---: | :---: |
| $[[72,62,3]]$ | $[[74,63,3]]$ |
| $[[88,78,3]]$ | $[[90,77,3]]$ |
| $[[96,86,3]]$ | $[[94,82,3]]$ |
| $[[104,94,3]]$ | $[[106,92,3]]$ |
| $[[256,246,3]]$ | $[[256,246,3]]$ |
| $[[264,254,3]]$ | $[[256,246,3]]$ |

the code $\pi_{(C, \ldots, C)}(D)$ is self-orthogonal under the symplectic inner product (6). We note further that the code

$$
\pi_{\left(C^{\prime}, \ldots, C^{\prime}\right)}\left(D^{\perp}\right) \oplus\left(C^{\perp(s)} \oplus \cdots \oplus C^{\perp(s)}\right)
$$

has minimum weight wt ${ }_{s}$ at least $d^{\perp}$. The proof is similar to that for Lemma 2.3, using the observation that the minimum weight $\mathrm{wt}_{s}$ of $\pi_{\left(C^{\prime}, \ldots, C^{\prime}\right)}\left(D^{\perp}\right)$ is at least $d^{\perp}$ (this follows from the definitions of $\mathrm{wt}_{s}$ and the concatenation). Applying Theorem 1.2 to $\pi_{(C, \ldots, C)}(D)$, the conclusion now follows.

The following two results are direct consequences of applying Theorem 3.10 to the projective line or an elliptic curve.

Corollary 3.11: Let $C, C^{\perp(s)}$ be as above. Then for any $d^{\perp}-1 \leq$ $N \leq 2^{k}+1$, there exists an $\left[\left[n N, n N-k\left(d^{\perp}-1\right), d^{\perp}\right]\right]$ quantum code.

Corollary 3.12: Let $C, C^{\perp(s)}$ be as above and let $\mathcal{X} / \boldsymbol{F}_{2^{k}}$ be an elliptic curve with $n^{\prime} \boldsymbol{F}_{2 k}$-rational points. Then for any $d^{\perp}+1 \leq$ $N \leq n^{\prime}$, there exists an $\left[\left[n N, n N-k d^{\perp}, d^{\perp}\right]\right]$ quantum code.

Example 3.9: Let $C$ be the direct sum of two $[8,4,4]$ binary Hamming codes. Then $C$ is a $[16,8,4]$ (here 4 is the minimum weight $\mathrm{wt}_{s}$ ) self-dual code under the symplectic inner product. We have $[[8 N, 8 N-$ 24, 4]] quantum codes, for $3 \leq N \leq 257$, from Corollary 3.11. This family of quantum codes are not as good as the quantum codes of parameters $\left[\left[2^{m}, 2^{m}-2 m-1,4\right]\right]$ in [7] when the length is $2^{m}$.

Example 3.10: Let $C$ be as in Example 3.9. Over $\boldsymbol{F}_{256}$, there exists an elliptic curve with 289 rational points [15]. Thus, we have quantum codes with parameters $[[8 N, 8 N-32,4]]$ for $5 \leq N \leq 289$.

Example 3.11: Let $C$ be the binary $[16,5]$ code generated by the following binary matrix:

$$
\left(\begin{array}{llllllllllllllll}
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right) .
$$

It is easy to see that $C$ is self-orthogonal under the symplectic inner product (1) with its dual $C^{\perp(s)}$ a $[16,11,3]$ code, where 3 means the minimum weight $\mathrm{wt}_{s}$. We have $[[8 N, 8 N-10,3]]$ quantum codes, for $2 \leq N \leq 33$, from Corollary 3.11. We compare the quantum codes in this family with some previously known quantum codes in Table V. All the previously known codes in the table are from [13]. We note that the quantum code of parameters [[256, 246,3]] is an optimal code. In this table, the other quantum codes in our family are better than the corresponding previously known quantum codes.

Example 3.12: Let $C$ be as in Example 3.11. There exists an elliptic curve over $\boldsymbol{F}_{32}$ with 44 rational points ([15]). Thus, we have quantum codes with parameters [[8N, $8 N-15,3]], 4 \leq N \leq 44$.

## IV. Conclusion

We have developed some methods of constructing quantum codes from concatenated algebraic-geometric codes and calculated many examples of good quantum codes. It seems that techniques from algebraic geometry not only yield asymptotically good quantum codes as in [5], [1], [6], they also lead to some good short quantum codes.

## Note Added in Proof

After this paper was submitted, we learned of the paper "Binary construction of quantum codes of minimum distance three and four" of Li and Li (IEEE Transactions on Information Theory, vol. 50, pp. 1331-1336, June 2004), in which the preprint form of our this paper was cited and some of our constructed quantum codes were improved.

## Acknowledgment

The authors are very grateful to two referees for their criticisms and comments on the manuscript, which helped to improve the results and presentation.

## References

[1] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, "Asymptotically good quantum codes," Phys. Rev. A, vol. 63, pp. 032311-032311, 2001.
[2] J. Bierbrauer and Y. Edel, "Quantum twisted codes," J. Comb. Des., vol. 8, pp. 174-188, 2000. Also see homepages of J. Bierbrauer and Y. Edel: http//www.math.mtu.edu/~jbierbra; http//www.mathi.uni-heidelberg.de/~yves.
[3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," IEEE Trans. Inf. Theory, vol. 44, no. 4, pp. 1369-1387, Jul. 1998.
[4] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A, vol. 54, pp. 1098-1105, Aug. 1996.
[5] H. Chen, "Some good quantum error-correcting codes from algebraic geometric codes," IEEE Trans. Inf. Theory, vol. 47, no. 5, pp. 2059-2061, Jul. 2001.
[6] H. Chen, S. Ling, and C. Xing, "Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound," IEEE Trans Inf. Theory, vol. 47, no. 5, pp. 2055-2058, Jul. 2001.
[7] G. Cohen, S. Encheva, and S. Litsyn, "On binary construction of quantum codes," IEEE Trans. Inf. Theory, vol. 45, no. 7, pp. 2495-2498, Nov. 1999
[8] 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. Berlin, Germany: Springer-Verlag, 1999, vol. 1719, pp. 231-244.
[9] E. M. Rains and N. J. A. Sloane, "Self-dual codes," in Handbook of Coding Theory, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science, 1998, vol. I, pp. 177-294.
[10] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," Phys. Rev., A, vol. 52, pp. R2493-R2496, Oct. 1995.
[11] A. M. Steane, "Multiple particle interference and quantum error correction," Proc. Roy. Soc. London, A, vol. 452, pp. 2551-2577, Nov. 1996.
[12] , "Quantum Reed-Muller codes," IEEE Trans. Inf. Theory, vol. 45, no. 5, pp. 1701-1703, Jul. 1999.
[13] -, "Enlargement of Calderbank-Shor-Steane quantum codes," IEEE Trans. Inf. Theory, vol. 45, no. 7, pp. 2492-2495, Nov. 1999.
[14] M. A. Tsfasman and S. G. Vlăduţ, Algebraic-Geometric Codes. Dor-drecht-Boston-London: Kluwer Academic, 1991.
[15] G. van der Geer and M. van der Vlugt. (2001) Tables of Curves With Many Points. [Online]. Available: http://www.science.uva.nl/~geer/


[^0]:    © 2005 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at:
    [http://dx.doi.org/10.1109/TIT.2005.851760].

