isid/ms/2008/04
June 18, 2008
http://www.isid.ac.in/~statmath/eprints

Quantum error correcting codes and Weyl commutation relations

K. R. Parthasarathy

Indian Statistical Institute, Delhi Centre
7, SJSS Marg, New Delhi–110 016, India

Quantum Error Correcting Codes and Weyl Commutation Relations

K. R. Parthasarathy
Indian Statistical Institute,
Delhi Centre
7, S. J. S. Sansanwal Marg,
New Delhi - 110 016, India
email: krp@isid.ac.in

To V. S. Varadarajan on his 70th birthday with affection and admiration

Abstract This is mainly an expository account of the general theory of quantum error correcting codes exploiting the commutation relations between the Weyl operators associated with a finite additive abelian group. There are some new elements of proofs and remarks, particularly, in the context of the Knill-Laflamme theorem [5].

Key words : quantum error correcting code, (n, k, d) quantum code, entanglement property for multipartite states.

1 Introduction

In the mathematical theory of quantum computation and quantum information [6] states of a quantum system described by a complex Hilbert space $\mathcal{H}$ are viewed as information resources which can be exploited to perform numerical computations or communicate messages by applications of quantum gates and making measurements. However, in such a process the states can get corrupted by external noise. To overcome the effects of noise one looks for a nice subspace $\mathcal{C} \subset \mathcal{H}$ with the property that states with support in $\mathcal{C}$ can be recovered by a recovery or decoding operation even though they get corrupted by noise, provided, the extent of corruption is limited. This can be expressed in the following pictorial form :

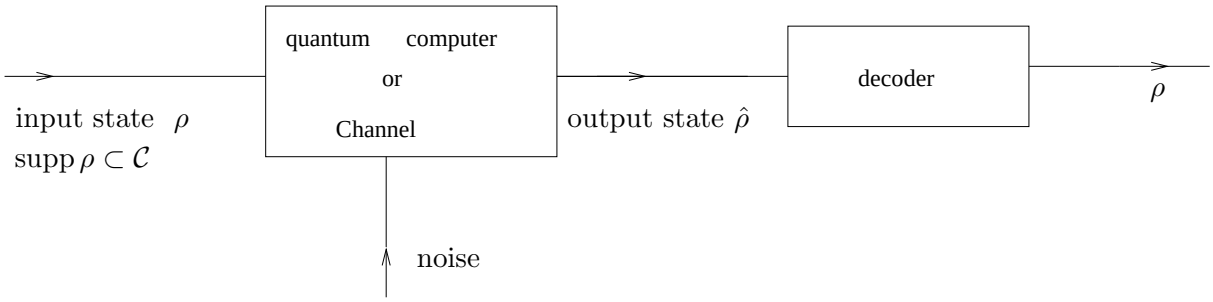


Figure 1: Encoding, transmission and decoding

It is useful to recall that $\mathrm{supp}\,\rho \subset \mathcal{C}$ means that ρ restricted to $\mathcal{C}^{\perp}$ is 0. The aim of the theory of quantum error correcting codes is to construct such a subspace $\mathcal{C}$ of reasonably large dimension and a decoding operation so that the picture above holds for a given model of noise. We assume that $\mathcal{H}$ is finite dimensional and the noise or corrupting operators come from a 'small' linear subspace $\mathcal{N}$ of the algbera $\mathcal{B}(\mathcal{H})$ of all operators on $\mathcal{H}$.

Given $\mathcal{N}$ we assume that any input state ρ produces a corrupted output state $\hat{\rho}$ of the form

$$\hat{\rho} = \frac{\sum_j N_j \rho N_j^{\dagger}}{\mathrm{Tr}\,\rho \sum_j N_j^{\dagger} N_j}, \qquad N_j \in \mathcal{N} \tag{1.1}$$

where the summations are finite. Repeated use of the same input state may result in different corrupt outputs, i.e., the operators N_j from $\mathcal{N}$ in (1.1) may change with the repetition.

To recover the original state from the corrupted output we employ a recovery or decoding operation of the form:

$$\mathbf{R}(\hat{\rho}) = \sum_i R_i \hat{\rho} R_i^{\dagger} \tag{1.2}$$

where $\mathbf{R} = (R_1, R_2, \ldots)$ is a finite sequence of operators on $\mathcal{H}$ satisfying the condition $\sum_i R_i^{\dagger} R_i = I$.

Thus the goal is to construct a reasonably 'large' subspace $\mathcal{C} \subset \mathcal{H}$ and design a recovery operation $\mathbf{R}$ satisfying the requirement

$$\mathbf{R}(\hat{\rho}) = \rho \quad \text{if} \quad \text{supp } \rho \subset \mathcal{C} \tag{1.3}$$

for all $\hat{\rho}$ of the form (1.1). Then the pair $(\mathcal{C}, \mathcal{R})$ is called a *quantum $\mathcal{N}$-correcting code*. If a subspace $\mathcal{C}$ admits a recovery operation $\mathbf{R}$ so that $(\mathcal{C}, \mathbf{R})$ is a quantum $\mathcal{N}$-correcting code we then say that $\mathcal{C}$, or equivalently, the orthogonal projection P on $\mathcal{C}$ is a *quantum $\mathcal{N}$-correcting code*. The dimension of $\mathcal{C}$ or $\operatorname{tr} P$ is called the *size* of the code.

The Knill-Laflamme theorem [5] gives a necessary and sufficient condition for a subspace $\mathcal{C}$ to be a quantum $\mathcal{N}$-correcting code. In the next section we shall present a proof of this theorem which, at the same time, yields an explicit decoding operation that can be implemented by a reflection in the tensor product of $\mathcal{H}$ with a natural ancillary Hilbert space arising from $\mathcal{N}$.

In section 3 we introduce the notion of a *quantum stabilizer code* in the sense of Gottesman [4], [1] using the language of Weyl operators associated with a finite abelian group. This describes the space of noise operators which can be detected or corrected by the stabilizer code and also provides an explicit formula for the decoding operation.

In the last section we apply the results of section 3 to a standard model of noise and conclude with an explicit example of a single error correcting code in a 5-fold product. This yields a family of perfectly entangled 5-partite states [8].

2 The Knill-Laflamme Theorem

Let $\mathcal{H}$ and $\mathcal{N} \subset \mathcal{B}(\mathcal{H})$ be as in section 1, $\mathcal{C} \subset \mathcal{H}$ a subspace and let $\mathbf{R}$ be a transformation of states (i.e., density operators) in $\mathcal{H}$ defined by

$$\mathbf{R}(\rho) = \sum_i R_j \rho R_j^\dagger \quad \text{for any state } \rho,$$

$R_1, R_2, \ldots$ being a finite sequence of operators in $\mathcal{H}$ satisfying the relation $\sum_j R_j^\dagger R_j = I$.

Proposition 2.1 The pair $(\mathcal{C}, \mathbf{R})$ is a quantum $\mathcal{N}$-correcting code if and only if there exist linear maps $\lambda_j : \mathcal{N} \to \mathbb{C}$ satisfying

$$R_j N|\psi\rangle = \lambda_j(N)|\psi\rangle \quad \forall \ \psi \in \mathcal{C}, N \in \mathcal{N}, j. \tag{2.1}$$

Proof First we prove necessity. Equations (1.1)-(1.3) imply that for any pure state $\rho = |\psi\rangle\langle\psi|$ with ψ in $\mathcal{C}$ and any N in $\mathcal{N}$

$$\mathbf{R}\left(\frac{N\,|\psi\rangle\langle\psi|\,N^\dagger}{\langle\psi|N^\dagger N|\psi\rangle}\right) = |\psi\rangle\langle\psi|.$$

Indeed, we get this by choosing the finite sequence $\{N_j\}$ to consist of one element N in $\mathcal{N}$. Thus

$$\sum_j R_j N|\psi\rangle\langle\psi|\,N^\dagger R_j^\dagger = \langle\psi|N^\dagger N|\psi\rangle\ |\psi\rangle\langle\psi| \ \forall\ \psi \in \mathcal{C}, N \in \mathcal{N}.$$

Fix ψ in $\mathcal{C}$, N in $\mathcal{N}$ and choose any unit vector $\varphi \perp \psi$. Taking expectations on both sides with respect to the state $|\varphi\rangle\langle\varphi|$ we have

$$\sum_i |\langle\varphi|R_j N|\psi\rangle|^2 = 0 \ \forall \ \psi \in \mathcal{C}, N \in \mathcal{N}, \varphi \perp \psi.$$

This is possible only if $R_j N|\psi\rangle$ is a scalar multiple of $|\psi\rangle$ for every ψ in $\mathcal{C}$, $N \in \mathcal{N}$ and j. Since $R_j N$ is an operator, equation (2.1) holds for some linear map $\lambda_j : \mathcal{N} \to \mathbb{C}$, completing the proof of necessity.

To prove sufficiency consider a state ρ with support in $\mathcal{C}$ and a finite sequence $\{N_i\}$ of operators in $\mathcal{N}$. By (2.1) and the fact that ρ is of the form $\sum_i p_r|\psi_r\rangle\langle\psi_r|$ for some ψ_r's in $\mathcal{C}$, $p_r \geq 0$, $\sum_r p_r = 1$ we have

$$\begin{aligned} \sum_j R_j \left(\sum_i N_i \rho N_i^\dagger \right) R_j^\dagger &= \sum_{i,j,r} |\lambda_j(N_i)|^2 \, p_r |\psi_r\rangle\langle\psi_r| \\ &= c \ \rho \end{aligned}$$

for some positive scalar c. Taking trace on both sides and using the relation $\sum_j R_j^\dagger R_j = I$ we have $c = \operatorname{Tr} \rho \sum_i N_i^\dagger N_i$. This completes the proof. □

Proposition 2.2 Let $(\mathcal{C}, \mathbf{R})$ be a quantum $\mathcal{N}$-correcting code. If P is the orthogonal projection on $\mathcal{C}$ then

$$P N_1^\dagger N_2 P = \lambda(N_1^\dagger N_2) P \ \forall \ N_1, N_2 \in \mathcal{N} \tag{2.2}$$

where $\lambda(N_1^\dagger N_2)$ is a scalar depending on the operator $N_1^\dagger N_2$.

Proof For any two vectors u, v in $\mathcal{H}$ and $\mathbf{R}$ as in Proposition 2.1 we have from the same proposition

$$\begin{aligned} \langle u|P N_1^\dagger N_2 P|v\rangle &= \langle u|P N_1^\dagger (\sum_j R_j^\dagger R_j) N_2 P|v\rangle \\ &= \sum_j \overline{\lambda_j(N_1)} \lambda_j(N_2) \langle Pu|Pv\rangle. \end{aligned}$$

Since the left hand side depends only on the operator $N_1^\dagger N_2$ it follows that there exists a scalar $\lambda(N_1^\dagger N_2)$ satisfying (2.2). □

Theorem 2.3(Knill-Laflamme [5]) Let $\mathcal{C} \subset \mathcal{H}$, $\mathcal{N} \subset \mathcal{B}(\mathcal{H})$ be subspaces of $\mathcal{H}$ and $\mathcal{N}$ respectively. Then $\mathcal{C}$ is a quantum $\mathcal{N}$-correcting code if and only if the orthogonal projection P on $\mathcal{C}$ satisfies the relation (2.2).

Proof The only if part is the same as Proposition 2.2. To prove the if part assume (2.2) and observe that the map $(N_1, N_2) \to \lambda(N_1^\dagger N_2)$ is a nonnegative definite sesquilinear form on $\mathcal{N} \times \mathcal{N}$. Denote by $\mathcal{N}_0 \subset \mathcal{N}$ the subspace $\left\{ N | N \in \mathcal{N}, \lambda(N^\dagger N) = 0 \right\}$. Then the quotient vector space $\widetilde{\mathcal{N}} = \mathcal{N}/\mathcal{N}_0$ becomes a Hilbert space with the scalar product $\langle [N_1] | [N_2] \rangle = \lambda(N_1^\dagger N_2)$

between the equivalence classes $[N_i] = N_i + \mathcal{N}_0$, $i = 1, 2$. Now choose and fix elements $[N_j]$, $1 \leq j \leq k$ which constitute an orthonormal basis for $\widetilde{\mathcal{N}}$. In particular, we have $\lambda(N_i^\dagger N_j) = \delta_{ij}$, $i, j \in \{1, 2, \ldots, k\}$. We have

$$N_i P N_i^\dagger N_j P N_j^\dagger = \delta_{ij} N_i P N_i^\dagger, i, j \in \{1, 2, \ldots, k\}.$$

If we write $P_i = N_i P N_i^\dagger$ it follows that $P_1, P_2, \ldots, P_k$ are mutually orthogonal projections. Define $Q = I - \sum_{i=1}^{k} P_i$ and the operators

$$R_j = \begin{cases} PN_j^\dagger & \text{if} \quad 1 \leq j \leq k, \\ Q & \text{if} \quad j = k+1. \end{cases} \tag{2.3}$$

Then $\sum_{j=1}^{k+1} R_j^\dagger R_j = I$ and for any ψ in $\mathcal{C}$ we have

$$\begin{aligned} QN|\psi\rangle &= \left(I - \sum_{j=1}^{k} N_j P N_j^\dagger \right) NP|\psi\rangle \\ &= \left(N - \sum_{j=1}^{k} \langle [N_j] | [N] \rangle N_j \right) P|\psi\rangle \\ &= MP|\psi\rangle \end{aligned}$$

where M is an element of $\mathcal{N}_0$. Hence

$$\begin{aligned} \|QN|\psi\rangle\|^2 &= \langle\psi|PM^\dagger MP|\psi\rangle \\ &= \lambda(M^\dagger M)\|\psi\|^2 \\ &= 0. \end{aligned}$$

Thus for any $N \in \mathcal{N}$, $\psi \in \mathcal{C}$ we have

$$\begin{aligned} \sum_{j=1}^{k+1} R_j N|\psi\rangle\langle\psi|N^\dagger R_j^\dagger &= \sum_{j=1}^{k} R_j N|\psi\rangle\langle\psi|N^\dagger R_j^\dagger \\ &= \sum_{j=1}^{k} PN_j^\dagger NP|\psi\rangle\langle\psi|PN_j^\dagger N_j P \\ &= \left(\sum_{j=1}^{k} |\langle [N_j] | [N] \rangle|^2 \right) |\psi\rangle\langle\psi| \end{aligned}$$

which, at once, implies that the decoding operation

$$\mathbf{R}(\rho) = \sum_{j=1}^{k+1} R_j \rho R_j^\dagger \quad \forall \text{ state } \rho \tag{2.4}$$

makes the pair $(\mathcal{C}, \mathbf{R})$ a quantum $\mathcal{N}$-correcting code. $\square$

We shall now adopt the notations of Theorem 2.3 and its proof and construct a quantum gate, i.e., a unitary operator in the tensor product $\mathcal{H} \otimes \left(\widetilde{\mathcal{N}} \oplus \mathbb{C}\right)$ which will recover any state with support in $\mathcal{C}$ by pushing the effect of any noise from $\mathcal{N}$ into the ancillary Hilbert space $\widetilde{N} \oplus \mathbb{C}$. To this end we consider the orthonormal basis $\{[N_1], [N_2], \ldots, [N_k], 1\}$ for the enlarged Hilbert space $\widetilde{N} \oplus \mathbb{C}$ of dimension $k+1$ and express any operator Z in $\mathcal{H} \otimes \left(\widetilde{\mathcal{N}} \oplus \mathbb{C}\right)$ as a matrix

$$Z = ((Z_{ij})), i, j \in \{1, 2, \ldots, k+1\}$$

of operators in $\mathcal{H}$ with respect to this basis. We now introduce the operator U in $\mathcal{H} \otimes \left(\widetilde{\mathcal{N}} \oplus \mathbb{C}\right)$

$$U = ((U_{ij})), i, j \in \{1, 2, \ldots, k+1\} \tag{2.5}$$

where

$$U_{ij} = \begin{cases} N_j P N_i^\dagger & \text{if} \quad i, j \in \{1, 2, \ldots, k\} \text{ and } i + j \neq k+2, \\ Q & \text{if} \quad i, j \in \{1, 2, \ldots, k\} \text{ and } i + j = k+2 \end{cases} \tag{2.6}$$

and

$$U_{i\,k+1} = U_{k+1i}^\dagger = \begin{cases} Q & \text{if} \quad i = 1, \\ N_{k+2-i} P N_i^\dagger & \text{if} \quad 2 \leq i \leq k, \\ N_1 P N_1^\dagger & \text{if} \quad i = k+1. \end{cases} \tag{2.7}$$

Then we have

Proposition 2.4 The operator U defined by equations (2.5)-(2.7) in $\mathcal{H} \otimes \left(\widetilde{\mathcal{N}} \oplus \mathbb{C}\right)$is self-adjoint and unitary. In particular, $U^2 = I$.

Proof The selfadjointness of U follows from its very definition and the fact that $U^2 = I$ follows from matrix multiplication using the orthonormality of the elements $[N_i]$, $1 \leq j \leq k$ in $\widetilde{N}$ and the definition of Q. $\square$

Proposition 2.5 Let $I \in \mathcal{N}$ and let the orthonormal basis $\{[N_1], [N_2], \ldots, [N_k], 1\}$ in $\widetilde{\mathcal{N}} \oplus \mathbb{C}$ be such that $N_1 = I$. Define $|\Omega\rangle = [I]$. Then the unitary operator U in Proposition 2.4 satisfies the following relations :

$$U\,|\psi\rangle|\Omega\rangle = ((U_{ij})) \begin{bmatrix} |\psi\rangle \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} P|\psi\rangle \\ PN_2^\dagger|\psi\rangle \\ \vdots \\ PN_k^\dagger|\psi\rangle \\ Q|\psi\rangle \end{bmatrix} \quad \forall \quad |\psi\rangle \in \mathcal{H}$$

and

$$UN|\psi\rangle|\Omega\rangle = |\psi\rangle|\Omega_N\rangle \quad \forall \quad |\psi\rangle \in \mathcal{C}$$

where

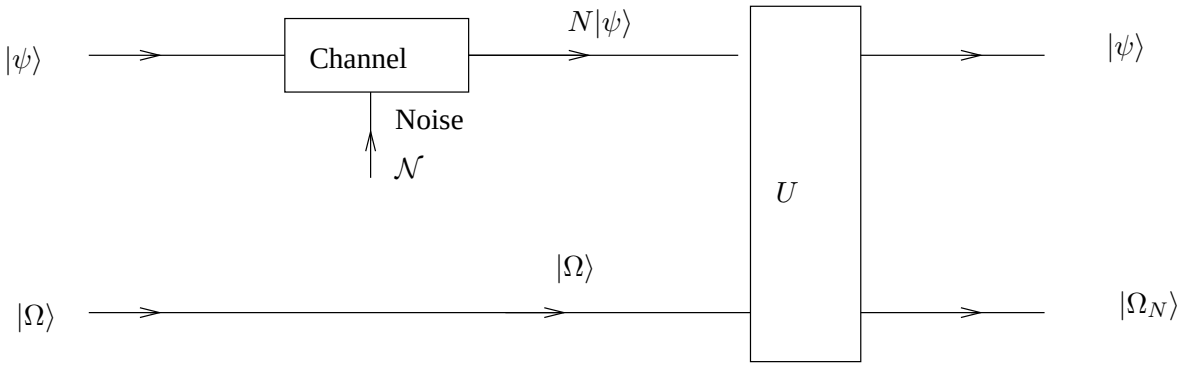
$$|\Omega_N\rangle = \left[\lambda(N), \lambda(N_2^\dagger N), \ldots, \lambda(N_k^\dagger N), 0\right]^T.$$

In particular, the decoding operator $\mathbf{R}$ given by (2.3) and (2.4) satisfies the relation

$$\mathbf{R}(\rho) = \mathrm{Tr}_2\, U\,(\rho \otimes |\Omega\rangle\langle\Omega|)\, U^\dagger \quad \text{for any state } \rho \text{ in } \mathcal{H}.$$

Proof This is immediate from the definition of U and the fact that $N_1 = I$. Note that $\lambda(N) = \lambda(I^\dagger N)$ and $Q\,|\psi\rangle = 0$ when $|\psi\rangle \in \mathcal{C}$. □

Remark The implementation of decoding by the unitary operator U in the tensor product of $\mathcal{H}$ and the ancillary Hilbert space $\widetilde{\mathcal{N}} \oplus \mathbb{C}$ is neatly expressed in the pictorial form of quantum circuits as follows : for any $|\psi\rangle \in \mathcal{C}$



The first wire indicates $\mathcal{H}$, the second indicates the ancillary Hilbert space $\widetilde{\mathcal{N}} \oplus \mathbb{C}$, the two parallel wires their tensor product, the input is $|\psi\rangle|\Omega\rangle$ and the final output after passage through the channel and the application of the quantum gate U is $|\psi\rangle|\Omega_N\rangle$ provided $|\psi\rangle$ is from the $\mathcal{N}$-correcting quantum code $\mathcal{C}$.

In view of this result we emphasize the importance of finding a convenient orthonormal basis of the Hilbert space $\widetilde{N}$ derived from the noise space $\mathcal{N}$ and the quantum $\mathcal{N}$-correcting code $\mathcal{C}$ in the Knill-Laflamme theorem.

3 Classical error correcting codes in the quantum language and their quantization

Let A be a finite set, usually called an *alphabet* in classical information theory. Any element of A may also be called a letter. An element x of A is transmitted through a noisy channel and the output y may differ from x. We may view A as an additive abelian group with null element 0 and say that $y = x + (y - x)$ where a noise element $n = y - x$ has been added to the input. Suppose the noise element n comes from a subset $N \subset A$ with the cardinality of N being 'small' compared to the cardinality of A. Let $C \subset A$ be a subset such that $C \cap (C + N) = \emptyset$. If an element $c \in C$ is transmitted through the channel then the output belongs to $c + N$ and

therefore does not belong to C. In other words, if only letters from C are communicated through the channel one can say that a noise element from N has been added to the input whenever the output lies outside C. We say that C is an N-detecting code. Thus C is an *N-detecting code* if

$$(C - C) \cap N = \emptyset. \tag{3.1}$$

Suppose $C = \{c_1, c_2, \ldots, c_k\}$ and for any $i \neq j$ the subsets $c_i + N$ and $c_j + N$ are disjoint. If elements from C alone are used as inputs for the channel then the output belongs to $c_i + N$ if and only if the input letter is c_i. Thus, from the output, we can decode the correct input if the only noise is addition of letters from N to any input from C. We say that C is an *$\mathcal{N}$-correcting classical code.* Thus C is an N-correcting classical code if

$$(C - C) \cap (N - N) = \{0\}. \tag{3.2}$$

In particular, if C is an M-detecting code and N satisfies the relation $N - N \subset M \cup \{0\}$ then C is an N-correcting code.

Now consider the Hilbert space $\mathcal{H} = L^2(A)$ with respect to the counting measure on A. Then equation (3.1) can be expressed as

$$1_C \, 1_{C+n} = 0 \quad \forall \quad n \in N, \tag{3.3}$$

1_B denoting the indicator of $B \subset A$, where as (3.2) can be expressed as

$$1_{C+n_1} 1_{C+n_2} = 0 \text{ if } n_1, n_2 \in N, n_1 \neq n_2. \tag{3.4}$$

If $a \to U_a$ is the regular representation of A and $P(C)$ denotes the projection operator of multiplication by 1_C then (3.3) can be expressed as

$$P(C)U_nP(C) = \begin{cases} 0 & \forall \quad n \in N, \\ P(C) & \text{if} \quad n = 0 \end{cases} \tag{3.5}$$

where as (3.4) can be expressed as

$$P(C)U_{n_1}^{\dagger}U_{n_2}P(C) = \begin{cases} 0 & \text{if} \quad n_1, n_2 \in N, n_1 \neq n_2, \\ P(C) & \text{if} \quad n_1 = n_2. \end{cases}$$

Let now $\mathcal{N}$ denote the linear span of $\{U_n | n \in N\}$ in $\mathcal{B}(\mathcal{H})$. If C is a classical N-correcting code then $P(C)$ is an $\mathcal{N}$-correcting quantum code, thanks to the Knill-Laflamme theorem.

Following (3.5) we now introduce a definition. If $\mathcal{H}$ is a Hilbert space and $\mathcal{N} \subset \mathcal{B}(\mathcal{H})$ is a linear subspace we say that a projection P is a quantum *$\mathcal{N}$-detecting code* if

$$PNP = \lambda(N)P \quad \forall \; N \in \mathcal{N}$$

for some linear function $\lambda : \mathcal{N} \to \mathbb{C}$ satisfying $\lambda(N^{\dagger}) = \overline{\lambda(N)}$ whenever N and $N^{\dagger}$ belong to $\mathcal{N}$. Without loss of generality we may assume that $I \in \mathcal{N}$ and $\mathcal{N}$ is closed under the adjoint

operation. If $\mathcal{E} \subset \mathcal{B}(\mathcal{H})$ is a subspace such that $\mathcal{E}^\dagger\mathcal{E} \subset \mathcal{N}$ and P is a quantum $\mathcal{N}$-detecting code then P is a quantum $\mathcal{E}$-correcting code.

In order to 'quantize' the classical picture of error correcting codes described above we enlarge the regular representation $a \to U_a$ of A to the projective Weyl representation for $A \times A$. This would enable us to tackle both translation and phase errors of quantum noise. To this end we choose and fix a symmetric nondegenerate bicharacter for A, i.e., a function $\langle x, y\rangle$, $x, y \in A$ satisfying the following:

(1) $|\langle x, y\rangle| = 1, \langle x, y\rangle = \langle y, x\rangle \quad \forall\ x, y \in A,$

(2) $\langle x, y_1 + y_2\rangle = \langle x, y_1\rangle\ \langle x, y_2\rangle \quad \forall\ x, y_1, y_2 \in A,$

(3) $\langle x, y\rangle = 1 \quad \forall\ y \in A$ if and only if $x = 0$.

Such a bicharacter always exists. For any a in A denote by $|a\rangle$ the indicator function $1_{\{a\}}$ of the singleton $\{a\}$. Then $\{|a\rangle, a \in A\}$ is a canonical orthonormal basis for $\mathcal{H}$. It is important to distinguish the scalar product $\langle a|b\rangle$ (in Dirac notation) and the symmetric bicharacter $\langle a, b\rangle$. Now we introduce the unitary operators U_a, V_a determined uniquely by the relations

$$\begin{aligned} U_a|x\rangle &= |x + a\rangle, \\ V_a|x\rangle &= \langle a, x\rangle\ |x\rangle \end{aligned}$$

for all x in A. Then we have the relations

$$U_aU_b = U_{a+b}, V_aV_b = V_{a+b}, V_bU_a = \langle a, b\rangle U_aV_b$$

for all a, b in A. These constitute the *Weyl commutation relations* for the group A. Introduce the Weyl operators

$$W(a, b) = U_aV_b, (a, b) \in A \times A.$$

Then

$$\begin{aligned} W(a, b)W(a', b') &= \langle b, a'\rangle W(a + a', b + b'), \\ W(a, b)W(x, y)W(a, b)^\dagger &= \langle b, x\rangle\overline{\langle a, y\rangle}W(x, y) \end{aligned}$$

for all a, a', b, b', x, y in A. We shall view $\mathcal{B}(\mathcal{H})$ as a Hilbert space with the scalar product $\langle X|Y\rangle = \text{tr}\, X^\dagger Y$ between any two elements X, Y in $\mathcal{B}(\mathcal{H})$. Since

$$\text{tr}\ W(x, y) = \begin{cases} 0 & \text{if } (x, y) \neq (0, 0) \\ \#A & \text{otherwise} \end{cases}$$

it follows that $\{(\#A)^{-1/2}W(x, y), (x, y) \in A \times A\}$ is an orthonormal basis for $\mathcal{B}(\mathcal{H})$ and any element X in $\mathcal{B}(\mathcal{H})$ admits a Fourier expansion

$$X = (\#A)^{-1} \sum_{x,y \in A} \langle W(x, y)|X\rangle W(x, y).$$

In particular $(x,y) \to W(x,y)$ is a projective and irreducible unitary representation for $A \times A$.

If A, B are two finite abelian groups with nondegenerate symmetric bicharacters $\langle .,. \rangle_A$, $\langle .,. \rangle_B$ respectively then for the cartesian product $A \times B$ the definition

$$\langle (a_1,b_1),(a_2,b_2) \rangle = \langle a_1,a_2 \rangle_A \langle b_1,b_2 \rangle_B \quad \forall \ a_1,a_2 \in A, b_1,b_2 \in B$$

determines a nondegenerate symmetric bicharacter and

$$W\left((a_1,b_1),(a_2,b_2)\right) = W(a_1,a_2) \otimes W(b_1,b_2), (a_i,b_i) \in A \times B, i = 1,2,$$

determines the Weyl operators for $A \times B$ where $L^2(A \times B)$ is naturally identified with $L^2(A) \otimes L^2(B)$. We shall use all these basic properties of the Weyl operators in the quantization of classical error correcting codes.

In section 2 we have seen that $\mathcal{N}$-correcting quantum codes are described by projections obeying the Knill-Laflamme property (2.2). Projections can be viewed as averages of group representations. For a given projection of this kind we can describe the errors that it can correct in the role of a quantum code. Keeping this intuitive approach in view we introduce the notion of a *Gottesman subgroup* of $A \times A$. A subgroup $S \subset A \times A$ is called a *Gottesman subgroup* if for any $(a,b),(a',b')$ in S one has $\langle a,b' \rangle = \langle b,a' \rangle$. For such a subgroup the Weyl operators $W(a,b)$ and $W(a',b')$ commute. Since we can simultaneously diagonalise the family $\{W(a,b),(a,b) \in S\}$ we can express these operators as

$$W(a,b) = \text{ diag } \left(\lambda_1(a,b), \lambda_2(a,b), \ldots\right), (a,b) \in S$$

in an orthonormal basis and therefore

$$\lambda_1(a,b)\lambda_1(a',b') = \langle b,a' \rangle \lambda_1(a+a', b+b') \quad \forall \ (a,b),(a',b') \in S.$$

Hence the map $(a,b) \to \overline{\lambda_1(a,b)} W(a,b)$ is a unitary representation of the subgroup S. We summarise this property in a convenient form.

Proposition 3.1 Let $S \subset A \times A$ be a Gottesman subgroup. Then there exists a scalar valued function φ on S of modulus unity such that for any character χ of the subgroup S the map

$$(a,b) \to \varphi(a,b)\chi(a,b)W(a,b), \quad (a,b) \in S$$

is a unitary representation of S.

Proof. Immediate. □

Given a Gottesman subgroup S and a character χ of S we define the projection

$$P^S(\{\chi\}) = \frac{1}{\#S} \sum_{(a,b) \in S} \varphi(a,b)\chi(a,b)W(a,b) \tag{3.6}$$

where φ is as in Proposition 3.1. Let $\hat{S}$ denote the dual group of all characters of S. Then the Schur orthogonality relations for characters implies that $\{P^S(\{\chi\}), \chi \in \hat{S}\}$ is a resolution of

the identity in $\mathcal{H}$ into orthogonal projections. For any $F \subset \hat{S}$ define the projection

$$P^S(F) = \sum_{\chi \in F} P^S(\{\chi\}). \tag{3.7}$$

We shall now describe a noise space $\mathcal{N} \subset \mathcal{B}(\mathcal{H})$ for which $P^S(F)$ is a quantum $\mathcal{N}$-detecting code. To this end we define a homomorphism $\gamma : A \times A \to \hat{S}$ by putting

$$\gamma(x,y)(a,b) = \langle a, y\rangle\overline{\langle b, x\rangle} \quad \forall\ (a,b) \in S. \tag{3.8}$$

Proposition 3.2 For any $\chi_1, \chi_2 \in \hat{S}$ and $(x,y) \in A \times A$ the following holds :

$$P^S(\{\chi_1\})W(x,y)P^S(\{\chi_2\}) = \begin{cases} 0 & \text{if } \gamma(x,y) \neq \chi_1\overline{\chi}_2, \\ (\overline{\chi_2\varphi})(x,y)P^S(\{\chi_2\}) & \text{if } (x,y) \in S, \\ W(x,y)P^S(\{\chi_2\}) & \text{otherwise.} \end{cases}$$

Proof This is straightforward algebra using (3.6), (3.8) and the orthogonality relations for characters. □

Theorem 3.3 (V. Arvind, P. Kurur and K. R. Parthasarathy [2]) Let $F \subset \hat{S}$. Then

$$P^S(F)W(x,y)P^S(F) = \begin{cases} 0 & \text{if } (x,y) \notin \gamma^{-1}(F\overline{F}), \\ \overline{\chi\varphi}(x,y)P^S(F) & \text{if } (x,y) \in S \text{ and } \chi(x,y) \\ & \text{ is independent of } \chi \text{ for } \chi \in F, \\ W(x,y)P^S(F \cap F\gamma(x,y)) & \text{otherwise.} \end{cases}$$

Proof This is immediate from the expansion of the left hand side and Proposition 3.2. □

Remark Let $\mathcal{N}$ denote the linear span of

$$\left\{ W(x,y) |\, (x,y) \notin \gamma^{-1}(F\overline{F}) \text{ or } (x,y) \in S \text{ and } \chi(x,y) \text{ is independent of } \chi \in F \right\}.$$

where γ is the homorphism from $A \times A$ into $\hat{S}$ defined by (3.8). Then it follows from Theorem 3.3 that $P^S(F)$ is a quantum $\mathcal{N}$-detecting code.

Corollary 3.4 (Gottesman [4], Calderbank et al [3]) Let

$$\mathcal{N} = \text{ linear span } \left\{ W(x,y) |\, (x,y) \in (S^\perp)' \cup S \right\}$$

where $S^\perp = \gamma^{-1}(\{1\})$, prime $'$ denotes complement and 1 denotes the trivial character. Then $P^S(\{1\})$ is a quantum $\mathcal{N}$-detecting code. If $E \subset A \times A$ satisfies the relation

$$E - E \subset (S^\perp)' \cup S$$

and

$$\mathcal{E} = \text{ linear span } \{W(x,y) | (x,y) \in E\}$$

then $P^S(\{1\})$ is a quantum $\mathcal{E}$-correcting code.

Proof. In Theorem 3.3 choose $F = \{1\}$ the singleton consisting of the trivial character. Then $\gamma^{-1}(F\overline{F}) = S^\perp$. If $(x,y) \in (S^\perp)'$ then $P^S(\{1\})W(x,y)P^S(\{1\}) = 0$. If $(x,y) \in S$ we have $P^S(\{1\})W(x,y)P^S(\{1\}) = \overline{\varphi(x,y)}P^S(\{1\})$. Thus $P^S(\{1\})$ is a quantum $\mathcal{N}$-detecting code. If $(x_1,y_1),(x_2,y_2)$ are in E then $W(x_1,y_1)^\dagger\ W(x_2,y_2)$ is a scalar multiple of $W(x_2-x_1,y_2-y_1)$ and $(x_2-x_1,y_2-y_1) \in E-E \subset (S^\perp)' \cup S$. Thus $P^S(\{1\})W(x_1,y_1)^\dagger W(x_2,y_2)P^S(\{1\})$ is a scalar multiple of $P^S(\{1\})$. Hence by the Knill-Laflamme theorem $P^S(\{1\})$ is a quantum $\mathcal{N}$-correcting code. □

Proposition 3.5 Let $S \subset A \times A$ be a Gottesman subgroup and let C be a cross section for the canonical homomorphism from $A \times A$ onto $A \times A/S^\perp$ so that C meets each coset of $S^\perp$ exactly in one point. Define $E = S + C$. Then $E - E \subset (S^\perp)' \cup S$.

Conversely, if $F \subset A \times A$ satisfies the condition $F - F \subset (S^\perp)' \cup S$ then there exists a cross section C as above such that $F \subset S + C$.

Proof If $(x,y) \in E - E$ then

$$(x,y) = (a,b) + (x_1,y_1) - (a',b') - (x_2,y_2)$$

where $(a,b),(a',b') \in S$ whereas $(x_i,y_i) \in C$ for $i = 1,2$. If $(x_1,y_1) = (x_2,y_2)$ then $(x,y) \in S$. If $(x_1,y_1) \neq (x_2,y_2)$ then $(x,y) \in S + (x_1-x_2,y_1-y_2)$ and by the definition of γ, $S^\perp$ and C, $\gamma(x_1,y_1) \neq \gamma(x_2,y_2)$. Thus $(x,y) \notin S^\perp$. This proves the first part.

To prove the second part, first assume that $(0,0) \in F$. Then $F = F - (0,0) \subset (S^\perp)' \cup S$. Write $F = (F \cap S) \cup G$ where $G \subset (S^\perp)'$. Choose and fix a coset decomposition of $A \times A$ with respect to $S^\perp$:

$$A \times A = S^\perp \cup S^\perp + (x_1,y_1) \cup \ldots \cup S^\perp + (x_m,y_m).$$

Then

$$G = \bigcup_{j=1}^{m} G \cap \left(S^\perp + (x_j,y_j)\right).$$

Let $G \cap \left(S^\perp + (x_j,y_j)\right) \neq \emptyset$. Consider two points in this set of the form $(a,b)+(x_j,y_j),(a',b')+(x_j,y_j)$ where $(a,b),(a',b') \in S^\perp$. Then their difference $(a-a',b-b') \in S^\perp$ and $(S^\perp)' \cup S$. Thus $(a-a',b-b') \in S$. If we fix a point $(a_0,b_0)+(x_j,y_j)$ in $G \cap \left(S^\perp + (x_j,y_j)\right)$ then any other point in it is of the form

$$\begin{aligned}(a,b)+(x_j,y_j) &= (a_0,b_0)+(a-a_0,b-b_0)+(x_j,y_j)\\ &\in S+(a_0,b_0)+(x_j,y_j)\\ &= S+(x_j',y_j')\end{aligned}$$

where

$$S^\perp + (x_j',y_j') = S^\perp + (x_j,y_j).$$

Thus G can be expressed as

$$G = \bigcup_{j=1}^{m} G \cap (S + (x_j',y_j'))$$

where

$$A \times A = \bigcup_{j=0}^{m} \left(S^{\perp} + (x'_j, y'_j) \right)$$

is another $S^{\perp}$-coset decomposition of $A \times A$ with $(x'_0, y'_0) = (0,0)$. Choose $(x'_j, y'_j) = (x_j, y_j)$ if $G \cap \left(S^{\perp} + (x_j, y_j) \right) = \emptyset$. Clearly,

$$F \subset S + \left\{ (x'_j, y'_j), 0 \leq j \leq m \right\}.$$

If $(0,0) \notin F$ then a translate F_1 of F contains $(0,0)$ with F_1 satisfying the required properties. Then $F \subset S + C_1$ for a different cross section C_1. $\square$

Codes of the form $P^S(\{1\})$ in Corollary 3.4 are called *quantum stabilizer codes* since vectors in such a code are fixed by the operators in the representation $(a,b) \to \varphi(a,b)W(a,b)$ of the Gottesman group S. Corollary 3.4 describes a set of errors which such codes can detect or correct. In this context it is useful to construct an orthonormal basis for the ancillary Hilbert space in the decoding operation of Proposition 2.5 applied to a quantum stabilizer code.

Theorem 3.6 Let $S, S^{\perp}$ and $P^S(\{1\})$ be as in Corollary 3.4. Suppose $(0,0) \in C \subset A \times A$ is a subset such that

$$A \times A = \bigcup_{(x,y) \in C} \left(S^{\perp} + (x,y) \right)$$

is an $S^{\perp}$-coset partition of $A \times A$ and

$$\mathcal{N} = \text{ linear span } \{ W(a+x, b+y), (a,b) \in S, (x,y) \in C \}.$$

Then $I \in \mathcal{N}$, $P^S(\{1\})$ is a quantum $\mathcal{N}$-correcting code and the set $\{[W(x,y)], (x,y) \in C\} \cup \{1\}$ is an orthonormal basis for the ancillary Hilbert space $\widetilde{\mathcal{N}} \oplus \mathbb{C}$ in Proposition 2.5.

Proof Only the last part remains to be proved. To this end let $(x,y) \in C$, $(a,b) \in S$. We claim that $[W(x+a, y+b) - \alpha W(x,y)] = 0$ for some scalar α of modulus unity. Indeed,

$$\begin{aligned} & P^S(\{1\}) \{W(x+a,y+b) - \alpha W(x,y)\}^{\dagger} \{W(x+a,y+b) - \alpha W(x,y)\} P^S(\{1\}) \\ = \; & P^S(\{1\}) \left(2I - \alpha W(x+a,y+b)^{\dagger} W(x,y) - \overline{\alpha} W(x,y)^{\dagger} W(x+a,y+b) \right) P^S(\{1\}) \end{aligned} \tag{3.9}$$

But $W(x+a,y+b)^{\dagger} W(x,y) = \lambda W(a,b)^{\dagger}$ for some scalar λ of modulus unity where the operator $\varphi(a,b)W(a,b)$ with $\varphi(a,b)$ as in (3.6) fixes every vector in the range of $P^S(\{1\})$. Thus right hand side of (3.9) is equal to $\{2 - \alpha\lambda\overline{\varphi(a,b)} - \overline{\alpha}\overline{\lambda}\varphi(a,b)\} P^S(\{1\})$. Choosing $\alpha = \overline{\lambda}\varphi(a,b)$ proves the claim. Now, if $(x,y), (x',y')$ are two distinct elements of C and (a,b), (a',b') are in S then $(x+a, y+b) - (x'+a', y'+b') \notin S^{\perp}$ and therefore, as in the proof of Corollary 3.4,

$$P^S(\{1\}) W(x+a, y+b)^{\dagger} W(x'+a', y'+b') P^S(\{1\}) = 0.$$

This completes the proof. $\square$

4 The standard model of noise

Let $\mathcal{H}$ be a finite dimensional Hilbert space and $\mathcal{H}^{\otimes^n}$ be its n-fold tensor product. For any integer $1 \leq t \leq n$ let $\mathcal{N}_t \subset \mathcal{B}(\mathcal{H}^{\otimes^n})$ be the subspace spanned by all operators of the form $X_1 \otimes X_2 \otimes \cdots \otimes X_n$ where the X_j's are operators in $\mathcal{H}$ and $\#\{i|X_i \neq I, 1 \leq i \leq n\} \leq t$. Any element of $\mathcal{N}_t$ is said to have *weight* not exceeding t. Thus elements of $\mathcal{N}_t \backslash \mathcal{N}_{t-1}$ are said to have weight equal to t. A quantum $\mathcal{N}_t$-correcting code is called a *t-error correcting code* of *length n*. A projection P in $\mathcal{H}^{\otimes^n}$ is called a quantum code of minimum distance $\geq d$ if

$$PNP = \lambda(N)P \quad \forall \quad N \in \mathcal{N}_{d-1}$$

where $\lambda(N)$ denotes a scalar depending on N. If, in addition, for some N in $\mathcal{N}_d$, PNP is not a scalar multiple of P we say that the quantum code P has *minimum distance d*. A projection P in $\mathcal{H}^{\otimes^n}$ of minimum distance d with $\operatorname{tr} P = k$ is called an (n, k, d) quantum code where k is called its *size*. The very definition raises some natural and difficult optimality problems of a combinatorial character. For given n, k what is the maximum possible value of d for which an (n, k, d) quantum code exists? For given values of n, d what is the maximum possible value of k? For given values of k, d what is the minimum possible value for n?

If X, Y are operators in $\mathcal{H}^{\otimes^n}$ with weight $\leq t$ then it is clear that $X^\dagger Y$ has weight $\leq 2t$. $\mathcal{N}_t$ is also closed under the adjoint operation and $I \in \mathcal{N}_t$. In particular any (n, k, d) quantum code is also a $\lfloor \frac{d-1}{2} \rfloor$-error correcting code.

We may identify $\mathcal{H}$ with $L^2(A)$ where A is a fixed finite additive abelian group with null element 0 and cardinality equal to the dimension of $\mathcal{H}$. Then $\mathcal{H}^{\otimes^n}$ can be identified with $L^2(A^n)$. Choose and fix a unitary orthogonal basis of Weyl operators $\{W(x, y), (x, y) \in A \times A\}$ for the Hilbert space $\mathcal{B}(\mathcal{H})$ and construct the product Weyl operator basis $\{W(\mathbf{x}, \mathbf{y}), (\mathbf{x}, \mathbf{y}) \in A^n \times A^n\}$ for $\mathcal{B}(\mathcal{H}^{\otimes^n})$ so that $W(\mathbf{x}, \mathbf{y}) = W(x_1, y_1) \otimes W(x_2, y_2) \otimes \ldots \otimes W(x_n, y_n)$ where $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ with $x_i, y_i \in A$ for each i. From the discussions in the beginning of Section 3 it is clear that the set

$$\{W(\mathbf{x}, \mathbf{y}) | \#\{i : (x_i, y_i) \neq (0, 0), 1 \leq i \leq n\} \leq t\}$$

is an orthogonal basis for the subspace $\mathcal{N}_t$ in $\mathcal{B}(\mathcal{H})$. In view of this property we say that an element $(\mathbf{x}, \mathbf{y})$ in $A^n \times A^n$ has weight t if $\#\{i : (x_i, y_i) \neq (0, 0),\ 1 \leq i \leq n\} = t$. Then we have the following :

Proposition 4.1 A projection P in $\mathcal{H}^{\otimes^n}$ is a quantum code of minimum distance d if and only if

$$PW(\mathbf{x}, \mathbf{y})P = \lambda(\mathbf{x}, \mathbf{y})P$$

for all $(\mathbf{x}, \mathbf{y})$ in $A^n \times A^n$ with weight $< d$. In such a case P is a $\lfloor \frac{d-1}{2} \rfloor$-error correcting quantum code.

We say that a subset $E \subset A^n \times A^n$ has minimum Hamming distance $\geq d$ if for any two distinct points $(\mathbf{x}, \mathbf{y})$, $(\mathbf{x}', \mathbf{y}')$ in E the weight of $(\mathbf{x} - \mathbf{x}', \mathbf{y} - \mathbf{y}')$ is not less than d. With

this definition we have the following fundamental theorem by combining Proposition 4.1 and Corollary 3.4.

Theorem 4.2 Let S be a Gottesman subgroup of $A^n \times A^n$ and let $S^\perp$ be the kernel of the homomorphism $\gamma : A^n \times A^n \to \hat{S}$ defined by (3.8). Then the quantum stabilizer code $P^S(\{1\})$ defined by (3.6) has minimum distance $\geq d$ if the set $S^\perp \backslash S \subset A^n \times A^n$ has minimum Hamming distance $\geq d$.

Proof Immediate. □

Remark Recall that tr $P^S(\{1\}) = (\#A)^n/\#S$ is the size and n is the length of the code in Theorem 4.2. If the minimum Hamming distance of $S^\perp \backslash S$ is d then $P^S(\{1\})$ is a (n, k, d) quantum code with $k = (\#A)^n/\#S$.

There is a considerable amount of recent literature on the search for Gottesman subgroups $S \subset A^n \times A^n$ for which every element in $S^\perp \backslash S$ has weight $\geq d$. Examples of such S can be constructed when A is the additive group of a finite field and the theory of classical error correcting codes is put to use. See for example [3], [9]. Such a discussion is beyond the scope of the present exposition. We conclude with an example of a single error correcting code of minimum distance 3 which exhibits an interesting entanglement property. To this end consider an automorphism τ of the abelian group A. Define

$$S_0 = \{(x, \tau(x) + \tau^{-1}(x)), x \in A\}$$

and assume that τ preserves the symmetric bicharacter $\langle ., . \rangle$ on $A \times A$. Let

$$\widetilde{W}(x) = \langle x, \tau(x) \rangle W(x, \tau(x) + \tau^{-1}(x)).$$

Then the map $x \to \widetilde{W}(x)$ is a representation of A. Suppose h is a homomorphism from A into another abelian group satisfying $h(x) = h(\tau(x)) \forall\, x \in A$. Then $S = \{(x, \tau(x) + \tau^{-1}(x)) | x \in A, h(x) = 0\}$ is a Gottesman subgroup. By Corollary 3.4 the projection

$$P^S = \sum_{x:h(x)=0} \langle x, \tau(x) \rangle, W\left(x, \tau(x) + \tau^{-1}(x)\right)$$

is a quantum stabilizer code satisfying

$$P^S W(x, y) P^S = \begin{cases} 0 & \text{if } \gamma(x, y) \neq 1, \\ \overline{\langle x, \tau(x) \rangle} P^S & \text{if } (x, y) \in S \end{cases}$$

where γ is defined by (3.8). If $E = S + C$ where C is a cross section for the canonical homomorphism $A \times A \to A \times A/S^\perp$ then P^S is an $\mathcal{N}$-correcting quantum code where $\mathcal{N}$ is the linear span of $\{W(x, y) | (x, y) \in E\}$.

Now we choose $A = B^5$ where B is an additive abelian group, $\tau(\mathbf{b}) = \sigma^2(\mathbf{b}), \mathbf{b} \in A$ where $\sigma(\mathbf{b}) = \sigma(b_0, b_1, b_2, b_3, b_4) = (b_1, b_2, b_3, b_4, b_0)$ is the backward cyclic permutation in B^5 and $h(\mathbf{b}) = b_0 + b_1 + b_2 + b_3 + b_4$. Then

$$S = \left\{(\mathbf{x}, \mathbf{y}) | \mathbf{y} = \tau(\mathbf{x}) + \tau^{-1}(\mathbf{x}), h(\mathbf{x}) = 0\right\} \subset B^5 \times B^5$$

and

$$\begin{aligned} S^{\perp} &= \left\{ (\mathbf{x},\mathbf{y}) |\, h\left(\mathbf{y} - \sigma^2(\mathbf{x}) - \sigma^{-2}(\mathbf{x})\right) = 0 \right\} \\ &= \left\{ (\mathbf{x},\mathbf{y}) \;\middle|\; \begin{array}{l} y_0 = z + x_2 + x_3, y_1 = z + x_3 + x_4, y_2 = z + x_0 + x_4 \\ y_3 = z + x_0 + x_1, y_4 = z + x_1 + x_2 \text{ for some } \; z \in B \end{array} \right\}. \end{aligned}$$

A simple analysis using the cyclic permutation symmetry of the construction shows that every element in $S^{\perp} \backslash S$ has weight 3. In other words P^S is a single error correcting code. When $B = \mathbb{Z}_2 = \{0, 1\}$ this example was arrived at by Laflamme by a computer search. P^S is a $(5, \#B, 3)$ quantum code for any B. It is an interesting fact that for any $\mathcal{H}$, a $(4, 2, 3)$ quantum code does not exist. More generally, for any $\mathcal{H}$ a $(4k, 2, 2k + 1)$ quantum code does not exist. In other words in any $\mathcal{H}^{\otimes 4k}$ it is not possible to have a k error correcting quantum code of size 2.

Going back to the projection P^S defined as above in $\mathcal{H}^{\otimes 5}$ with $\mathcal{H} = L^2(B)$ consider a pure state $|\psi\rangle\langle\psi|$ with $P^S|\psi\rangle = |\psi\rangle$. Let $\mathcal{H}^{\otimes 5} = \mathcal{H}_1 \otimes \mathcal{H}_2$ where $\mathcal{H}_1 = \mathcal{H}^{\otimes 2}$, $\mathcal{H}_2 = \mathcal{H}^{\otimes 3}$ where $\mathcal{H}$ denotes any one of the five copies of $\mathcal{H}$ in $\mathcal{H}^{\otimes 5}$. Then

$$\mathrm{Tr}_{\mathcal{H}_2} |\psi\rangle\langle\psi| = (\#B)^{-2} I \text{ in } \mathcal{H}_1.$$

In other words any pure state in the range of P^S is maximally entangled in every factorization of $\mathcal{H}^{\otimes 5}$ into $\mathcal{H}_1 \otimes \mathcal{H}_2$. It should be interesting to investigate subspaces of $\mathcal{H}^{\otimes n}$ where every state exhibits such a perfect entanglement. See [8].

References

[1] V. Arvind, K.R.Parthasarathy, 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.Lakshmibhai et al,Hindustan Book Agency,New Delhi,133-153 (2003).

[2] V. Arvind, P. Kurur and K. R. Parthasarathy, Nonstabilizer quantum codes from abelian subgroups of the error group, in Quantum Information, Statistics, Probability, Dedicated to Alexander Holevo on the occassion of his 60th birthday, (ed. O. Hirota) Rinton Press Inc. (2004) 1-29.

[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 44 (4); 1369-1387, 1998.

[4] D. Gottesman, Stabilizer Codes and Quantum Error Correction. Ph.D. Thesis, California Institute of Technology, Pasadena (1997).

[5] E. Knill and R. Laflamme, A theory of quantum error correcting codes, Phys. Rev. A, 55:900, 1997.

[6] M.A.Nielsen, I.L.Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge (2000).

[7] K. R. Parthasarathy, Lectures on Quantum Computation, Quantum Error Correcting Codes and Information Theory, Tata Institute of Fundamental Research, Mumbai, Narosa Publishing House, New Delhi (2006).

[8] K. R. Parthasarathy, Extremality and entanglements of states in coupled quantum systems, in Quantum Computing, Back Action 2006 (Ed. D. Goswami) AIP Conference Proceedings 864, New York (2006) 54-66.

[9] E. M. Rains, Nonbinary quantum codes. IEEE Trans. Inf. Theory 45 (6) : 1827-1832, 1999.