Boolean Functions, Projection Operators and Quantum Error Correcting Codes

Vaneet Aggarwal
Department of Electrical Engineering
Princeton University
Email: vaggarwa@princeton.edu

A. Robert Calderbank
Department of Electrical Engineering
Princeton University
Email: calderbk@math.princeton.edu

***Abstract*—This paper describes a common mathematical framework for the design of additive and non-additive Quantum Error Correcting Codes. It is based on a correspondence between boolean functions and projection operators. The new framework extends to operator quantum error correcting codes.**

I. Introduction

The additive or stabilizer construction of Quantum Error Correcting Codes (QECC) takes a classical binary code that is self-orthogonal with respect to a certain symplectic inner product, and produces a quantum code, with minimum distance determined by the classical code (For more details see [6], [7] and [11]). In [16], Rains *et al.* presented the first non-additive quantum error-correcting code. This code was constructed numerically by building a projection operator with a given weight distribution. Grassl and Beth [10] generalized this construction by introducing union quantum codes, where the codes are formed by taking the sum of subspaces generated by two quantum codes. Roychowdhury and Vatan [18] gave some sufficient conditions for the existence of nonadditive codes, and Arvind *et al.* [4] developed a theory of non-additive codes based on the Weyl commutation relations. Followed by this, Kribs *et al.* [13] introduced Operator Quantum Error Correction (OQEC) which is a unifying approach that incorporates the standard error correction model, the method of decoherence-free subspaces, and the noiseless subsystems as special cases.

We will describe a mathematical framework for code design that encompasses both additive and non-additive quantum error correcting codes. It is based on a correspondence between boolean functions and projection operators in Hilbert space that is described in Sections II, III and V. This type of correspondence was first given in [2] where this relation was used to construct space-time codes. We will give sufficient conditions for the existence of QECC in terms of the existence of the boolean function satisfying a few properties in Section VII. Hence, we convert the problem of finding a quantum code into a problem of finding boolean function satisfying some properties. For some parameters of Quantum code, we have given examples of the boolean functions satisfying these properties. We focus on non-degenerate codes which is reasonable given that we know of no parameters k, M and d for which there exists a $((k, M, d))$ degenerate QECC but not a $((k, M, d))$ non-degenerate QECC. Further, in Section VIII, we will see how this scheme fits into a general framework of operator quantum error correcting codes.

II. Boolean Function

A boolean function is defined as a mapping $f : \{0,1\}^m \rightarrow \{0,1\}$. To each m-tuple representing an assignment of values for the variables $v = (v_1, ..., v_m)$, $v_i \in \{0,1\}$, an integer v from the set $\{0, 1, ..., 2^m - 1\}$ can be assigned by the mapping $v = \sum_{i=1}^{m} v_i 2^{i-1}$. This value of v is called the decimal index for a given m-tuple.

An m-variable boolean function f can be specified by listing the values at all decimal indices. The binary-valued vector of function values $Y = [y_0, y_1, ..., y_{2^m-1}]$ is called the truth vector for f.

An m-variable boolean function $f(v_1, ..., v_m)$ can be represented as $\sum_{i=0}^{2^m-1} y_i v_1^{c_0(i)} v_2^{c_1(i)} ....v_m^{c_{m-1}(i)}$ where y_j is the value of the boolean function at the decimal index j and $c_0(j)$, $c_1(j)$, ... , $c_{m-1}(j) \in \{0,1\}$ are the coordinates in the binary representation for j (with c_{m-1} as the most significant bit and c_0 as the least significant bit) with $v_j^1 = v_j$ and $v_j^0 = \bar{v}_j$.

Definition 1: The Hamming weight of a boolean function is defined as the number of nonzero elements in Y.

Definition 2: The autocorrelation function of a boolean function $f(v)$ at a is the inner product of f with a shift of f by a. More precisely, $r(a) = \sum_{v=0}^{2^m-1} (-1)^{f(v) \oplus f(v \oplus a)}$ where $a \in \{0, 1, ..., 2^m - 1\}$, $a = \sum_{i=1}^{m} a_i 2^{i-1}$. An autocorrelation function is represented as a vector $B = [r(0), r(1), ..., r(2^m - 1)]$

Definition 3: The complementary set of a boolean function $f(v)$ is defined by $Cset_f = \{a | \sum_{v=0}^{2^m-1} f(v) f(v \oplus a) = 0\}$

This means that for any element a in the $Cset_f$, $f(v)f(v \oplus a) = 0$ for any choice of $v \in \{0, 1, ..., 2^m - 1\}$. The complementary set links distinguishability in the quantum world (orthogonality of subspaces) with properties of boolean functions. The quantity $f(v \oplus a)$ plays the counterpart in the

1-4244-1429-6/07/$25.00 ©2007 IEEE

Quantum world of the Quantum subspace after the error has occurred, which is to be orthogonal to the original subspace corresponding to $f(v)$.

Lemma 1: If the Hamming weight of the boolean function f is M, and $M \leq 2^{m-1}$, then the $Cset_f = \{a|r(a) = 2^m - 4M\}$

III. Boolean Functions and a Logic of Projection Operators

In [2], the authors introduced boolean logic for projection operators derived from the Heisenberg-Weyl group. In this section, we generalize results from [2] for a larger class of projection operators.

Let $\mathbb{B}(H)$ be the set of bounded linear operators on a Hilbert space H. An operator $P \in \mathbb{B}(H)$ is called a projection operator (sometimes we will use the terms orthogonal projection operator and self-adjoint projection operator) on H iff $P = PP^\dagger$. We denote the set of projection operators on H by $\mathbb{P}(H)$ and the set of all subspaces in H by $\mathbb{L}(H)$.

Definition 4:
1) If $S \subseteq H$, the span of S is defined as $\vee S = \cap\{K|K$ is a subspace in H with $S \subseteq K\}$. It is easy to see that $\vee S$ is the smallest subspace in H containing S.
2) If $S \subseteq H$, the orthogonal complement of S is defined as $S^\perp = \{x \in H|x \perp s \, \forall s \in S\}$.
3) If $\mathbb{S}$ is a collection of subsets of H, we write $\vee_{S\in\mathbb{S}} S = \vee(\cup_{S\in\mathbb{S}} S)$.

Definition 5: Let $P \in \mathbb{P}(H)$ and let $K = image(P) = \{Px|x \in H\}$. We call P the projection of H onto K. Two projections P and Q onto K and L are orthogonal (denoted $P \perp Q$) if $PQ = 0$. It is easy to verify that $PQ = 0 \Leftrightarrow K \perp L \Leftrightarrow QP = 0$. (Theorem 5B.9, [8])

Definition 6: Let $P, Q \in \mathbb{P}(H)$ with $K = image(P)$ and $L = image(Q)$. Then we define

- $P < Q$ iff K$\subset$ L ($K \neq L$)
- $P \vee Q$ is the projection of H onto $K \vee L$
- $P \wedge Q$ is the projection of H onto $K \cap L$.
- $\tilde{P}$ is the projection of H onto $K^\perp$ (We will also sometimes use $\bar{P}$ in place of $\tilde{P}$).

The structure $(\mathbb{P}(H), \leqslant, \perp)$ is a logic with unit I_H (identity map on H) and zero Z_H ($Z_H(x) = 0 \; \forall x \in H$) (Theorem 5B.18, [8]). This logic is called *Projection Logic*.

Lemma 2: (Theorem 5B.18, [8]) The map $P \rightarrow image(P)$ from $\mathbb{P}(H)$ to $\mathbb{L}(H)$ is a bijection that preserves order, orthogonality, meet($\wedge$) and join($\vee$).

Lemma 3: If P and Q are commutative operators, then the distributive law holds (and this law fails to hold for non-commutative operators). Also, in this case,

$$P \wedge Q = PQ$$
$$P \oplus Q \triangleq (P \wedge \tilde{Q}) \vee (\tilde{P} \wedge Q) = P + Q - 2PQ$$
$$\tilde{P} = I - P$$
$$P \vee Q = P + Q - PQ$$

Now we define projection function along the lines of [2].

Definition 7: Given an arbitrary boolean function $f(v_1, ..., v_m)$, we define the projection function $f(P_1, ..., P_m)$ in which v_i in the boolean function is replaced by P_i, multiplication in the boolean logic is replaced by the meet operation in the projection logic, summation in the boolean logic (or the *or* function) is replaced by the join operation in the projection logic and the not operation in boolean logic by the tilde ($\tilde{P}$) operation in the projection logic.

As is standard when writing boolean functions, we use *xor* in place of *or*, hence by above definition, we will replace the *xor* in the boolean logic by the *xor* operation in the projection logic.

Theorem 1: If $(P_1, ..., P_m)$ are pairwise commutative projection operators, each of dimension 2^{m-1}, such that $P_1P_2..P_m$, $P_1P_2..\bar{P}_m$, ... $\bar{P}_1\bar{P}_2..\bar{P}_m$ are all one-dimensional projection operators and H is of dimension 2^m, then $P_f = f(P_1, ...P_m)$ is an orthogonal projection on the subspace of dimension $Tr(P_f) = wt(f)$, where $wt(f)$ is the Hamming weight of the boolean function f.

Theorem 1 is a generalization of the Theorem 1 of [2] because we consider *any* pairwise commutative projection operators, while in [2], a special case of commutative projection operators using Heisenberg-Weyl group was used. This special case is described in Section V. Hence, to prove Theorem 1, we use projection logic [8] rather than the properties of a particular commutative subgroup.

IV. The Heisenberg-Weyl Group

Let σ_x, σ_y, and σ_z be the Pauli matrices, given by

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \sigma_y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix},$$

and consider linear operators E of the form $E = e_1 \otimes \ldots \otimes e_m$, where $e_j \in \{I_2, \sigma_x, \sigma_y, \sigma_z\}$. We form the Heisenberg-Weyl group (sometimes we will use the terms extra-special 2-group or Pauli group) E_m of order 4^{m+1}, which is realized as a group of linear operators $\alpha E, \alpha = \pm 1, \pm i$. (For a detailed description of extra-special group and its use to construct quantum codes see [6], [7].)

Next we define the symplectic product of two vectors.

Definition 8: The symplectic inner product of vectors $(a, b), (a', b') \in \mathbb{F}_q^{2m}$ is given by

$$(a, b) * (a', b') = a \cdot b' \oplus a' \cdot b.$$

The center of the group E_m is $\{\pm I_{2^m}, \pm iI_{2^m}\}$ and the quotient group $\overline{E}_m$ is isomorphic to the binary vector space $\mathbb{F}_2^{2m}$. We associate with binary vectors $(a, b) \in \mathbb{F}_2^{2m}$ operators $E_{(a,b)}$ defined by

$$E_{(a,b)} = e_1 \otimes \ldots \otimes e_m,$$
$$\text{where } e_i = \begin{cases} I_2, & a_i = 0, b_i = 0, \\ \sigma_x, & a_i = 1, b_i = 0, \\ \sigma_z, & a_i = 0, b_i = 1, \\ \sigma_y, & a_i = 1, b_i = 1. \end{cases}$$

V. The Construction of Commutative Projection Operators from the Heisenberg-Weyl Group

We will now describe how to construct commutative projection operators along the lines of [2]. Take m linearly independent vectors $x_1, x_2, ..., x_m$ of length 2m bits with the property that the symplectic product between any pair is equal to zero. If we take $P_i = \frac{1}{2}(I + E_{x_i})$, then P_1, ... P_m satisfy all the properties of Theorem 1, and hence, $f(P_1, ..., P_m)$ is an orthogonal projection operator [2]. This technique has been used earlier to construct grasmannian packings associated with binary Reed-Muller and Nordstrom-Robinson codes in [2] and [1] respectively.

VI. Fundamentals of Quantum Error Correction

A $((k, M))$ quantum error correcting code is an M-dimensional subspace of $\mathbb{C}^{2^k}$. The parameter k is the code-length and the parameter M is the dimension or the size of the code. Let Q be the quantum code, and P be the corresponding orthogonal projection operator on Q. (For a detailed description, see [3].)

Definition 9: An error operator E is called detectable iff $PEP = c_E P$, where c_E is a constant that depends only on E.

Following [9], we confine ourselves to the errors in the Heisenberg-Weyl group. Next, we define the minimum distance of the code.

Definition 10: The minimum distance of Q is the maximum integer d such that any error E, with symplectic weight at most d-1 is detectable.

The parameters of the quantum error correcting code are written $((k, M, d))$ where the additional parameter d is the minimum distance of Q. We say that $((k, M, d))$ Quantum error correcting code exist if there exists a $((k, M))$ Quantum error correcting code with minimum distance $\geq d$. In this paper, we focus on non-degenerate $((k, M, d))$ codes, for which $PEP = 0$ for all errors E of symplectic weight $\leq$ d-1, which is a sufficient condition for existence of the quantum code. The assumption of non-degeneracy is reasonable since we are not aware of any case when degenerate code performs better than a non-degenerate code. A quantum code is additive iff it can be constructed by the stabilizer framework of [7][11]. A quantum code is non-additive if it is not additive.

VII. Quantum Error Correcting Codes with Minimum Distance d

Theorem 2: A $((k, M, d))$-QECC is determined by a boolean function f with the following properties

1) f is a function of k variables and has weight M.
2) The complementary set associated with f contains the set $\{[x_1, x_2, ...x_{2k}] \times w^T |\ w$ is a 2k bit vector of symplectic weight $\leq d-1\}$ and the matrix $A_f = [x_1 x_2 ..... x_{2k}]_{k \times 2k}$ has the property that any two rows have symplectic product zero and that all the rows are linearly independent.

The projection operator corresponding to the QECC is obtained as follows:

1) Construct the matrix A_f as above.
2) Define k projection operators each of the form $\frac{1}{2}(I+E_v)$ where v is a row of the matrix A_f, with P_k corresponding to the 1^{st} row, P_{k-1} corresponding to the 2^{nd} row and so on, so that P_1 corresponds to the last row (as described in Section V).
3) Transform the boolean function f into the projection operator P_f using Definition 7 where the commutative projection operators P_1 .... P_k are determined by the matrix A_f.

Example 1: For $m \geq 2$, we construct a $((2m, 4^{m-1}, 2))$ additive QECC as an example of the above approach. Note that Rains [17] has shown that $M \leq 4^{m-1}$ for any $((2m, M, 2))$ quantum code and this example meets the upper bound. Take $f(v) = v_{2m} v_{2m-1}$. It is a function of $k = 2m$ variables with Hamming weight 4^{m-1} and the corresponding complementary set is $\{(010..0), (010...01), ...(111...1)\}$ (or $\{4^{m-1}, 4^{m-1}+1, ..., 4^m - 1\}$ in decimal notation). This complementary set contains the set $\{x_1, x_2...x_{2k}, x_1+x_{k+1}...x_k+x_{2k}\}$ where x_1 = x_2 = ... = x_k = (0 1 0 .. 0) (or 4^{m-1}), x_{k+1} = (1 0 1 .. 1), x_{k+2} = (1 0 1 0 .. 0), x_{k+3} = (1 0 0 1 0 .. 0), .. , x_{2k-1} = (1 0 0 .. 0 1) and x_{2k} = (1 0 0 .. 0). The matrix A_f is given by

$$A_f = \left(\begin{array}{ccccc|ccccc} 0 & \dots & 0 & 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & \dots & 0 & 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 & 0 & \dots & 0 & 1 & 0 \end{array}\right)$$

We see that the symplectic inner product of any two rows is zero. Hence, we have constructed a $((2m, 4^{m-1}, 2))$ QECC. Tracing through the construction of the projection operator P_f we find that $P_f = P_{2m} P_{2m-1}$, where $P_i = \frac{1}{2}(I + E_{v_i})$ and v_i is the $(2m + 1 - i)^{th}$ row of the matrix A_f. Hence, $P_{2m} = \frac{1}{2}(I + E_{00..0|11..1})$ and $P_{2m-1} = \frac{1}{2}(I + E_{11..1|00..0})$.

Example 2: For $m \geq 2$, we construct a $((2m, 4^{m-1}, 2))$ non-additive QECC as an example of the above approach. Consider the boolean function $f(v) = v_{2m}v_{2m-1}v_{2m-2} + v_{2m}v_{2m-1}\bar{v}_{2m-2}(v_{2m-3}+\bar{v}_{2m-3}v_{2m-4}+\bar{v}_{2m-3}\bar{v}_{2m-4}v_{2m-5} + ... + \bar{v}_{2m-4}\bar{v}_{2m-3}...\bar{v}_2 v_1) + v_{2m}\bar{v}_{2m-1}v_{2m-2}...v_1$. It is a function of $k = 2m$ variables with weight 4^{m-1}, and the corresponding complementary set is $\{(011..1), (100...0), (100...1), ...(111...1)\}$ (or $\{2^{2m-1}-1, 2^{2m-1}, ..., 4^m-1\}$ in decimal notation). This complementary contains the set $\{x_1, x_2, ..., x_{2k}, x_1+x_{k+1}...x_k+x_{2k}\}$ where x_1 = x_2 = ... = x_k = (0 1 1 .. 1) (or $2^{2m-1}-1$), x_{k+1} = (1 0 1 .. 1), x_{k+2} = (1 0 1 0 .. 0), x_{k+3} = (1 0 0 1 0 .. 0), .. , x_{2k-1} = (1 0 0 .. 0 1) and x_{2k} = (1 0 0 .. 0). The matrix A_f

is given by

$$A_f = \left(\begin{array}{ccccc|ccccc} 0 & \dots & 0 & 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & \dots & 1 & 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & \cdots & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & \cdots & 1 & 1 & 0 & 0 & \dots & 1 & 0 & 0 \\ 1 & \cdots & 1 & 1 & 0 & 0 & \dots & 0 & 1 & 0 \end{array}\right)$$

Hence, we can also see that the second property is satisfied. Hence, we have constructed a $((2m, 4^{m-1}, 2))$ QECC that is non-additive. Note that this construction has $((4, 4, 2))$-QECC as a special case, which was mentioned as an open question in [17].

Example 3: The $((5, 6, 2))$-QECC constructed by Rains *et al.* [16] is also a special case of the above procedure. Take the boolean function $f(v) = v_1v_2v_3 + v_3v_4v_5 + v_2v_3v_4 + v_1v_2v_5 + v_1v_4v_5 + v_2v_3v_4v_5$. It is a function of 5 variables with weight 6, and the corresponding complementary set is $\{1, 3, 4, 6, 8, 11, 12, 14, 17, 19, 21, 22, 24, 26, 28, 31\}$. Take $(x_1, \dots, x_{10})$ to be (6, 12, 24, 17, 3, 14, 31, 28, 26, 22) and form the matrix

$$A_f = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

The symplectic inner product of any two rows is zero and the corresponding projection operator P_f coincides with the one determined by ((5,6,2))-QECC in [16].

Lemma 4:
- If there exists a $((k, M, 2))$ QECC, then there exists a $((k+2, 4M, 2))$ QECC determined by same $f(v)$ and $A_{f'} = (x_1, x_2, \dots, x_{k-1}, x_k, x_k, x_k, x_{k+1}, x_{k+2}, \dots, x_{2k-1}, 2^{k+1}+2^k+x_{2k}, 2^k+x_{2k}, 2^{k+1}+x_{2k})$
- If there exists a $((k, M, 2))$ QECC, then there exists a $((k, M-1, 2))$ QECC determined by same A_f and $f'(v)$ having support (support is the set of inputs of the boolean function at which the output is 1) a subset of f(v).

Example 4: We can extend the Rains code to get $((2m+1, 3 \times 2^{2m-3}, 2))$-QECC for $m > 2$ using the above lemma.

Example 5: The perfect $((5, 2, 3))$ code of R. Laflamme *et al.* [14] can be obtained by the above approach. Take $f(v) = v_5v_4v_3v_2$. The corresponding complementary set is {2, 3, ... , 31}. The matrix A_f is given by

$$A_f = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and it is easy to see that all rows are linearly independent, and that the symplectic inner product of any two rows is zero.

VIII. Operator Quantum Error Correction (OQEC)

The theory of Operator Quantum error correction [13] uses the framework of noiseless subsystems to improve the performance of decoding algorithms which might help improve the threshold for fault-tolerant quantum computation. It requires a fixed partition of the systems Hilbert space $H = A \otimes B \oplus C^{\perp}$. Information is encoded on the A subsystem; the logical quantum state $\rho_A \in \mathbb{B}_A$ is encoded as $\rho_A \otimes \rho_B \oplus 0^{C^{\perp}}$ with an arbitrary $\rho_B \in \mathbb{B}_B$ (where $\mathbb{B}_A$ and $\mathbb{B}_B$ are the sets of all endomorphisms on subsystems A and B respectively). We say that the error E is correctable on subsystem A when there exists a physical map R that reverses its action, up to a transformation on the B subsystem. In other words, this error correcting procedure may induce some nontrivial action on the B subsystem in the process of restoring information encoded in the A subsystem. In the case of classical quantum error correcting codes, the dimension of B is 1.

Given a $((k, MN, d))$-QECC as above, we take MN basis vectors, say g_1, g_2, ... g_{MN} for the MN-dimensional vector space. Consider a sector of this subspace formed by $\rho_A \otimes \rho_B$ where $\rho_A \in \mathbb{B}_A$ and $\rho_B \in \mathbb{B}_B$. We can encode information on subsystem A, giving an $((k, M, N, d))$-OQEC, where M is the dimension of the subsystem on which we encode the information (called the logical subsystem), and N is the dimension of the subsystem that is allowed to suffer a transformation on the occurrence of error (called the Gauge subsystem). We also see that given such an $((k, M, N, d))$-OQEC, we can define a $((k, M, d))$-QECC in which the M-dimensional subspace is formed by $\rho_A \otimes I_B$. This is because this M dimensional subspace is a subspace of the above MN dimensional subspace, and we know that any subspace of the quantum code is also a quantum code. In other words, if we fix ρ_B (for example I_B above), we get the classical error correcting code. Thus, we have a general method of constructing non-additive and additive OQEC. In the classical quantum error correcting codes, $N = 1$. In standard quantum error correcting codes, one requires the ability to apply a procedure which exactly reverses on the error-correcting subspace any correctable error. In contrast, for operator error-correcting subsystems, the correction procedure need not undo the error which has occurred, but instead one must perform corrections only modulo the subsystem structure (subsystem B). This leads to recovery routines which explicitly make use of the subsystem structure [5].

Example 6: Consider the $((5, 6, 2))$-QECC code as in Example 3. In the 6-dimensional space, we take 6 basis vectors g_1, g_2, .. , g_6.

Let

$$\rho_A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

is an endomorphism on 3-dimensional subspace.

$$\rho_A \otimes I_B = \begin{pmatrix} a & 0 & b & 0 & c & 0 \\ 0 & a & 0 & b & 0 & c \\ d & 0 & e & 0 & f & 0 \\ 0 & d & 0 & e & 0 & f \\ g & 0 & h & 0 & i & 0 \\ 0 & g & 0 & h & 0 & i \end{pmatrix}$$

is an endomorphism in the 6-dimensional space which forms $((5,3,2))$-QECC.

Also, quantum state ρ_A is encoded as $\rho_A \otimes \rho_B \oplus 0^{C^\perp}$ =

$$\begin{pmatrix} aj & ak & bj & bk & cj & ck \\ al & am & bl & bm & cl & cm \\ dj & dk & ej & ek & fj & fk \\ dl & dm & el & em & fl & fm \\ gj & gk & hj & hk & ij & ik \\ gl & gm & hl & hm & il & im \end{pmatrix}$$

for arbitrary j , k , l and m. This operator is w.r.t. basis formed by g_1, g_2 , .. , g_6. At the receiver, from the corrupted version of $\rho_A \otimes \rho_B \oplus 0^{C^\perp}$, we can recover ρ_A (we need just ρ_A since our information is only encoded on the subsystem A) by taking projection onto $U = \{\rho_1 \otimes \rho_2 | \rho_1 \in \mathbb{B}_A, \rho_2 \in \mathbb{B}_B\}$ followed by taking the trace over the subsystem B.

Example 7: The stabilizer framework for OQEC is given in [15] which provides a method of constructing the stabilizer OQEC. We denote by X_j the matrix X (the Pauli matrix) acting on the j^{th} qubit, and similarly for Y_j and Z_j. The Pauli group $P_n =< i, X_1, Z_1, ..., X_n, Z_n >$. The first step in constructing a stabilizer code is to choose a set of $2n$ operators $\{X'_j, Z'_j\}_{j=1,..,n}$ from P_n that is Clifford isomorphic to the set of single-qubit Pauli operators $\{X_j, Z_j\}_{j=1,..,n}$ in the sense that the primed and unprimed operators obey the same commutation relations among themselves. The operators $\{X'_j, Z'_j\}_{j=1,..,n}$ generate P_n and behave as single-qubit Pauli operators. We can think of them as acting on n virtual qubits.

Suppose there exists a $((k, 2^s, d))$-additive QECC corresponding to a 2^s dimensional subspace, say C by the above framework of boolean functions. This means that for $f(v) = v_{s+1}v_{s+2}...v_k$, there exists a matrix A_f such that all its rows are linearly independent and have pairwise symplectic product zero. The first $k-s$ rows correspond to the stabilizers of the code. Form Z'_1, ... , Z'_k corresponding to the rows of matrix A_f. (The image of the first row in the Pauli group gives Z'_1 and so on.) Given all the Z'_j, we can easily find X'_j which have symplectic product of 1 with X'_j and symplectic product of 0 with all other X'_l, $l \neq j$.

Hence, the stabilizer group is given by $S =< Z'_1, Z'_2, ..., Z'_{k-s} >$. If we want to construct a $((k, 2^t, 2^{s-t}, d))$-OQEC, then we need to find a subsystem of dimension 2^t in the above subspace C of dimension 2^s. It is easy to see that if we take the Gauge group (corresponding to the Gauge subsystem defined before) $G =< S, X'_{k-s+1}, Z'_{k-s+1}, ..., X'_{k-t}, Z'_{k-t} >$ and the logical group $L =< X'_{k-t+1}, Z'_{k-t+1}, ..., X'_k, Z'_k >$, the action of any $l \in L$ and $g \in G$ restricted to the code subspace C is given by

$$gP = I_A \otimes g^B$$
$$lP = l^A \otimes I_B$$

for some l^A, g^B in $\mathbb{B}_A$ and $\mathbb{B}_B$ respectively, where A and B are the required subsystems [15][19].

IX. Conclusion

We have described a new mathematical framework that unifies the construction of additive and non-additive quantum codes. It is based on a correspondence between boolean functions and projection operators. We have given sufficient conditions for the existence of QECC in terms of existence of a boolean function satisfying certain properties. Examples of boolean functions have been presented that satisfy these properties. Using these boolean functions, we have presented a construction of additive and non-additive ((2m, 4^{m-1}, 2)) codes, the original ((5,6,2)) code constructed by Rains et. al., the extension of this code to ((2m+1, $3\times 2^{2m-3}$, 2)) codes, and the perfect ((5,2,3)) code. Finally we have shown how the new framework can be integrated with operator quantum error correcting codes.

References

[1] V. Aggarwal, A. Ashikhmin and A.R. Calderbank, "A grassmannian packing based on the nordstrom-robinson code," *IEEE Information Theory Workshop*, pp. 1-5, Chengdu, China, Oct. 2006.

[2] A. Ashikhmin and A.R. Calderbank, "Space-time reed-muller codes for noncoherent MIMO transmission," *IEEE International Symposium on Information Theory*, pp. 1952-1956, Adelaide, Australia, Sept. 2005.

[3] A. Ashikhmin and S. Litsyn, "Foundations of quantum error correction," *Recent Trend in Coding Theory and its Applications*, 2007.

[4] V. Arvind, P.P. Kurur and K.R. Parthasarathy, "Nonstabilizer quantum codes from abelian subgroups of the error group," *quant-ph/0210097*.

[5] D. Bacon, "Operator quantum error-correcting subsystems for self-correcting quantum memories," *Phys. Rev. A 73*, 012340, 2006.

[6] A.R. Calderbank, E.M. Rains, P.M. Shor and N.J.A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. on Inf. Th.*, Jul 1998.

[7] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry", *Phys. Rev. Lett*, vol. 78, pp. 405-409, 1997.

[8] D.W. Cohen, "An introduction to hilbert space and quantum logic," *Springer-Verlag*, 1989.

[9] A. Ekert and C. Macchiavello, "Quantum error correction for communication," *Phys. Rev. Lett. 77,* pp. 2585-2588, Sept. 1996.

[10] M. Grassl and T. Beth, "A note on non-additive quantum codes," *quant-ph/9703016*, March 1997.

[11] D. Gottesman, "Stabilizer codes and quantum error correction," *PhD Thesis*, quant-ph/9705052.

[12] A. Ketkar, A. Klappenecker, S. Kumar and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Transactions on Information Theory*, pp. 4892-4914, Nov. 2006.

[13] David Kribs, Raymond Laflamme and David Poulin, "Unified and generalized approach to quantum error correction," *Phys. Rev. Lett. 94*, 180501, 2005.

[14] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett. 77*, pp. 198201, 1996.

[15] D. Poulin, "Stabilizer formalism for operator quantum error correction," *quant-ph/0508131* , Jun 2006.

[16] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, "A nonadditive quantum code," *Phys. Rev. Lett. 79*, pp. 953954, 1997.

[17] E.M. Rains, "Quantum codes of minimum distance two," *IEEE Transactions on Information Theory*, pp. 266-271, Jan 1999.

[18] V. P. Roychowdhury and F. Vatan, "On the existence of nonadditive quantum codes", *Lecture notes in computer science*, Springer, 1998.

[19] P. Zanardi, D. A. Lidar, and S. Lloyd, "Quantum tensor product structures are observable induced," *Phys. Rev. Lett. 92*, 060402, 2004.