Proc. Indian Acad. Sci. (Math. Sci.) Vol. 114, No. 4, November 2004, pp. 365–374.

On the maximal dimension of a completely entangled subspace for finite level quantum systems

K R PARTHASARATHY

Indian Statistical Institute, Delhi Centre, 7, S.J.S. Sansanwal Marg,
New Delhi 110 016, India
E-mail: krp@isid.ac.in

MS received 19 March 2004; revised 16 August 2004

Abstract. Let $\mathcal{H}_i$ be a finite dimensional complex Hilbert space of dimension d_i associated with a finite level quantum system A_i for $i = 1, 2, \ldots, k$. A subspace $S \subset \mathcal{H} = \mathcal{H}_{A_1 A_2 \ldots A_k} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_k$ is said to be *completely entangled* if it has no non-zero product vector of the form $u_1 \otimes u_2 \otimes \cdots \otimes u_k$ with u_i in $\mathcal{H}_i$ for each i. Using the methods of elementary linear algebra and the intersection theorem for projective varieties in basic algebraic geometry we prove that

$$\max_{S \in \mathcal{E}} \dim S = d_1 d_2 \ldots d_k - (d_1 + \cdots + d_k) + k - 1,$$

where $\mathcal{E}$ is the collection of all completely entangled subspaces.

When $\mathcal{H}_1 = \mathcal{H}_2$ and $k = 2$ an explicit orthonormal basis of a maximal completely entangled subspace of $\mathcal{H}_1 \otimes \mathcal{H}_2$ is given.

We also introduce a more delicate notion of a *perfectly entangled* subspace for a multipartite quantum system, construct an example using the theory of stabilizer quantum codes and pose a problem.

Keywords. Finite level quantum systems; separable states; entangled states; completely entangled subspaces; perfectly entangled subspace; stabilizer quantum code.

1. Completely entangled subspaces

Let $\mathcal{H}_i$ be a complex finite dimensional Hilbert space of dimension d_i associated with a finite level quantum system A_i for each $i = 1, 2, \ldots, k$. A state ρ of the combined system $A_1 A_2 \ldots A_k$ in the Hilbert space

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_k \tag{1.1}$$

is said to be *separable* if it can be expressed as

$$\rho = \sum_{i=1}^{m} p_i \rho_{i1} \otimes \rho_{i2} \otimes \cdots \otimes \rho_{ik}, \tag{1.2}$$

where ρ_{ij} is a state of A_j for each j, $p_i > 0$ for each i and $\sum_{i=1}^{m} p_i = 1$ for some finite m. A state which is not separable is said to be *entangled*. Entangled states play an important role in quantum teleportation and communication [3]. The following theorem due to Horodecki and Horodecki [2] suggests a method of constructing entangled states.

Theorem 1.1 [2]. *Let ρ be a separable state in $\mathcal{H}$. Then the range of ρ is spanned by a set of product vectors.*

For the sake of readers' convenience and completeness we furnish a quick proof.

Proof. Let ρ be of the form (1.2). By spectrally resolving each ρ_{ij} into one-dimensional projections we can rewrite (1.2) as

$$\rho = \sum_{i=1}^{n} q_i |u_{i1} \otimes u_{i2} \otimes \cdots \otimes u_{ik}\rangle\langle u_{i1} \otimes u_{i2} \otimes \cdots \otimes u_{ik}|, \tag{1.3}$$

where u_{ij} is a unit vector in $\mathcal{H}_j$ for each i, j and $q_i > 0$ for each i with $\sum_{i=1}^{n} q_i = 1$. We shall prove the theorem by showing that each of the product vectors $u_{i1} \otimes u_{i2} \otimes \cdots \otimes u_{ik}$ is, indeed, in the range of ρ. Without loss of generality, consider the case $i = 1$. Write (1.3) as

$$\rho = q_1 |u_{11} \otimes u_{12} \otimes \cdots \otimes u_{1k}\rangle\langle u_{11} \otimes u_{12} \otimes \ldots \otimes u_{1k}| + T, \tag{1.4}$$

where $q_1 > 0$ and T is a non-negative operator. Suppose $\psi \neq 0$ is a vector in $\mathcal{H}$ such that $T|\psi\rangle = 0$ and $\langle u_{11} \otimes u_{12} \otimes \cdots \otimes u_{1k}|\psi\rangle \neq 0$. Then $\rho|\psi\rangle$ is a non-zero multiple of the product vector $u_{11} \otimes u_{12} \otimes \cdots \otimes u_{1k}$ and $u_{11} \otimes u_{12} \otimes \cdots \otimes u_{1k} \in R(\rho)$, the range of ρ. Now suppose that the null space $N(T)$ of T is contained in $\{u_{11} \otimes u_{12} \otimes \cdots \otimes u_{1k}\}^{\perp}$. Then $R(T) \supset \{u_{11} \otimes u_{12} \otimes \cdots \otimes u_{1k}\}$ and therefore there exists a vector $\psi \neq 0$ such that

$$T|\psi\rangle = |u_{11} \otimes u_{12} \otimes \cdots \otimes u_{1k}\rangle.$$

Note that $\rho|\psi\rangle \neq 0$, for otherwise, the positivity of ρ, T and q_1 in (1.4) would imply $T|\psi\rangle = 0$. Thus (1.4) implies

$$\rho|\psi\rangle = (q_1\langle u_{11} \otimes u_{12} \otimes \cdots \otimes u_{1k}|\psi\rangle + 1)\ |u_{11} \otimes u_{12} \otimes \cdots \otimes u_{1k}\rangle.$$

□

COROLLARY

If a subspace $S \subset \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_k$ does not contain any non-zero product vector of the form $u_1 \otimes u_2 \otimes \cdots \otimes u_k$ where $u_i \in \mathcal{H}_i$ for each i, then any state with support in S is entangled.

Proof. Immediate. □

DEFINITION 1.2

A non-zero subspace $S \subset \mathcal{H}$ is said to be *completely entangled* if S contains no non-zero product vector of the form $u_1 \otimes u_2 \otimes \cdots \otimes u_k$ with $u_i \in \mathcal{H}_i$ for each i.

Denote by $\mathcal{E}$ the collection of all completely entangled subspaces of $\mathcal{H}$. Our goal is to determine $\max_{S \in \mathcal{E}} \dim S$.

PROPOSITION 1.3

There exists $S \in \mathcal{E}$ satisfying

$$\dim\ S = d_1 d_2 \ldots d_k - (d_1 + d_2 + \cdots + d_k) + k - 1.$$

Proof. Let $N = d_1+d_2+\cdots+d_k-k+1$. Without loss of generality, assume that $\mathcal{H}_i = \mathbb{C}^{d_i}$ for each i, with the standard scalar product. Choose and fix a set $\{\lambda_1, \lambda_2, \ldots, \lambda_N\} \subset \mathbb{C}$ of cardinality N. Define the column vectors

$$u_{ij} = \begin{bmatrix} 1 \\ \lambda_i \\ \lambda_i^2 \\ \vdots \\ \lambda_i^{d_j-1} \end{bmatrix}, 1 \le i \le N, \quad 1 \le j \le k \tag{1.5}$$

and consider the subspace

$$S = \{u_{i1} \otimes u_{i2} \otimes \cdots \otimes u_{ik}, \quad 1 \le i \le N\}^{\perp} \subset \mathcal{H}. \tag{1.6}$$

We claim that S has no non-zero product vector. Indeed, let

$$0 \ne v_1 \otimes v_2 \otimes \cdots \otimes v_k \in S, \quad v_i \in \mathcal{H}_i.$$

Then

$$\prod_{j=1}^{k} \langle v_j | u_{ij} \rangle = 0, \quad 1 \le i \le N. \tag{1.7}$$

If

$$E_j = \{i | \langle v_j | u_{ij} \rangle = 0\} \subset \{1, 2, \ldots, N\}, \tag{1.8}$$

then (1.7) implies that

$$\{1, 2, \ldots, N\} = \cup_{j=1}^{k} E_j$$

and therefore

$$N \le \sum_{j=1}^{k} \# E_j.$$

By the definition of N it follows that for some j, $\# E_j \ge d_j$. Suppose $\# E_{j_0} \ge d_{j_0}$. From (1.8) we have

$$\langle v_{j_0} | u_{ij_0} \rangle = 0 \quad \text{for} \quad i = i_1, i_2, \ldots, i_{d_{j_0}},$$

where $i_1 < i_2 < \cdots < i_{d_{j_0}}$. From (1.5) and the property of van der Monde determinants it follows that $v_{j_0} = 0$, a contradiction. Clearly, dim $S \ge d_1 d_2 \ldots d_k - (d_1 + \cdots + d_k) + k - 1$. □

PROPOSITION 1.4

Let $S \subset \mathcal{H}$ be a subspace of dimension $d_1 d_2 \ldots d_k - (d_1 + \cdots + d_k) + k$. Then S contains a non-zero product vector.

Proof. Identify $\mathcal{H}_j$ with $\mathbb{C}^{d_j}$ for each $j = 1, 2, \ldots, k$. For any non-zero element v in a complex vector space $\mathcal{V}$ denote by $[v]$ the equivalence class of v in the projective space $\mathbb{P}(\mathcal{V})$. Consider the map

$$T : \mathbb{P}(\mathbb{C}^{d_1}) \times \mathbb{P}(\mathbb{C}^{d_2}) \times \cdots \times \mathbb{P}(\mathbb{C}^{d_k}) \to \mathbb{P}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_k})$$

given by

$$T([u_1], [u_2], \ldots, [u_k]) = [u_1 \otimes \cdots \otimes u_k].$$

The map T is algebraic and hence its range $R(T)$ is a complex projective variety of dimension $\sum_{i=1}^{k}(d_i - 1)$. By hypothesis, $\mathbb{P}(S)$ is a projective variety of dimension $d_1 d_2 \ldots d_k - (d_1 + \cdots + d_k) + k - 1$. Thus

$$\begin{aligned} \dim \mathbb{P}(S) + \dim R(T) &= d_1 d_2 \ldots d_k - 1 \\ &= \dim \mathbb{P}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_k}). \end{aligned}$$

Hence by Theorem 6, p. 76 in [4] we have

$$\mathbb{P}(S) \cap R(T) \neq \emptyset.$$

In other words, S contains a product vector. □

Theorem 1.5. *Let $\mathcal{E}$ be the collection of all completely entangled subspaces of $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_k$. Then*

$$\max_{S \in \mathcal{E}} \dim S = d_1 d_2 \ldots d_k - (d_1 + d_2 + \cdots + d_k) + k - 1.$$

Proof. Immediate from Propositions 1.3 and 1.4. □

2. An explicit orthonormal basis for a completely entangled subspace of maximal dimension in $\mathbb{C}^n \otimes \mathbb{C}^n$

Let $\{|x\rangle, x = 0, 1, 2, \ldots, n-1\}$ be a labelled orthonormal basis in the Hilbert space $\mathbb{C}^n$. Choose and fix a set

$$E = \{\lambda_1, \lambda_2, \ldots, \lambda_{2n-1}\} \subset \mathbb{C}$$

of cardinality $2n - 1$ and consider the subspace

$$S = \{u_{\lambda_i} \otimes u_{\lambda_i}, 1 \leq i \leq 2n-1\}^{\perp},$$

where

$$u_\lambda = \sum_{x=0}^{n-1} \lambda^x |x\rangle, \quad \lambda \in \mathbb{C}.$$

By the proof of Proposition 1.3 and Theorem 1.5 it follows that S is a maximal completely entangled subspace of dimension $n^2 - 2n + 1$. We shall now present an explicit orthonormal basis for S.

First, observe that S is orthogonal to a set of symmetric vectors and therefore S contains the antisymmetric tensor product space $\mathbb{C}^n \wedge \mathbb{C}^n$ which has the orthonormal basis

$$B_0 = \left\{ \frac{|xy\rangle - |yx\rangle}{\sqrt{2}}, \quad 0 \le x < y \le n-1 \right\}. \tag{2.1}$$

Thus, in order to construct an orthonormal basis of S, it is sufficient to search for symmetric tensors lying in S and constituting an orthonormal set. Any symmetric tensor in S can be expressed as

$$\sum_{\substack{0 \le x \le n-1 \\ 0 \le y \le n-1}} f(x, y)|xy\rangle, \tag{2.2}$$

where $f(x, y) = f(y, x)$ and

$$\sum_{\substack{0 \le x \le n-1 \\ 0 \le y \le n-1}} f(x, y)\lambda_i^{x+y} = 0, \quad 1 \le i \le 2n-1,$$

which reduces to

$$\sum_{\substack{0 \le x \le n-1 \\ 0 \le j-x \le n-1}} f(x, j-x) = 0 \quad \forall\, 0 \le j \le 2n-2. \tag{2.3}$$

Define $\mathcal{K}_j$ to be the subspace of all symmetric tensors of the form (2.2) where the coefficient function f is symmetric, has its support in the set $\{(x, j-x), 0 \le x \le n-1, 0 \le j-x \le n-1\}$ and satisfies (2.3). Simple algebra shows that $\mathcal{K}_0 = \mathcal{K}_1 = \mathcal{K}_{2n-3} = \mathcal{K}_{2n-2} = 0$ and

$$S = \mathcal{H} \wedge \mathcal{H} \oplus \oplus_{j=2}^{2n-4} \mathcal{K}_j.$$

We shall now present an orthonormal basis B_j for $\mathcal{K}_j, 2 \le j \le 2n-4$. This falls into four cases.

Case 1. $2 \le j \le n-1, \quad j$ even.

$$B_j = \left\{ \frac{1}{\sqrt{j(j+1)}} \left[\sum_{m=0}^{(j/2)-1} (|mj-m\rangle + |j-mm\rangle) - j \left| \frac{j}{2}\, \frac{j}{2} \right\rangle \right] \right\}$$
$$\cup \left\{ \frac{1}{\sqrt{j}} \sum_{m=0}^{(j/2)-1} \mathrm{e}^{4i\pi mp/j} (|mj-m\rangle + |j-mm\rangle), \quad 1 \le p \le \frac{j}{2} - 1 \right\}.$$

Case 2. $2 \le j \le n-1, \quad j$ odd.

$$B_j = \left\{ \frac{1}{\sqrt{j+1}} \sum_{m=0}^{(j-1)/2} \mathrm{e}^{4i\pi mp/(j+1)} (|mj-m\rangle + |j-mm\rangle), \right.$$
$$\left. 1 \le p \le \frac{j-1}{2} \right\}.$$

Case 3. $n \leq j \leq 2n-4, \quad j$ even.

$$B_j = \left\{ \frac{1}{\sqrt{(2n-2-j)(2n-1-j)}} \left[\sum_{m=0}^{((2n-2-j)/2)-1} (|j-n+m \right.\right.$$

$$+ 1\ n-m-1\rangle + |n-m-1\ j-n+m+1\rangle)$$

$$\left.\left. -(2n-2-j)\left|\frac{j}{2}\frac{j}{2}\right\rangle \right]\right\}$$

$$\cup \left\{ \frac{1}{\sqrt{2n-2-j}} \sum_{m=0}^{((2n-2-j)/2)-1} e^{4i\pi mp/(2n-2-j)} (|j-n+m \right.$$

$$+ 1\ n-m-1\rangle |n-m-1\ j-n+m+1\rangle),$$

$$\left. 1 \leq p \leq \frac{2n-2-j}{2} - 1 \right\}.$$

Case 4. $n \leq j \leq 2n-4, \quad j$ odd.

$$B_j = \left\{ \frac{1}{\sqrt{2n-1-j}} \sum_{m=0}^{((2n-1-j)/2)-1} e^{4i\pi mp/(2n-1-j)} \right.$$

$$+ (|j-n+m+1\ n-m-1\rangle + |n-m-1\ j-n+m+1\rangle),$$

$$\left. 1 \leq p \leq \frac{2n-1-j}{2} - 1 \right\}.$$

The set $B_0 \cup \cup_{j=2}^{2n-4} B_j$, where B_0 is given by (2.1) and the remaining B_j's are given by the four cases above constitute an orthonormal basis for the maximal completely entangled subspace S.

3. Perfectly entangled subspaces

As in §1, let $\mathcal{H}_i$ be a complex Hilbert space of dimension d_i associated with a finite level quantum system A_i for each $i = 1, 2, \ldots, k$. For any subset $E \subset \{1, 2, \ldots, k\}$ let

$$\mathcal{H}(E) = \otimes_{i \in E} \mathcal{H}_i,$$

$$d(E) = \prod_{i \in E} d_i,$$

so that the Hilbert space $\mathcal{H} = \mathcal{H}(\{1, 2, \ldots, k\})$ of the joint system $A_1 A_2 \ldots A_k$ can be viewed as $\mathcal{H}(E) \otimes \mathcal{H}(E')$, E' being the complement of E. For any operator X on $\mathcal{H}$ we write

$$X(E) = \mathrm{Tr}_{\mathcal{H}(E')} X,$$

where the right-hand side denotes the relative trace of X taken over $\mathcal{H}(E')$. Then $X(E)$ is an operator in $\mathcal{H}(E)$. If ρ is a state of the system $A_1 A_2 \ldots A_k$ then $\rho(E)$ describes the marginal state of the subsystem $A_{i_1} A_{i_2} \ldots A_{i_r}$ where $E = \{i_1, i_2, \ldots, i_r\}$.

DEFINITION 3.1

A non-zero subspace $\mathcal{S} \subset \mathcal{H}$ is said to be *perfectly entangled* if for any $E \subset \{1, 2, \ldots, k\}$ such that $d(E) \leq d(E')$ and any unit vector $\psi \in \mathcal{S}$ one has

$$(|\psi\rangle\langle\psi|)\,(E) = \frac{I_E}{d(E)},$$

where I_E denotes the identity operator in $\mathcal{H}(E)$.

For any state ρ, denote by $S(\rho)$ the von Neumann entropy of ρ. If ψ is a pure state in $\mathcal{H}$ then $S((|\psi\rangle\langle\psi|)(E)) = S((|\psi\rangle\langle\psi|)(E'))$. Thus perfect entanglement of a subspace $\mathcal{S}$ is equivalent to the property that for every unit vector ψ in $\mathcal{S}$, the pure state $|\psi\rangle\langle\psi|$ is maximally entangled in every decomposition $\mathcal{H}(E) \otimes \mathcal{H}(E')$, i.e.,

$$S((|\psi\rangle\langle\psi|)(E)) = S((|\psi\rangle\langle\psi|)(E')) = \log_2 d(E)$$

whenever $d(E) \leq d(E')$. In other words, the marginal states of $|\psi\rangle\langle\psi|$ in $\mathcal{H}(E)$ and $\mathcal{H}(E')$ have the maximum possible von Neumann entropy.

Denote by $\mathcal{P}$ the class of all perfectly entangled subspaces of $\mathcal{H}$. It is an interesting problem to construct examples of perfectly entangled subspaces and also compute $\max_{\mathcal{S}\in\mathcal{P}} \dim \mathcal{S}$.

Note that a perfectly entangled subspace $\mathcal{S}$ is also completely entangled. Indeed, if $\mathcal{S}$ has a unit product vector $\psi = u_1 \otimes u_2 \otimes \cdots \otimes u_k$ where each u_i is a unit vector in $\mathcal{H}_i$ then $(|\psi\rangle\langle\psi|)(E)$ is also a pure product state with von Neumann entropy zero. Perfect entanglement of $\mathcal{S}$ implies the stronger property that every unit vector ψ in $\mathcal{S}$ is *indecomposable*, i.e., ψ cannot be factorized as $\psi_1 \otimes \psi_2$ where $\psi_1 \in \mathcal{H}(E)$, $\psi_2 \in \mathcal{H}(E')$ for any proper subset $E \subset \{1, 2, \ldots, k\}$.

PROPOSITION 3.2

Let $\mathcal{S} \subset \mathcal{H}$ be a subspace and let P denote the orthogonal projection on $\mathcal{S}$. Then $\mathcal{S}$ is perfectly entangled if and only if, for any proper subset $E \subset \{1, 2, \ldots, k\}$ with $d(E) \leq d(E')$,

$$(PXP)(E) = \frac{\operatorname{Tr} PX}{d(E)} I_E$$

for all operators X on $\mathcal{H}$.

Proof. Sufficiency is immediate. To prove necessity, assume that S is perfectly entangled. Let X be any hermitian operator on $\mathcal{H}$. Then by spectral theorem and Definition 3.1 it follows that $(PXP)(E) = \alpha(X) I_E$ where $\alpha(X)$ is a scalar. Equating the traces of both sides we see that $\alpha(X) = d(E)^{-1} \operatorname{Tr} PX$. If X is arbitrary, then X can be expressed as $X_1 + iX_2$ where X_1 and X_2 are hermitian and the required result is immediate. □

Using the method of constructing single error correcting 5 qudit stabilizer quantum codes in the sense of Gottesman [1, 3] we shall now describe an example of a perfectly entangled d-dimensional subspace in $h^{\otimes^5}$ where h is a d-dimensional Hilbert space. To this end we identify h with $L^2(A)$ where A is an abelian group of cardinality d with group operation + and null element 0. Then $h^{\otimes^5}$ is identified with $L^2(A^5)$. For any $\mathbf{x} = (x_0, x_1, x_2, x_3, x_4)$ in A^5 denote by $|\mathbf{x}\rangle$ the indicator function of the singleton subset $\{\mathbf{x}\}$ in A^5. Then $\{|\mathbf{x}\rangle, \mathbf{x} \in A^5\}$

is an orthonormal basis for $h^{\otimes^5}$. Choose and fix a non-degenerate symmetric bicharacter $\langle .\,,\ .\rangle$ for the group A satisfying the following:

$$|\langle a, b\rangle| = 1, \langle a, b\rangle = \langle b, a\rangle, \langle a, b+c\rangle = \langle a, b\rangle\langle a, c\rangle \quad \forall\, a, b, c \in A$$

and $a = 0$ if and only if $\langle a, x\rangle = 1$ for all $x \in A$. Define

$$\langle \mathbf{x},\ \mathbf{y}\rangle = \prod_{i=0}^{4} \langle x_i,\ y_i\rangle,\ \mathbf{x},\ \mathbf{y} \in A^5.$$

(Note that $\langle \mathbf{x},\ \mathbf{y}\rangle$ denotes the bicharacter evaluated at $\mathbf{x},\ \mathbf{y}$ whereas $\langle \mathbf{x}|\mathbf{y}\rangle$ denotes the scalar product in $\mathcal{H} = L^2(A^5)$.) With these notations we introduce the unitary Weyl operators $U_{\mathbf{a}}$, $V_{\mathbf{b}}$ in $\mathcal{H}$ satisfying

$$U_{\mathbf{a}}|\mathbf{x}\rangle = |\mathbf{a}+\mathbf{x}\rangle,\ V_{\mathbf{b}}|\mathbf{x}\rangle = \langle \mathbf{b}, \mathbf{x}\rangle\ |\mathbf{x}\rangle,\ \mathbf{x} \in A^5.$$

Then we have the Weyl commutation relations:

$$U_{\mathbf{a}}U_{\mathbf{b}} = U_{\mathbf{a}+\mathbf{b}},\ V_{\mathbf{a}}V_{\mathbf{b}} = V_{\mathbf{a}+\mathbf{b}}, V_{\mathbf{b}}U_{\mathbf{a}} = \langle \mathbf{a}, \mathbf{b}\rangle U_{\mathbf{a}}V_{\mathbf{b}}$$

for all $\mathbf{a}, \mathbf{b} \in A^5$. The family $\{d^{-5/2}U_{\mathbf{a}}V_{\mathbf{b}}, \mathbf{a}, \mathbf{b} \in A^5\}$ is an orthonormal basis for the Hilbert space of all operators on $\mathcal{H}$ with the scalar product $\langle X|Y\rangle = \mathrm{Tr}\ X^{\dagger}Y$ between two operators X, Y.

Introduce the cyclic permutation σ in A^5 defined by

$$\sigma((x_0, x_1, x_2, x_3, x_4)) = (x_4, x_0, x_1, x_2, x_3). \tag{3.1}$$

Then σ is an automorphism of the product group A^5 and

$$\sigma^{-1}((x_0, x_1, x_2, x_3, x_4)) = (x_1, x_2, x_3, x_4, x_0).$$

Define

$$\tau(\mathbf{x}) = \sigma^2(\mathbf{x}) + \sigma^{-2}(\mathbf{x}). \tag{3.2}$$

Let $C \subset A^5$ be the subgroup defined by

$$C = \{\mathbf{x}|x_0 + x_1 + x_2 + x_3 + x_4 = 0\}.$$

Define

$$W_{\mathbf{x}} = \langle \mathbf{x}, \sigma^2(\mathbf{x})\rangle U_{\mathbf{x}}V_{\tau(\mathbf{x})}, \quad \mathbf{x} \in A^5. \tag{3.3}$$

Then the correspondence $\mathbf{x} \to W_{\mathbf{x}}$ is a unitary representation of the subgroup C in $\mathcal{H}$. Define the operator P_C by

$$P_C = d^{-4}\sum_{\mathbf{x}\in C} W_{\mathbf{x}}. \tag{3.4}$$

Then P_C is a projection satisfying $\mathrm{Tr}\ P_C = d$. The range of P_C is an example of a stabilizer quantum code in the sense of Gottesman. From the methods of [1] it is also known that P_C is a single error correcting quantum code. The range $R(P_C)$ of C is given by

$$R(P_C) = \{|\psi\rangle | W_{\mathbf{x}}|\psi\rangle = |\psi\rangle \quad \text{for all } \mathbf{x} \in C\}.$$

Our goal is to establish that $R(P_C)$ is perfectly entangled in $L^2(A)^{\otimes^5}$. To this end we prove a couple of lemmas.

Lemma 3.3. *For any* $\mathbf{a}, \mathbf{b} \in A^5$ *the following holds*:

$$\langle \mathbf{a}|P_C|\mathbf{b}\rangle = \begin{cases} 0, & \text{if } \sum_{i=0}^4 (a_i - b_i) \neq 0, \\ d^{-4}\langle \mathbf{a}, \sigma^2(\mathbf{a})\rangle \overline{\langle \mathbf{b}, \sigma^2(\mathbf{b})\rangle}, & \text{otherwise}. \end{cases}$$

Proof. We have from (3.1)–(3.4) that

$$\langle \mathbf{a}|P_C|\mathbf{b}\rangle = d^{-4} \sum_{x_0+x_1+x_2+x_3+x_4=0} \langle \mathbf{x}, \sigma^2(\mathbf{x})\rangle \langle \tau(\mathbf{x}), \mathbf{b}\rangle \langle \mathbf{a}|\mathbf{x}+\mathbf{b}\rangle$$

which vanishes if $\sum_{i=0}^4 (a_i - b_i) \neq 0$. Now assume that $\sum_{i=0}^4 (a_i - b_i) = 0$. Then

$$\begin{aligned} \langle \mathbf{a}|P_C|\mathbf{b}\rangle &= d^{-4}\langle \mathbf{a}-\mathbf{b}, \sigma^2(\mathbf{a}-\mathbf{b})\rangle \langle \sigma^2(\mathbf{a}-\mathbf{b}), \mathbf{b}\rangle \langle \mathbf{a}-\mathbf{b}, \sigma^2(\mathbf{b})\rangle \\ &= d^{-4}\langle \mathbf{a}, \sigma^2(\mathbf{a})\rangle \overline{\langle \mathbf{b}, \sigma^2(\mathbf{b})\rangle}. \end{aligned}$$

□

Lemma 3.4. *Consider the tensor product Hilbert space*

$$L^2(A)^{\otimes^5} = \mathcal{H}_0 \otimes \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 \otimes \mathcal{H}_4,$$

where $\mathcal{H}_i$ *is the i-th copy of* $L^2(A)$. *Then for any* $(\{i, j\}) \subset \{0, 1, 2, 3, 4\}$ *and* $\mathbf{a}, \mathbf{b} \in A^5$ *the operator* $(P_C|\mathbf{a}\rangle\langle \mathbf{b}|P_C)$ $(\{i, j\})$ *is a scalar multiple of the identity in* $\mathcal{H}_i \otimes \mathcal{H}_j$.

Proof. By Lemma 3.2 and the definition of relative trace we have, for any $x_0, x_1, y_0, y_1 \in A$,

$$\begin{aligned} &\langle x_0, x_1|(P_C|\mathbf{a}\rangle\langle \mathbf{b}|P_C)\ (\{0, 1\})|y_0, y_1\rangle \\ &\quad = \sum_{x_2,x_3,x_4 \in A} \langle x_0, x_1, x_2, x_3, x_4|P_C|\mathbf{a}\rangle\langle \mathbf{b}|P_C|y_0, y_1, x_2, x_3, x_4\rangle \\ &\quad = d^{-8} \sum_{\substack{x_2+x_3+x_4=\sum a_i - x_0 - x_1 \\ x_2+x_3+x_4=\sum b_i - y_0 - y_1}} \langle \mathbf{x}, \sigma^2(\mathbf{x})\rangle \overline{\langle \mathbf{a}, \sigma^2(\mathbf{a})\rangle} \langle \mathbf{b}, \sigma^2(\mathbf{b})\rangle \\ &\qquad \times \overline{\langle y_0, y_1, x_2, x_3, x_4, \sigma^2(y_0, y_1, x_2, x_3, x_4)\rangle}. \end{aligned}$$

The right-hand side vanishes if $\sum(a_i - b_i) \neq x_0 + x_1 - y_0 - y_1$. Now suppose that $\sum(a_i - b_i) = x_0 + x_1 - y_0 - y_1$. Then the right-hand side is equal to

$$\begin{aligned} &d^{-8}\overline{\langle \mathbf{a}, \sigma^2(\mathbf{a})\rangle} \langle \mathbf{b}, \sigma^2(\mathbf{b})\rangle \left\langle \sum a_i - x_0 - x_1, x_0 + x_1 - y_0 - y_1 \right\rangle \\ &\quad \times \sum_{x_2,x_4 \in A} \langle x_2, y_1 - x_1\rangle \langle x_4, y_0 - x_0\rangle \\ &\quad = \begin{cases} 0, & \text{if } x_0 \neq y_0 \text{ or } x_1 \neq y_1, \\ d^{-6}\overline{\langle \mathbf{a}, \sigma^2(\mathbf{a})\rangle} \langle \mathbf{b}, \sigma^2(\mathbf{b})\rangle, & \text{otherwise}. \end{cases} \end{aligned}$$

This proves the lemma when $i = 0$, $j = 1$. A similar (but tedious) algebra shows that the lemma holds when $i = 0$, $j = 2$.

The cyclic permutation σ of the basis $\{|\mathbf{x}\rangle, \mathbf{x} \in A^5\}$ induces a unitary operator U_σ in A^5. Since σ leaves C invariant it follows that $U_\sigma P_C = P_C U_\sigma$ and therefore

$$U_\sigma P_C |\mathbf{a}\rangle\langle\mathbf{b}| P_C U_\sigma^{-1} = P_C|\sigma(\mathbf{a})\rangle\langle\sigma(\mathbf{b})|P_C,$$

which, in turn, implies that

$$\begin{aligned}&\langle x_1, x_2|(P_C|\mathbf{a}\rangle\langle\mathbf{b}|P_C)\ (\{1,2\})|y_1, y_2\rangle \\ &\quad = \langle x_1, x_2|P_C|\sigma^{-1}(\mathbf{a})\rangle\langle\sigma^{-1}(\mathbf{b})|P_C)(\{0,1\})|y_1, y_2\rangle.\end{aligned}$$

By what has been already proved the lemma follows for $i = 1$, $j = 2$. A similar covariance argument proves the lemma for all pairs $\{i, j\}$. □

Theorem 3.5. *The range of P_C is a perfectly entangled subspace of $L^2(A)^{\otimes^5}$ and* $\dim P_C = \#A$.

Proof. Immediate from Lemma 3.3 and the fact that every operator in $L^2(A^{\otimes^5})$ is a linear combination of operators of the form $|\mathbf{a}\rangle\langle\mathbf{b}|$ as $\mathbf{a}, \mathbf{b}$ vary in A^5. □

Note added in Proof. The example in §2 has been recently generalized and simplified considerably by B V Rajarama Bhat. See arXiv: quant-ph/0409032 VI 6 Sep. 2004.

Acknowledgement

The author would like to thank A J Parameswaran and V Pati for their help in explaining to him the role of basic algebraic geometry in the proof of Proposition 1.4.

References

[1] Arvind V and Parthasarathy K R, A family of quantum stabilizer codes based on the Weyl commutation relations over a finite field, in: A tribute to C.S. Seshadri, perspectives in geometry and representation theory (eds) V Lakshmibai *et al* (India: Hindustan Book Agency) (2003) pp. 133–153

[2] Horodecki M and Horodecki R, Separability of mixed states: necessary and sufficient conditions, *Phys. Lett.* **A223(1-2)** (1996) 1–8

[3] Nielsen M A and Chuang I L, Quantum computation and quantum information (Cambridge: Cambridge University Press) (1999)

[4] Shafarevich I R, Basic Algebraic Geometry I, Second edition (Berlin: Springer Verlag) (translated from Russian) (1994)