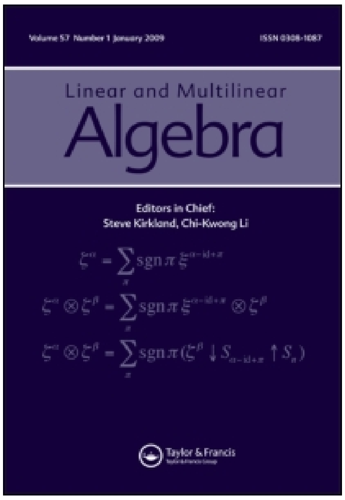

Linear and Multilinear Algebra
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t713644116

Quantum codes from Hadamard matrices

W. F. Ke[a]; K. F. Lai[a]; R. B. Zhang[b]
[a] Department of Mathematics and National Center for Theoretical Sciences, National Cheng Kung University, Tainan 701, Taiwan [b] School of Mathematics and Statistics, University of Sydney, Sydney, NSW 2006, Australia

First published on: 13 April 2010

To cite this Article Ke, W. F. , Lai, K. F. and Zhang, R. B.(2010) 'Quantum codes from Hadamard matrices', Linear and Multilinear Algebra,, First published on: 13 April 2010 (iFirst)

To link to this Article: DOI: 10.1080/03081080903062121

URL: http://dx.doi.org/10.1080/03081080903062121

Linear and Multilinear Algebra
2010, 1–8, iFirst

Taylor & Francis
Taylor & Francis Group

Quantum codes from Hadamard matrices

W.F. Ke[a], K.F. Lai[a*] and R.B. Zhang[b]

[a]*Department of Mathematics and National Center for Theoretical Sciences, National Cheng Kung University, Tainan 701, Taiwan;* [b]*School of Mathematics and Statistics, University of Sydney, Sydney, NSW 2006, Australia*

Communicated by M. Chebotar

(*Received 29 April 2009; final version received 21 May 2009*)

From each $q \times q$ unitary matrix Φ, we construct a family of quantum codes $\mathscr{C}_t(\Phi)$, $t \geq 1$, for q-state systems which encode $(2t+1)^2$ q-states into one q-state. We show that such codes are capable of correcting the errors of weight up to t if and only if Φ is a complex Hadamard matrix.

Keywords: complex Hadamard matrix; quantum code

1. Introduction

Since Shor's discovery of the 9-qubit code [13] which is capable of correcting single-qubit errors in quantum communication, much research has been done on quantum error correcting codes. Although most of the efforts are concentrated on binary codes, non-binary codes also attract more interest, both for applications and for further theoretical developments. Ashikhmin and Knill [1], Matsumoto and Uyematsu [9] and Parthasarathy [11] constructed quantum codes for p^{m}-state systems (p a prime), while Bierbrauer and Edel [3] developed constructions using twisted BCH-codes.

In this article, we construct quantum codes for q-state systems using $q \times q$ unitary matrices. The idea came from the construction of Shor's 9-qubit code.

In his original construction, Shor used the repetition of the states $|v_1\rangle = \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$ and $|v_2\rangle = \frac{1}{\sqrt{2}}|000\rangle - \frac{1}{\sqrt{2}}|111\rangle$ in $(\mathbb{C}^2)^{\otimes 3}$ to correct the single qubit errors introduced by the environment. Observe that the transition matrix between the set of vectors $\{|000\rangle, |111\rangle\}$ and $\{|v_1\rangle, |v_2\rangle\}$ is the unitary matrix $\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix}$, which is usually referred to as a Walsh–Hadamard matrix.

A natural way of generalizing the idea is to use unitary matrices coupled with repetitions to construct q-state quantum codes. Take a $q \times q$ unitary matrix $\Phi = (\varphi_{ij})$ with $q \geq 2$. For $t \geq 1$, consider the vector space $\mathscr{C}_t(\Phi)$ generated by the states $\underbrace{|\Phi_i^{(t)}\rangle \otimes |\Phi_i^{(t)}\rangle \otimes \cdots |\Phi_i^{(t)}\rangle}_{2t+1}$, $1 \leq i \leq q$, where each $|\Phi_i^{(t)}\rangle = \sum_{j=1}^{q} \varphi_{ji} |\underbrace{ii \cdots i}_{2t+1}\rangle \in (\mathbb{C}^q)^{\otimes 2t+1}$. Can this code do what we are hoping it will do, namely, correct quantum errors, and

*Corresponding author. Email: kinglai@mail.ncku.edu.tw

ISSN 0308–1087 print/ISSN 1563–5139 online

DOI: 10.1080/03081080903062121
http://www.informaworld.com

if so, how good is it? We will see that, in Theorem 2.2, the code $\mathscr{C}_t(\Phi)$ can correct quantum errors if and only if Φ satisfies

$$\|\varphi_{ij}\|^2 = \frac{1}{q} \quad \text{for all} \quad i, j \in \{1, \ldots, q\}. \tag{1}$$

For a quantum code $\mathscr{C}$ with an orthonormal basis $\{|1\rangle, \ldots, |k\rangle\}$, the distance d of $\mathscr{C}$ is defined to be the minimum weight of the error operators E such that

$$\langle i|E|j\rangle \neq c_E \delta_{ij} \tag{2}$$

for some $|i\rangle$ and $|j\rangle$, where $c_E \in \mathbb{C}$ is a constant (cf. [12, Section 7.3.1]). We say that a quantum code for a q-state system with length n, k encoded q-states and distance d is an $[[n, k, d]]_q$ quantum code. Such a code can correct an error of weight $\leq \frac{1}{2}(d-1)$. In our case, $\mathscr{C}_t(\Phi)$ is an $[[m^2, 1, m]]_q$ quantum error correcting code.

Note that unitary matrices satisfying condition (1) exist in abundance. Recall that a $q \times q$ matrix H is called a (complex) Hadamard matrix if the entries of H are the roots of unity and $H^\dagger H = qI_q$, where I_q is the $q \times q$ identity matrix and $H^\dagger$ denotes the Hermitian conjugate of H [15]. Hadamard matrices which appear in combinatorial design theory have entries of either 1 or -1, and are called real Hadamard matrices. In the real case, it is known that q is either 2 or is divisible by 4 [14, Theorem 2.2.3]. But in general, i.e. when the roots of unity other than ± 1 are allowed, q can be any integer ≥ 2. Now, if H is a Hadamard matrix, then $\Phi = \frac{1}{\sqrt{q}} H$ is a unitary matrix satisfying condition (1), which can be used to construct a series of quantum error correcting codes. Shor's construction comes about naturally within this framework.

Shor's 9-qubit code can also be described by using stabilizer codes [4]. However, our construction does not yield stabilizer codes in general (Remark 3.1(2)). The proof of Theorem 2.2 gives another insight to how these codes work.

In the next section, we set up the notation, describe our code and state our main theorem. We first prove the case of weight $t = 1$, and the general construction then follows.

We note that for any $q \geq 2$, $q \times q$ unitary matrices satisfying condition (1) are abundant. In fact, for $q \geq 2$, let $\omega = e^{2\pi i/q}$, and set $\varphi_{st} = \frac{\omega^{st}}{\sqrt{q}}$ for $s, t \in \{1, 2, \ldots, q\}$. Then $\Phi = (\varphi_{st})$ is a unitary matrix satisfying the condition (1). Such matrices are often referred to as Fourier matrices, and are used in discrete Fourier transform.

Finally, complex Hadamard matrices have been used in quantum information to construct nice error bases, to study mutually unbiased bases, in solving Mean King Problems or to construct quantum designs (cf. [2,5–7]). Beside Fourier matrices, there are many other complex Hadamard matrices. A nice catalogue of them with a good pointer to various references can be found in [17].

2. The machine

Start with the vector space $\mathbb{C}^q$ over the complex numbers $\mathbb{C}$ of dimension $q \geq 2$. For any integer $t \geq 1$ we introduce tensor spaces $\mathscr{V} = (\mathbb{C}^q)^{\otimes(2t+1)}$ (i.e. the tensor product of $\mathbb{C}^q$ with itself $2t+1$ times) and $\mathscr{H} = \mathscr{V}^{\otimes(2t+1)}$.

Let $\{|1\rangle, |2\rangle, \ldots, |q\rangle\}$ be an orthonormal basis of $\mathbb{C}^q$ with respect to the usual Hermitian inner product. Thus $\langle i|j\rangle = \delta_{ij}$. The tensor product of the vector $|i\rangle$ with itself $2t$+1 times will be denoted by $|i^{(t)}\rangle$.

To a given $q \times q$ complex matrix $\Phi = (\varphi_{ij})$, we associate the following vectors in $\mathscr{V}$:

$$|\Phi_j^{(t)}\rangle = \sum_{i=1}^{q} \varphi_{ij} |i^{(t)}\rangle, \quad j = 1, 2, \ldots, q. \tag{3}$$

Then we take tensor product to get the vector

$$|\underbrace{\Phi_j^{(t)}\Phi_j^{(t)}\cdots\Phi_j^{(t)}}_{2t+1}\rangle = \underbrace{|\Phi_j^{(t)}\rangle \otimes |\Phi_j^{(t)}\rangle \otimes \cdots \otimes |\Phi_j^{(t)}\rangle}_{2t+1}$$

in $\mathscr{H}$. Finally, set

$$\mathscr{C}_t(\Phi) := \bigoplus_{j=1}^{q} \mathbb{C}|\underbrace{\Phi_j^{(t)}\Phi_j^{(t)}\cdots\Phi_j^{(t)}}_{2t+1}\rangle. \tag{4}$$

This subspace $\mathscr{C}_t(\Phi)$ of $\mathscr{H}$ will be our code.

Definition 2.1 By a $q \times q$ *generalized Hadamard matrix* we mean a unitary matrix $\Phi = (\varphi_{ij})$ satisfying condition (1).

Let $\mathfrak{T}$ denote the set of operators on $\mathscr{H}$ of the form $U_1 \otimes U_2 \otimes \cdots \otimes U_{(2t+1)^2}$, where all the $q \times q$ matrices U_j are the identity matrix except for at most t of them. Let $\mathfrak{E}$ be the subspace of the algebra End($\mathscr{H}$) of linear operators on $\mathscr{H}$ spanned by $\mathfrak{T}$. Therefore, $\mathfrak{E}$ consists of all possible error operators of weight at most t in End($\mathscr{H}$).

We can now state our theorem.

THEOREM 2.2 *The q-dimensional subspace $\mathscr{C}_t(\Phi)$ of $\mathscr{H}$ is a quantum code, which can correct all the errors of weights up to t given in $\mathfrak{E}$ if and only if Φ is a generalized Hadamard matrix.*

3. The proof

Let H be a finite-dimensional Hilbert space over the complex numbers. If C is a subspace of H, we write P_C for the projection operator from H to C. Let $\mathscr{E}$ be a subspace of the algebra End(H) of endomorphisms on H. According to Knill–Laflamme ([8, Theorem III.2], [10, Theorem 10.1], [4, Section 3, Theorem 3]), the subspace C of H is a quantum error correcting code capable of correcting the errors in $\mathscr{E}$ if and only if for any E and F in $\mathscr{E}$ there exists a complex number $c(E, F)$ such that

$$P_C E F^{\dagger} P_C = c(E, F) P_C. \tag{5}$$

Here $F^{\dagger}$ denotes the adjoint of F defined with respect to the inner product of the Hilbert space H.

Thus, Theorem 2.2 is equivalent to the statement that the condition (5) is satisfied if and only if the condition (1) holds.

To make our arguments easier, we shall first prove the case of $t = 1$ before we tackle the general case.

3.1. *Weight 1 case*

In this section $t=1$. $\mathscr{V}$ is now the vector space $(\mathbb{C}^q)^{\otimes 3}$ and $\mathscr{H}=(\mathbb{C}^q)^{\otimes 3}\otimes(\mathbb{C}^q)^{\otimes 3}\otimes(\mathbb{C}^q)^{\otimes 3}$. These vector spaces are equipped with natural Hermitian inner products.

Let $\Phi=(\varphi_{ij})$ be a $q\times q$ unitary matrix, that is, Φ satisfies $\Phi^\dagger\Phi=I_q$, where I_q is the identity matrix and $\Phi^\dagger$ is the Hermitian conjugate of Φ in the complex algebra $\mathrm{End}(\mathbb{C}^q)$ of endomorphisms on $\mathbb{C}^q$. We put $|\Phi_i\rangle=\sum_{j=1}^q \varphi_{ji}|jjj\rangle\in(\mathbb{C}^q)^{\otimes 3}$ for $i=1,2,\dots,q$. Then $\langle\Phi_i|\Phi_j\rangle=\delta_{ij}$ for all i and j and so $\{|\Phi_i\rangle, 1\le i\le q\}$ forms another orthonormal basis of the subspace $\oplus_{i=1}^q\mathbb{C}|iii\rangle$ of $\mathscr{V}$. Our code space determined by Φ is now the following q-dimensional subspace of $\mathscr{H}$:

$$\mathscr{C}_t(\Phi)=\oplus_{i=1}^q\mathbb{C}|\Phi_i\rangle\otimes|\Phi_i\rangle\otimes|\Phi_i\rangle.$$

Let $P:\mathscr{H}\to\mathscr{C}_t(\Phi)$ be the projection operator. Then P can be expressed as

$$\begin{aligned}P&=\sum_{i=1}^q|\Phi_i\Phi_i\Phi_i\rangle\langle\Phi_i\Phi_i\Phi_i|\\&=\sum_{i=1}^q|\Phi_i\rangle\langle\Phi_i|\otimes|\Phi_i\rangle\langle\Phi_i|\otimes|\Phi_i\rangle\langle\Phi_i|.\end{aligned}$$

Let $\mathfrak{T}$ denote the set of operators on $\mathscr{H}$ of the form

$$X^{(\alpha)}=1^{\otimes(\alpha-1)}\otimes X\otimes 1^{\otimes(9-\alpha)}, \tag{6}$$

where $\alpha=1,2,\dots,9$ and $X\in\mathrm{End}(\mathbb{C}^q)$. The error space $\mathfrak{E}$ is the vector space spanned by $\mathfrak{T}$. Then

$$\mathfrak{E}\cong\underbrace{\mathrm{End}(\mathbb{C}^q)\oplus\mathrm{End}(\mathbb{C}^q)\oplus\cdots\oplus\mathrm{End}(\mathbb{C}^q)}_{9}. \tag{7}$$

3.1.1. *Proof of Theorem 2.2 in the case t = 1*

Let E_{ij} stand for the $q\times q$ matrix unit having 1 at the (i,j) position and 0 elsewhere. In order to prove the theorem, it suffices to consider the error operators of the form (in the notation of Equation (6))

$$E=E_{ij}^{(\alpha)},\quad F=E_{kl}^{(\beta)}$$

for $\alpha,\beta\in\{1,2,\dots,9\}$ and $i,j,k,l\in\{1,2,\dots,q\}$. We shall write $E_{ij}^{(\alpha)}$ as a triple tensor product of operators inEnd$((\mathbb{C}^q)^{\otimes 3})$, e.g.

$$\begin{aligned}E_{ij}^{(1)}&=(E_{ij}\otimes 1\otimes 1)\otimes(1\otimes 1\otimes 1)\otimes(1\otimes 1\otimes 1),\\E_{lk}^{(4)}&=(1\otimes 1\otimes 1)\otimes(E_{lk}\otimes 1\otimes 1)\otimes(1\otimes 1\otimes 1).\end{aligned}$$

We also introduce the ceiling function $\lceil\cdot\rceil$ defined for any non-negative real number r by setting $\lceil r\rceil$ to be the smallest positive integer $\ge r$.

We remind ourselves that in the condition (5) the adjoint † means to take the conjugate linear anti-involution on $\mathrm{End}((\mathbb{C}^q)^{\otimes 9})$ defined by

$$X_1\otimes X_2\otimes\cdots\otimes X_9\mapsto X_1^\dagger\otimes X_2^\dagger\otimes\cdots\otimes X_9^\dagger,$$

where each X_i is a $q\times q$ matrix.

There are three cases to be discussed depending on the values of α and β. First, suppose that $\lceil \beta/3 \rceil \neq \lceil \alpha/3 \rceil$. We have

$$PEF^{\dagger}P = \sum_{s} \langle \Phi_s | E_{ij} \otimes 1 \otimes 1 | \Phi_s \rangle \langle \Phi_s | E_{lk} \otimes 1 \otimes 1 | \Phi_s \rangle \\ \times \big(|\Phi_s\rangle\langle\Phi_s| \otimes |\Phi_s\rangle\langle\Phi_s| \otimes |\Phi_s\rangle\langle\Phi_s| \big). \tag{8}$$

Some remarks are given below. Note that the values of $\langle \Phi_s | E_{ij} \otimes 1 \otimes 1 | \Phi_s \rangle$ and $\langle \Phi_s | E_{lk} \otimes 1 \otimes 1 | \Phi_s \rangle$ are independent of the positions of the matrix units, namely, for all i, j,

$$\langle \Phi_s | E_{ij} \otimes 1 \otimes 1 | \Phi_s \rangle = \langle \Phi_s | 1 \otimes E_{ij} \otimes 1 | \Phi_s \rangle = \langle \Phi_s | 1 \otimes 1 \otimes E_{ij} | \Phi_s \rangle.$$

We have already used this fact in deriving the formula (8) for $PEF^{\dagger}P$, and shall use it later without further explanation. Now

$$\langle \Phi_s | E_{ij} \otimes 1 \otimes 1 | \Phi_s \rangle = \delta_{ij} \overline{\varphi_{is}} \varphi_{is},$$

and using this in (8) we arrive at

$$PEF^{\dagger}P = \delta_{ij}\delta_{lk} \sum_{s} w_{s,ik} \big(|\Phi_s\rangle\langle\Phi_s| \otimes |\Phi_s\rangle\langle\Phi_s| \otimes |\Phi_s\rangle\langle\Phi_s| \big),$$

where $w_{s,ik} = \overline{\varphi_{is}}\varphi_{is}\overline{\varphi_{ks}}\varphi_{ks}$. Now $PEF^{\dagger}P$ is proportional to P if and only if $w_{s,ik}$ is s-independent. This is equivalent to the condition that there exists some positive real number ξ_i such that

$$\overline{\varphi_{is}}\varphi_{is} = \xi_i \quad \text{for all } s.$$

As Φ is a unitary matrix, we see that $\xi_i = 1/q$ for all i, that is,

$$\overline{\varphi_{is}}\varphi_{is} = \frac{1}{q}, \quad \text{for all s.} \tag{9}$$

Next, suppose that $\alpha = \beta$. Then

$$PEF^{\dagger}P = \delta_{jl}\delta_{ik} \sum_{s} \overline{\varphi_{is}}\varphi_{is} \big(|\Phi_s\rangle\langle\Phi_s| \otimes |\Phi_s\rangle\langle\Phi_s| \otimes |\Phi_s\rangle\langle\Phi_s| \big).$$

Finally, suppose that $\lceil \beta/3 \rceil = \lceil \alpha/3 \rceil$ and $\beta \neq \alpha$. We have

$$\begin{aligned} PEF^{\dagger}P &= \sum_{s} \langle \Phi_s | E_{ij} \otimes E_{lk} \otimes 1 | \Phi_s \rangle \big(|\Phi_s\rangle\langle\Phi_s| \otimes |\Phi_s\rangle\langle\Phi_s| \otimes |\Phi_s\rangle\langle\Phi_s| \big) \\ &= \delta_{ij}\delta_{kl} \sum_{s} \overline{\varphi_{is}}\varphi_{is} \big(|\Phi_s\rangle\langle\Phi_s| \otimes |\Phi_s\rangle\langle\Phi_s| \otimes |\Phi_s\rangle\langle\Phi_s| \big). \end{aligned}$$

We easily see that in both cases, the condition (9) is necessary and sufficient to render $PEF^{\dagger}P$ proportional to P. This completes the proof. ■

Remark 3.1 For any $q \times q$ matrices X and Y, we denote by E either $X \otimes Y \otimes I$, $X \otimes I \otimes Y$ or $I \otimes X \otimes Y$. Then

$$\langle iii | E | jjj \rangle = \delta_{ij} \langle i | X | j \rangle \langle i | Y | j \rangle, \quad \forall i, j.$$

We consider the vectors $|iii\rangle$ instead of $|ii\rangle$, precisely because of this property. For it may happen that $\langle ii | X \otimes Y | jj \rangle \neq 0$ even when $i \neq j$.

3.2. *Weight $t > 1$ case*

Now we take t to be an arbitrary (but fixed) positive integer, and return to the set-up of Section 2.

Proof The projection P from $\mathscr{C}_t(\Phi)$ to $\mathscr{H}$ can be expressed as

$$P = P_1 + P_2 + \cdots + P_q,$$

where

$$P_i = \underbrace{|\Phi_i^{(t)}\rangle\langle\Phi_i^{(t)}| \otimes |\Phi_i^{(t)}\rangle\langle\Phi_i^{(t)}| \otimes \cdots \otimes |\Phi_i^{(t)}\rangle\langle\Phi_i^{(t)}|}_{2t+1} \tag{10}$$

satisfies the relations $P_i\ P_j = \delta_{ij} P_i$.

First, assume that $\mathscr{C}_t(\Phi)$ can correct the errors in $\mathfrak{E}$. Then for every pair $E, F \in \mathfrak{E}$ there exists a constant $c(E,F) \in \mathbb{C}$ such that

$$PEF^\dagger P = c(E,F)P. \tag{11}$$

Consider $E = F = E_{kl}^{(1)} = \underbrace{E_{kl} \otimes 1 \otimes \cdots \otimes 1}_{2t+1} \in \mathfrak{T}$. Then $EF^\dagger = E_{kk}^{(1)}$, and so

$$PEF^\dagger P = \sum_{s,r} P_s EF^\dagger P_r = \sum_s P_s E_{kk}^{(1)} P_s.$$

For every $s = 1, 2, \ldots, q$, we have

$$P_s E_{kk}^{(1)} P_s = \langle\Phi_s^{(t)}|E_{kk} \otimes 1 \otimes \cdots \otimes 1|\Phi_s^{(t)}\rangle P_s = \overline{\varphi_{ks}}\varphi_{ks} P_s.$$

Therefore, $\overline{\varphi_{ks}}\varphi_{ks} = c(E,F)$ for all $k, s \in \{1, 2, \ldots, q\}$. This means that $|\varphi_{ks}|^2$ is a constant for all $k, s \in \{1, 2, \ldots, q\}$. As Φ is a unitary matrix, $|\varphi_{ks}|^2 = \frac{1}{q}$ for all k and s.

Conversely, we assume that Φ is a generalized Hadamard matrix. Take arbitrary $E, F \in \mathfrak{T}$, and write

$$E = \mathbf{U}_1 \otimes \mathbf{U}_2 \otimes \cdots \otimes \mathbf{U}_{2t+1}, \quad F = \mathbf{V}_1 \otimes \mathbf{V}_2 \otimes \cdots \otimes \mathbf{V}_{2t+1},$$

where $\mathbf{U}_k, \mathbf{V}_l \in \mathrm{End}((\mathbb{C}^q)^{\otimes(2t+1)})$. We can express $EF^\dagger$ as

$$\mathbf{W}_1 \otimes \mathbf{W}_2 \otimes \cdots \otimes \mathbf{W}_{2t+1}, \tag{12}$$

where $\mathbf{W}_k = \mathbf{U}_k \mathbf{V}_k^\dagger$. It is crucial to note that at most t of the $\mathbf{U}_i$ (resp. $\mathbf{V}_j$) are not the identity operators on $(\mathbb{C}^q)^{\otimes(2t+1)}$. Therefore, at least one of the $\mathbf{W}_k$ is the identity operator on $(\mathbb{C}^q)^{\otimes(2t+1)}$. By using (10) for each P_i, we easily see that

$$PEF^\dagger P = \sum_{i,j=1}^{q} P_i EF^\dagger P_j = \sum_{i=1}^{q} P_i EF^\dagger P_i,$$

and

$$\begin{aligned} P_i EF^\dagger P_i &= \langle\Phi_i^{(t)}|\mathbf{W}_1|\Phi_i^{(t)}\rangle|\Phi_i^{(t)}\rangle\langle\Phi_i^{(t)}| \otimes \cdots \otimes \langle\Phi_i^{(t)}|\mathbf{W}_{2t+1}|\Phi_i^{(t)}\rangle|\Phi_i^{(t)}\rangle\langle\Phi_i^{(t)}| \\ &= \left(\prod_{l=1}^{2t+1} \langle\Phi_i^{(t)}|\mathbf{W}_l|\Phi_i^{(t)}\rangle\right) P_i. \end{aligned}$$

Now we observe that $\mathbf{W}_l$ can be written as $W_{11} \otimes W_{l2} \otimes \cdot \otimes W_{lm}$ with at least one of the operator W_{lj} (acting on $\mathbb{C}^q$) being the identity operator. As Φ satisfies (1), $\langle \Phi_i^{(t)} | \mathbf{W}_l | \Phi_i^{(t)} \rangle$ is independent of i, and so is also the coefficient $\prod_{l=1}^{2t+1} \langle \Phi_i^{(t)} | \mathbf{W}_l | \Phi_i^{(t)} \rangle$. Hence

$$PEF^{\dagger}P = P \prod_{l=1}^{2t+1} \langle \Phi_i^{(t)} | \mathbf{W}_l | \Phi_i^{(t)} \rangle.$$

This completes the proof. ■

Remark Note that the function $c \colon \mathfrak{E} \times \mathfrak{E} \to \mathbb{C}$ defines a sesquilinear form, namely, c is linear in the first variable and conjugate linear in the second.

4. Conclusions

We have shown that given any $q \times q$ generalized Hadamard matrix, one can construct a family of quantum codes $\mathscr{C}$ from a q-state system, which are capable of correcting arbitrary errors of weights up to t. In this construction, $q^n = \dim \mathscr{H} = q^{(2t+1)^2}$ and $q^k = \dim \mathscr{C} = q$. Suppose that $E, F \in \mathfrak{E}$ are the errors of weight $t+1$. Then, when expressed as in the form (12), it is possible that none of the $\boldsymbol{W}_k$'s is the identity operator on $(\mathbb{C}^q)^{\otimes(2t+1)}$. In this case, the arguments used in the proof of Theorem 2.2 break down. Hence the minimal distance d of the code $\mathscr{C}_t(\Phi)$ is less than $2(t+1)$. On the other hand, d is at least $2t+1$. Therefore, $d = 2t+1$ and so $\mathscr{C}$ is a $[[(2t+1)^2; 1; 2t+1]]_q$ quantum code. It is clear that we recover from the above construction the 9-qubit code of Shor [13] as a special case by using the Hadamard matrix $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Acknowledgements

W.F. Ke was partially supported by The National Science Council, Taiwan, under grants NSC-94-2115-M-006-008 and NSC-95-2115-M-006-004.

References

[1] A. Ashikhmin and E. Knill, *Nonbinary quantum stabilizer codes*, IEEE Trans. Inform. Theory 47 (2001), pp. 3065–3072.

[2] I. Bengtsson, *Three ways to look at mutually unbiased bases*, in *Foundations of Probability and Physics – 4, Proceedings of the Conference*, G. Adenier, C. Fuchs, and A.Y. Khrennikov, eds., Växjö, Sweden, 4–9 June, 2006. American Institute of Physics (AIP), Melville, NY, 2007. pp. 40–51.

[3] J. Bierbrauer and Y. Edel, *Twisted BCH-codes*, J. Combin. Des. 5 (1997), pp. 377–389.

[4] D. Gottesman, *An introduction to quantum error correction*, in *Quantum Computation: A Grand Mathematical Challenge for the Twenty-first Century and the Millennium*, S.J. Lomonaco Jr., ed., American Mathematical Society, Providence, RI, 2002, pp. 221–235.

[5] J.L. Hayden, *Generalized Hadamard matrices*, Des., Codes Cryptogr. 12 (1997), pp. 69–73.

[6] A. Klappenecker and M. Rötteler, *New Tales of the Mean King*, IEEE International Symposium on Information Theory, Adelaide, Australia, 2005.

[7] E. Knill, *Group representations, error bases and quantum codes*, Technical Report LAVR-96-2807, 1996.

[8] E. Knill and R. Laflamme, *A theory of quantum error-correcting codes*, Phys. Rev. A 55 (1997), pp. 900–911.

[9] R. Matsumoto and T. Uyematsu, *Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes*, IEICE Trans. Fundamentals E83-A (2000), pp. 1878–1883.

[10] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, UK, 2000.

[11] K.R. Parthasarathy, *An inducing construction of quantum codes from classical error correcting codes*, J. Appl. Probab. 38A (2001), pp. 27–32.

[12] J. Preskill, *Quantum computation, lecture notes*. Available at http://www.theory.caltech.edu/people/preskill/ph229/.

[13] P.W. Shor, *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev. A 52 (1995), pp. 2493–2496.

[14] V.D. Tonchev, *Combinatorial Configurations, Designs, Codes*, Longman, New York, 1988.

[15] J.S. Wallis, *Hadamard Matrices*, *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 292 (1972), pp. 273–490.

[16] R.F. Werner, *All teleportation and dense coding schemes*, J. Phys. A: Math. Gen. 34 (2001), pp. 7081–7094.

[17] K. Życzkowski and W. Tadej. *Complex Hadamard matrices, a catalogue*. Available at http://chaos.if.uj.edu.pl/˜karol/hadamard/index.php.