International Electronic Journal of Pure and Applied Mathematics

Volume 9 No. 3 2015, 181-190
ISSN: 1314-0744
url: http://www.e.ijpam.eu
doi: http://dx.doi.org/10.12732/iejpam.v9i3.7

QUANTUM ERROR CORRECTION AND STABILIZER CODES

Artur Elezi

Department of Mathematics and Statistics
American University
4400 Mass Ave NW, Washington DC 20016, USA

Abstract: The goal of this paper is to provide a self contained detailed and rigorous mathematical introduction to some aspects of the quantum error-correcting codes and especially quantum stabilizer codes without venturing much, if at all, into the world of physics. While most of the results presented are not new, it is not easy to extract a precise mathematical formulation of results and to provide their rigorous proofs by reading the vast number of papers in the field, quite a few of which are written by computer scientists or physicists. It is this formulation and proofs - quite a few of of them new - that we present here. The connections between (a) quantum stabilizer codes and classical self-orthogonal codes and (b) between error correction and error detection have been established in details. Techniques from algebra of finite fields as well as representations of finite abelian groups have been employed here.

AMS Subject Classification: 81P70, 81P15, 94B05
Key Words: linear codes, self-orthogonal codes, quantum error-correcting codes, stabilizer codes

1. Introduction

In recent years there has been an explosion of interest in the theory of error-correcting quantum coding theory. Probably the most important class of quantum codes are quantum stabilizer codes - it is frequently said that they are to quantum coding what linear codes are to general codes. General binary quantum stabilizer

Received: July 21, 2014

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 3 (2015)

codes were introduced by Calderbank et. al. (see [3]) and Gottesman (see [7]). In a later paper, Calderbank et. al. connected stabilizer codes to classical self-orthogonal codes (see [4]). Many new good quantum codes have been constructed using this connection. In [5], [6] we use self-orthogonal Goppa codes from Algebraic Geometry to construct certain stabilizer codes from algebraic curves with automorphisms. The construction of nonbinary quantum stabilizer codes was completed by Ashikhmin and Knill (see [1]).

2. Classic and Quantum Codes

In classical binary coding theory, messages are encoded for error correction as a string of 0s and 1s. They are *the only* two states of the classical units of information; we call them *bits*. The string is then transmitted through a noisy communications channel such as a telephone line, radio/satellite communications link, etc. The noise could be lightning, human error, equipment failures etc. The encoding involves sufficient redundancies so that the receiver may detect error occurring during transmission.

Definition 1. A *binary linear code of dimension k and length n* is a k-dimensional $\mathbf{F}_2$-linear subspace C of $\mathbf{F}_2^n$.

The quantity k/n is called *the rate* of the code C.
Various inner products may be considered in $\mathbf{F}_2^n$, the standard one being the Euclidean product:

$$\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + ... + a_k b_k.$$

A linear code C is called *self-orthogonal* relative to an inner product iff $C \subset C^{\perp}$ and *self-dual* iff $C = C^{\perp}$.

In binary quantum coding, the unit of information - called a *qubit* - exists as a superposition of the two classical states. More precisely, a qubit is a linear combination

$$\psi := \alpha \mathbf{0} + \beta \mathbf{1}$$

where α and β are complex numbers satisfying

$$|\alpha|^2 + |\beta|^2 = 1.$$

It is said that *the state space* of a single qubit is the Hilbert space $\mathbf{C}^2$, with the *computational* basis $\mathbf{0} := \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $\mathbf{1} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and the standard Hermitian inner product.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 3 (2015)

Remark 2. One of the principles of quantum computing is that the global phase is not noticeable physically. In down-to-earth terms this means that the qubits ψ and $e^{i\theta}\psi$ will be considered identical for any real number θ.

The Hilbert space $\mathbf{C}^{2^{\otimes n}}$ is the natural state space for the composite/string of n qubits. It is called *the quantum register* of n-qubits. Pure tensors in the quantum register are called **separate** states, the rest are called **entangled** states. The basis $\{\mathbf{0}, \mathbf{1}\}$ of qubits yields a *computational basis* in the quantum register; this basis is indexed by binary n-tuples $\mathbf{a} := a_1a_2...a_n$ via $a_1a_2...a_n \mapsto \mathbf{a}_1 \otimes \mathbf{a}_2 \otimes ... \otimes \mathbf{a}_n$.

Definition 3. *A binary quantum code of length n and size K* is a linear subspace $\mathbf{Q}$ of a quantum register $\mathbf{C}^{2^{\otimes n}}$ of dimension K over $\mathbf{C}$.

One may think of $\mathbf{Q}$ as a a system of $\log_2 K$ qubits, for example the quantum register $\mathbf{C}^{2^{\otimes n}}$ is a quantum code of size 2^n and length $n = \log_2 2^n$. *The rate* of $\mathbf{Q}$ is given by $(\log_2 K)/n$.

3. Quantum Error Group

A quantum circuit is a sequence of *quantum gates*. Each gate may be identified with a unitary transformation. As a single qubit passes through a noisy quantum circuit, a quantum error may occur, thus forcing a change in the qubit. We will think of these quantum errors as linear transformation, i.e. 2x2 matrices. A basis of such transformations consist of the following unitary Pauli matrices:

$$I, \quad \sigma_x := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

This choice of σ_y differs by a factor of i from what one usually sees in the literature. This is a matter of convenience; after all σ_y and $i\sigma_y$ yield the same linear action due to the the global phase principle.

It is easy to see that $\sigma_x^2 = \sigma_z^2 = I$ and $\sigma_x\sigma_z = -\sigma_z\sigma_x = \sigma_y$. It follows that $\mathcal{E}_1 = \{\pm I, \pm\sigma_x, \pm\sigma_y, \pm\sigma_z\}$ is a group, called *the error group for single qubits*. Notice that the matrix σ_x corresponds to the classical bit error $\mathbf{0} \leftrightarrow \mathbf{1}$ while the matrix σ_z corresponds to the phase error $\mathbf{0} \leftrightarrow \mathbf{0},\ \mathbf{1} \leftrightarrow -\mathbf{1}$.

Similarly, the set of tensors

$$\mathcal{E}_n := \{e_1 \otimes e_2 \otimes ... \otimes e_n : \quad (\forall i = 1, 2, ..., n)(e_i \in \mathcal{E}_1)\}$$

forms a group under the component-by-component multiplication, it is called the *error group of a composite system of n qubits*. These are the errors that occur

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 3 (2015)

during a quantum transmission of n qubits. Notice that with the exception of $\pm I$ all matrices in $\mathcal{E}_n$ are traceless.

Since $\sigma_x\sigma_z = \sigma_y = -\sigma_z\sigma_x$, every element of $\mathcal{E}_n$ may be written uniquely as

$$\pm\sigma_x^{a_1}\sigma_z^{b_1} \otimes ... \otimes \sigma_x^{a_n}\sigma_z^{b_n} = \pm\sigma_x(\mathbf{a})\sigma_y(\mathbf{b}),$$

where $\sigma_x(\mathbf{a}) = \sigma_x^{a_1} \otimes ... \otimes \sigma_x^{a_n}$ and $\sigma_z(\mathbf{b}) = \sigma_z^{b_1} \otimes ... \otimes \sigma_z^{b_n}$ for

$$\mathbf{a} = (a_1, ..., a_n),\ \mathbf{b} = (b_1, ..., b_n) \in \mathbf{F}_2^n.$$

Let $\Psi_n : \mathcal{E}_n \to \mathbf{F}_2^{2n}$ given by $\Psi_n(\pm\sigma_x(\mathbf{a})\sigma_y(\mathbf{b})) = (\mathbf{a}, \mathbf{b})$. It is a surjective homomorphism with $\ker(\Psi_n) = \{\pm I\}$. It follows that $\mathcal{E}_n$ has $2 \cdot 2^n \cdot 2^n = 2^{2n+1}$ elements.

Proposition 4. *Elements of $\mathcal{E}_n$ either commute or anti-commute. In fact, for $E = \pm X_\sigma(\mathbf{a})Z_\sigma(\mathbf{b}), E' = \pm X_\sigma(\mathbf{a}')Z_\sigma(\mathbf{b}') \in \mathcal{E}_n$*

$$E'E = (-1)^{\mathbf{ab}'-\mathbf{a}'\mathbf{b}}EE',$$

where $\mathbf{xy} = x_1y_1 + ... + x_ny_n$ is the standard Euclidean product for $\mathbf{x}, \mathbf{y} \in \mathbf{F}_2^n$.

In what follows, elements of $\mathbf{F}_2^{2n}$ will be represented by pairs $(\mathbf{x}, \mathbf{y})$ where $\mathbf{x}, \mathbf{y} \in \mathbf{F}_2^n$.

Definition 5. Define *the symplectic inner product* in $\mathbf{F}_2^{2n}$ by $\langle(\mathbf{a}, \mathbf{b}), (\mathbf{a}', \mathbf{b}')\rangle := \mathbf{ab}' - \mathbf{a}'\mathbf{b}$.

Let $\mathcal{G}$ be a subgroup of $\mathcal{E}_n$ such that $-I \in \mathcal{G}$. Notice that for such a group $\pm\sigma_x(\mathbf{a})\sigma_y(\mathbf{b})$ are simultaneously in or out of $\mathcal{G}$. Then

$$C_\mathcal{G} := \Psi_n(\mathcal{G}) = \{(\mathbf{a}, \mathbf{b}) :\ \sigma_\mathbf{x}(\mathbf{a})\sigma_\mathbf{y}(\mathbf{b}) \in \mathcal{G}\}$$

is a binary linear code of length $2n$ with $|\mathcal{G}|/2$ elements. Hence $\dim C_\mathcal{G} = \log_2|\mathcal{G}| - 1$. Furthermore, $\mathcal{G}$ is abelian iff $C_\mathcal{G}$ is self-orthogonal via the symplectic inner product in $\mathbf{F}_2^{2n}$. Conversely, if C is a self-orthogonal linear code of length $2n$ then

$$\mathcal{G}_C := {\Psi_n}^{-1}(C) = \{\pm\sigma_x(\mathbf{a})\sigma_z(\mathbf{b}) :\ (\mathbf{a}, \mathbf{b}) \in C\}$$

is an abelian subgroup of $\mathcal{E}_n$ and $-I \in \mathcal{G}_C$. We obtain the following

Proposition 6. *The correspondences $\mathcal{G} \to C_\mathcal{G}$, $C \to \mathcal{G}_C$ yield a bijective map from the set of self-orthogonal linear codes of length $2n$ to the set of abelian subgroups $\mathcal{G} \subset \mathcal{E}_n$ such that $-I \in \mathcal{G}$.*

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 3 (2015)

Both $\mathbf{F}_2^{2n}$ and $\mathcal{E}_n$ come with notions of *weight* which are compatible under the map Ψ_n.

Definition 7. (a) The *weight* of an element $(\mathbf{a}, \mathbf{b}) \in \mathbf{F}_2^{2n}$ is defined as $\mathrm{wt}(\mathbf{a}, \mathbf{b}) := \#\{i : \ (a_i, b_i) \neq (0, 0)\}$.

(b) The *weight* of an element $E = e_1 \otimes e_2 \otimes ... \otimes e_n \in \mathcal{E}_n$ is defined as $\mathrm{wt}(E) := \#\{i : \ e_i \neq I\}$.

It is immediate that the function Ψ_n preserves the weight, i.e. $\mathrm{wt}(\mathbf{a}, \mathbf{b}) = \mathrm{wt}(\pm\sigma_x(\mathbf{a})\sigma_z(\mathbf{b}))$.

4. Error Detecting and Correcting

Let $\mathbf{Q}$ be a quantum code of length n and size K, E an error, and $P : \mathbf{C}^{\otimes 2^n} \to \mathbf{Q}$ the orthogonal projection operator.

Definition 8. It is said that the quantum code $\mathbf{Q}$ *detects* the error E iff $(\forall x, y \in \mathbf{Q},)\ (x \perp y \Rightarrow x \perp E(y))$.

Theorem 9. *$\mathbf{Q}$ detects the error E iff there is a constant C_E such that $PEP = C_E P$ as matrices.*

Proof. Assume that $\mathbf{Q}$ detects E. Let $e_1, e_2, ..., e_K$ be an orthonormal basis of $\mathbf{Q}$. Then $E(e_i) \perp e_j$ for $i \neq j$. It follows that

$$E(e_i) = \lambda_i e_i + a_i,$$

where λ_i is some scalar and $a_i \in \mathbf{Q}^{\perp}$. One can easily see that $e_i - e_j \perp e_i + e_j$ for all i, j. It follows that

$$\lambda_i e_i + a_i - \lambda_j e_j - a_j = E(e_i - e_j) \perp e_i + e_j.$$

But both $a_i, a_j \in \mathbf{Q}^{\perp}$, which implies that $\lambda_i e_i - \lambda_j e_j \perp e_i + e_j$. Now $0 = (\lambda_i e_i - \lambda_j e_j)(e_i + e_j) = \lambda_i - \lambda_j$. Then $\lambda_1 = \lambda_2 = ... = \lambda_K = \lambda$ and $E(e_i) = \lambda e_i + a_i$ for all i. Hence $E(x) = \lambda x + x_E$ for some $x_E \in \mathbf{Q}^{\perp}$. Now

$$PEP(x) = P(\lambda P(x) + P(x)_E) = \lambda P^2(x) = \lambda P(x).$$

Here we used $P^2 = P$ and $P(P(x)_E) = 0$ since $P(x)_E \in \mathbf{Q}^{\perp}$.

Assume now that $PEP = c_E P$. Let $x \perp y$ be two elements of $\mathbf{Q}$. Then $P(y) = y$ and $PE(y) = PEP(y) = c_E P(y) = c_E y$. It follows that $E(y) = c_E y + y_E$ with $y_E \in \mathbf{Q}^{\perp}$. One can easily see that $x \perp E(y)$. □

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 3 (2015)

Recall that for an$n \times n$ matrix with complex entries E we denote by $E^\dagger$ its adjoint, i.e. its conjugate transpose matrix. If $\langle u, v\rangle := \sum u_i^* v_i$ is the standard inner product on $\mathbf{C}^n$, then

$$\langle E^\dagger(u), v\rangle = \langle u, E(v)\rangle.$$

Definition 10. *A measurement* on a quantum register is described by a set O of outcomes, a collection $\{P_o : o \in O\}$ of linear operators on the quantum register, which are called *measurement operators* and satisfy the *completeness equation*

$$\sum_{o\in O} P_o^\dagger P_0 = I$$

The probability of outcome o for a state α is $p(o) = \langle P_o(\alpha), P_o(\alpha)\rangle$. Notice that from the completeness equation $\sum_{o\in O} p(o) = 1$. The state of α after the measurement is

$$\frac{P_o(\alpha)}{\sqrt{p(o)}}.$$

Definition 11. *A quantum algorithm* on a quantum register is a finite composition of unitary and measurement operators.

Let $\mathbf{Q}$ be a binary quantum code of length n and size K, $P : \mathbf{C}^{\otimes 2^n} \to \mathbf{Q}$ the orthogonal projection operator, and $\mathcal{E}$ a collection of $2^n \times 2^n$ matrix, not just from the error group ϵ_n.

Definition 12. It is said that $\mathbf{Q}$ corrects $\mathcal{E}$ iff for every $E \in \mathcal{E}$ and every $x \in \mathbf{Q}$ there exists a quantum algorithm $\mu_{(E,x)}$ such that $\mu_{(E,x)}(Ex) = x$.

There is a characterization of the errors that are corrected by the codes $\mathbf{Q}$ which also unveils an interesting connection between the notions of detecting and correcting. Our treatment follows that of Knill and LaFlamme [8], for an alternative treatment see Bennett et. al. [2].

Theorem 13. *(see [8], [2]) If the dimension of* $\mathbf{Q}$ *is at least three then the following are equivalent:*

1. *The code* $\mathbf{Q}$ *corrects* $\mathcal{E}$.
2. *The code* $\mathbf{Q}$ *detects* $E^\dagger E'$ *for all* $E, E' \in \mathcal{E}$.
3. *If* x, y *are two orthogonal elements of* $\mathbf{Q}$ *then* $Ex, E'y$ *are also orthogonal for any* $E, E' \in \mathcal{E}$.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 3 (2015)

4. *There exists an orthonormal basis* $\{v_i\}$ *of* $\mathbf{Q}$ *and a scalar* $\lambda(E, E')$ *for every* $E, E' \in \mathcal{E}$ *such that*

$$\langle E(v_i), E'(v_j)\rangle = \lambda(E, E')\delta_{i,j}.$$

5. *For every* $E, E' \in \mathcal{E}$*, there exists a scalar* $\mu(E, E')$ *such that*

$$PE^{\dagger}E'P = \mu(E, E')P.$$

Proof. Will demonstrate only (5) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) $\Rightarrow$ (4) $\Leftrightarrow$ (3).
(2) $\Leftrightarrow$ (3) follows from the definition of detectable and the property of adjoint matrix.
(2) $\Leftrightarrow$ (5) follows from the previous theorem.
(3) $\Rightarrow$ (4). Let $x \perp y$ be two norm one elements of $\mathbf{Q}$. Then $x - y$ and $x + y$ are also perpendicular, hence

$$E(x) \perp E'(y),\ E'(x) \perp E(y),\ E(x - y) \perp E'(x + y).$$

It follows that $\langle E(x), E'(x)\rangle = \langle E(y), E'(y)\rangle$. From the connectedness of being orthogonal, $\langle E(x), E'(x)\rangle$ is constant on the unit sphere in $\mathbf{Q}$.
(4) $\Rightarrow$ (3). This follows easily from $\langle E(x), E'(y)\rangle = \lambda(E, E')\langle x, y\rangle$. □

5. Quantum Stabilizer Codes

Let $\mathcal{G}$ be an abelian subgroup of $\mathcal{E}_n$. It is a 2-subgroup; denote its order by 2^{k+1}. A linear character on $\mathcal{G}$ is a group homomorphism $\mu : \mathcal{G} \to \mathbf{S}^1$. If $-I \in \mathcal{G}$ then $\chi(-I) = \pm 1$ and exactly 2^k of them satisfy $\chi(-I) = -1$. Consider one of these linear characters.

Definition 14. The stabilizer code determined by χ is given by

$$\mathbf{Q}_{\mathcal{G},\chi} := \{x \in \mathbf{C}^{2^{\otimes n}} :\ E(x) = \chi(E)x \text{ for all } E \in \mathcal{G}\}.$$

Remark 15. $-I$ commutes will every matrix. If $-I \notin \mathcal{G}$, then the extension $\mathcal{G}'$ of $\mathcal{G}$ by $-I$ will still be an abelian subgroup and χ may be extended to a linear character $\chi' : \mathcal{G}' \to \mathbf{S}^1$ via $\chi(-I) = -1$. Furthermore

$$\mathbf{Q}_{\mathcal{G}',\chi'} = \mathbf{Q}_{\mathcal{G},\chi}.$$

Therefore, from now on we will assume that

$$\mathcal{G} \text{ is an abelian subgroup of } \mathcal{E}_n,\ -I \in \mathcal{G},\ \chi : \mathcal{G} \to \mathbf{S}^1,\ \chi(-I) = -1.$$

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 3 (2015)

Let

$$P_\chi := \frac{1}{|\mathcal{G}|}\sum_{E\in\mathcal{G}}\overline{\chi}(E)E$$

and $E' \in \mathcal{G}$. We compute

$$E'P_\chi := \frac{1}{|\mathcal{G}|}\sum_{E\in\mathcal{G}}\overline{\chi}(E)E'E$$

$$= \frac{1}{|\mathcal{G}|}\sum_{E\in\mathcal{G}}\chi(E')\overline{\chi}(E'E)E'E = \frac{1}{|\mathcal{G}|}\sum_{A\in\mathcal{G}}\chi(E')\overline{\chi}(A)A = \chi(E')P_\chi.$$

Proposition 16. *Let $C_\mathcal{G}$ be the self orthogonal linear code that correspond to $\mathcal{G}$ and P_χ be the projection $P_\chi : \mathbf{C}^{2^{\otimes n}} \to \mathbf{Q}_{\mathcal{G},\chi}$. Then the stabilizer code $\mathbf{Q}_{\mathcal{G},\chi}$ is the $+1$ eigenspace of the operator P_χ and dim $\mathbf{Q}_{\mathcal{G},\chi} = 2^{n-\dim\ C_\mathcal{G}}$.*

Proof. Assume first that $P_\chi(x) = x$. For $E \in \mathcal{G}$, we obtain: $E(x) = EP_\chi(x) = \chi(E)P_\chi(x) = \chi(E)x$, hence $x \in \mathbf{Q}_{\mathcal{G},\chi}$.

Now assume that $x \in \mathbf{Q}_{\mathcal{G},\chi}$. We compute

$$P_\chi(x) = \frac{1}{|\mathcal{G}|}\sum_{E\in\mathcal{G}}\overline{\chi}(E)E(x) = \frac{1}{|\mathcal{G}|}\sum_{E\in\mathcal{G}}\overline{\chi}(E)\chi(E)x = \frac{1}{|\mathcal{G}|}\sum_{E\in\mathcal{G}}x = x.$$

Assume that $|\mathcal{G}| = 2^{k+1}$ hence $k = \dim\ C_\mathcal{G}$. We have dim $\mathbf{Q}_{\mathcal{G},\chi}$ = trace (P_χ). We notice that only I and $-I$ have nonzero trace. Hence

$$\dim\ \mathbf{Q}_{\mathcal{G},\chi} = \text{trace }(P_\chi) = \frac{1}{|\mathcal{G}|}\sum_{E\in\mathcal{G}}\overline{\chi}(E)\ \text{trace }(E)$$

$$= \frac{1}{|\mathcal{G}|}\left(\overline{\chi}(I)\ \text{trace }(I) + \overline{\chi}(-I)\ \text{trace }(-I)\right) = \frac{1}{2^{k+1}}(2^n + 2^n) = 2^{n-k}.$$

□

As explained in the second section, the abelian subgroup $\mathcal{G}$ corresponds to a linear code $C = C_\mathcal{G}$ which is of length $2n$ and self-orthogonal $C \subset C^\perp$. The following statement is immediate:

Proposition 17. *$\mathcal{G}_{C^\perp}$ is the centralizer $\mathcal{Z}(\mathcal{G})$ of $\mathcal{G}$.*

It is a basic fact from linear algebra that the self-orthogonal linear code C can be extended to a self-dual linear code C^* of dimension n. The maximal abelian subgroup $\mathcal{G}_{C^*}$ has order 2^{n+1} and $\mathcal{G} = \mathcal{G}_C \subset \mathcal{G}_{C^*}$.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 3 (2015)

Proposition 18. *The only errors that are not detectable by* $\mathbf{Q}_{\mathcal{G},\chi}$ *are* $E \in \mathcal{Z}(\mathcal{G}) - \mathcal{G}$.

Proof. Assume first that $E \in \mathcal{G}$. Let $x \perp y$ with $x, y \in \mathbf{Q}_{\mathcal{G},\chi}$. Then $E(y) = \chi(E)y \perp x$. Hence $\mathbf{Q}_{\mathcal{G},\chi}$ detects E.

Now assume that $E \notin \mathcal{Z}(\mathcal{G})$. Since elements of $\mathcal{E}_n$ either commute or anticommute, there is a matrix $E' \in \mathcal{G}$ such that $E'E = -EE'$. Matrices of $\mathcal{G}$ that commute with E form a normal subgroup $\mathcal{G}_0$ of index 2. The nontrivial coset $\mathcal{G}_1 := \mathcal{G} - \mathcal{G}_0$ consist of matrices of $\mathcal{G}$ that anticommute with E. For $P = P_\chi$ we compute

$$|\mathcal{G}|PEP = \sum_{A\in\mathcal{G}} \overline{\chi}(A)AEP = E\left(\sum_{A\in\mathcal{G}_0} \overline{\chi}(A)AP - \sum_{A\in\mathcal{G}_1} \overline{\chi}(A)AP\right)$$

$$= E\left(\sum_{A\in\mathcal{G}_0} \overline{\chi}(A)\chi(A)P - \sum_{A\in\mathcal{G}_1} \overline{\chi}(A)\chi(A)P\right) = 0.$$

So, $PEP = 0 = 0P$ hence, E is detectable.

Finally, assume that $E \in \mathcal{Z}(\mathcal{G}) - \mathcal{G}$. We first notice that since E commutes with all the matrices of $\mathcal{G}$ then E fixes the subspace $\mathbf{Q}_{\mathcal{G},\chi}$, i.e. if $x \in \mathbf{Q}_{\mathcal{G},\chi}$ then $E(x) \in \mathbf{Q}_{\mathcal{G},\chi}$. Now if E is detectable by $\mathbf{Q}_{\mathcal{G},\chi}$ then $PEP = C_E P$ for some scalar C_E. SInce it fixes $\mathbf{Q}_{\mathcal{G},\chi}$, E must act as the scalar matrix C_E on $\mathbf{Q}_{\mathcal{G},\chi}$, i.e. $\mathbf{Q}_{\mathcal{G},\chi}$ must be a C_E-eigenspace for E. Let us show that this is not possible. First, we extend $\mathcal{G}$ by E to obtain an abelian group $\mathcal{G}_E$ of order 2^{k+2}. We then extend the linear character χ to χ_E on $\mathcal{G}_E$ via $\chi_E(E) = c_E$. This new linear character defines a subspace $\mathbf{Q}_{\mathcal{G}_E,\chi_E} \subset \mathbf{Q}_{\mathcal{G},\chi}$ of dimension is 2^{n-k-1} which is half of the dimension of $\mathbf{Q}_{\mathcal{G},\chi}$. It follows that $\mathbf{Q}_{\mathcal{G},\chi}$ can not be an eigenspace of E. □

Recall that $\mathcal{G}_{C^\perp} = \mathcal{Z}(\mathcal{G})$. Let d be the the minimum weight of the codewords in $C^\perp - C$ (or the minimum weight in $\mathcal{Z}(\mathcal{G}) - \mathcal{G}$). Every error of weight $d-1$ or less is detectable, hence the minimum distance of $\mathbf{Q}_{\mathcal{G},\chi}$ is d. From Proposition 6 and the construction of quantum stabilizer codes we obtain:

Theorem 19. *Let* $C \subset \mathbf{F}_2^{2n}$ *be a* $(n-k)$*-dimensional subspace such that* $C \subset C^\perp$ *(i.e.* C *is self-orthogonal). Then, there exists a quantum code* $\mathbf{Q} \subset \mathbf{C}^{2^{\otimes n}}$ *of dimension* 2^k *and minimum distance* $d = min\{wt(x)|x \in C^\perp - C\}$.

References

[1] A. Ashikhmin, E. Knill, Nonbinary quantum stabilizer codes, *IEEE Transactions on Information Theory*, **47**, No 7 (2001), 3065-3072, **doi:** 10.1109/18.959288.

[2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters, Mixed-state entanglement and quantum error correction, *Phys. Rev. A*, **54**, No 5 (1996), 3824-3851, **doi:** 10.1103/PhysRevA.54.3824.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, Quantum error correction and orthogonal geometry, *Phys. Rev. Lett.*, 78 (1997), 405-409, **doi:** 10.1103/PhysRevLett.78.405.

[4] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Info. Theory*, **44** (1998), 1369-1387, **doi:** 10.1109/18.681315.

[5] A. Elezi, T. Shaska, Quantum codes from superelliptic curves, *Albanian J. Math.*, **5**, No 4 (2011), 175-191.

[6] A. Elezi, T. Shaska, Cyclic covers of the projective line and quantum codes, in preparation.

[7] D. Gottesman, A class of quantum error-correcting codes saturating the quantum Hamming bound, *Phys. Rev. A.*, **54** (1996), 1862-1868, **doi:** 10.1103/PhysRevA.54.1862.

[8] E. Knill, R. Laflamme, A theory of quantum error-correcting codes, *Phys. Rev. A*, **55** (1997), 900-911, **doi:** 10.1103/PhysRevA.55.900.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 9, No. 3 (2015)