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 $v = \sum_{i=1}^{2^m-1} v_i 2^{i-1}$. 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 $\sum_{i=0}^{2^m-1} y_i v_1^{c_0(i)} v_2^{c_1(i)} ... v_m^{c_m(i)}$ where $y_i$ is the value of the boolean function at the decimal index $j$ and $c_0(j), c_1(j), ..., c_m(j) \in \{0, 1\}$ 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 $v_j^0 = v_j = v_j^1$.

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, $r(a) = \sum_{v=0}^{2^m-1} (-1)^{f(v)\oplus a} f(v\oplus a)$ 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
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 \( \text{Cset}_f = \{ a | r(a) = 2^m - 4M \} \)

### 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 \( B(H) \) be the set of bounded linear operators on a Hilbert space \( H \). An operator \( P \in B(H) \) is called a projection operator (sometimes we will use the terms orthogonal projection operator and self-adjoint projection operator) on \( H \) if \( P = P^2 \).

We denote the set of projection operators on \( H \) by \( \text{P}(H) \) and the set of all subspaces in \( H \) by \( \text{L}(H) \).

**Definition 4:**
1. If \( S \subseteq H \), the span of \( S \) is defined as \( \text{vspan} S = \cap \{ K | K \text{ is a subspace in } H \text{ with } S \subseteq K \} \). It is easy to see that \( \text{vspan} S \text{ is the smallest subspace in } H \) containing \( S \).
2. If \( S \subseteq H \), the orthogonal complement of \( S \) is defined as \( S^\perp = \{ x \in H | x \perp v \in S \} \).
3. If \( S \) is a collection of subsets of \( H \), we write \( \text{vspan} S = \cup \{ S \subseteq S \} \).

**Definition 5:** Let \( P \in \text{P}(H) \) and let \( K = \text{image}(P) = \{ Px | x \in H \} \). 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 \( PQ = 0 \iff K \perp L \rightleftharpoons QP = 0 \). (Theorem 5B.9, [8])

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

- \( P \perp Q \) if \( K \subseteq L \) (\( K \neq L \))
- \( P \perp Q \) is the projection of \( H \) onto \( K \perp L \)
- \( P \perp Q \) is the projection of \( H \) onto \( K \perp L \)
- \( P \perp Q \) is the projection of \( H \) onto \( K \perp L \)
- \( P \perp Q \) is the projection of \( H \) onto \( K \perp L \)

We will also sometimes use \( P \) in place of \( P \).

The structure \((\text{P}(H), \leq, \perp)\) 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 \( P \rightleftharpoons \text{image}(P) \) from \( \text{P}(H) \) to \( \text{L}(H) \) 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,

\[
\begin{align*}
P \wedge Q &= PQ \\
P \vee Q &= (P \wedge \tilde{Q}) \vee (\tilde{P} \wedge Q) = P + Q - 2PQ \\
\tilde{P} &= I - P \\
P \vee Q &= P + Q - PQ
\end{align*}
\]

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

**Definition 7:** Given an arbitrary boolean function \( f(v_1, \ldots, v_m) \), we define the projection function \( f(P_1, \ldots, P_m) \) 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 \( (P_1, \ldots, P_m) \) are pairwise commutative projection operators, each of dimension \( 2^{m-1} \), such that \( P_1 P_2 \ldots P_m, P_1 P_2 \ldots \tilde{P}_m \) are all one-dimensional projection operators and \( H \) is of dimension \( 2^m \), then \( f = f(P_1, \ldots, P_m) \) 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 \( \sigma_x, \sigma_y, \) and \( \sigma_z \) 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 \( E = e_1 \sigma_1 \otimes \ldots \otimes e_m \), 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 \( 2^m+1 \), 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 \( (a, b), (a', b') \in \mathbb{F}_{2^m}^2 \) is given by

\[
(a, b) \cdot (a', b') = a \cdot b' \pm a' \cdot b.
\]

The center of the group \( E_m \) is \( \{ \pm I_2, \pm i I_2 \} \) and the quotient group \( E_m \) is isomorphic to the binary vector space \( \mathbb{F}_{2^m}^2 \). We associate with binary vectors \( (a, b) \in \mathbb{F}_{2^m}^2 \) operators \( E(a, b) \) defined by

\[
E(a, b) = e_1 \otimes \ldots \otimes e_m,
\]

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-WEYLN 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 $P_t = \frac{1}{2}(I + E_{x_t})$, 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 Grassmannian 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 $\mathbb{C}^d$. 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 $P EP = c_E P$, 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 $(k,M,d)$ Quantum error correcting code with minimum distance $\geq d$. In this paper, we focus on non-degenerate $(k,M,d)$ codes, for which $PE = 0$ 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 if 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 $\{x_1, x_2, ..., x_{2k}\} \times w^T$ where $w$ 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 $\frac{1}{2}(I + EV)$ 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 $P_k$ 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 $\{x_1, x_2, x_3, x_4, x_5, x_6\}$. The matrix $A_f$ is given by

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

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 $P_i = \frac{1}{2}(I + EV_i)$ and $V_i$ is the $(2m + 1 - i)^{th}$ row of the matrix $A_f$. Hence, $P_{2m} = \frac{1}{2}(I + EV_{2m-1})$ and $P_{2m-1} = \frac{1}{2}(I + EV_{2m-1})$.

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 $f(v) = v_{2m}v_{2m-1}v_{2m-2} + v_{2m-2}v_{2m-3} - v_{2m-3}v_{2m-4} + v_{2m-3}v_{2m-4}v_{2m-5} + ... + v_{2m-3}v_{2m-4}v_{2m-5}v_{2m-6} + v_{2m-3}v_{2m-4}v_{2m-5}v_{2m-6}v_{2m-7}$. It is a function of $k = 2m$ variables with weight $4^{m-1}$, and the corresponding complementary set is $\{(011..1), (010..0), (010..01), ..., (111..1)\}$ (or $\{2^{m-1} - 1, 2^{m-1} - 1, ..., 4^{m-1}\}$ in decimal notation). This complementary set contains the set $\{x_1, x_2, ..., x_{2k}, x_1 + x_{k+1} + x_{2k}\}$ where $x_1 = x_2 = ... = x_k = (0 \ 1 \ 0 \ 0 \ 0 \ 0)$ (or $2^{m-1} - 1$, $x_{k+1} = (1 \ 0 \ 0 \ 0 \ 0 \ 0)$, $x_{k+2} = (1 \ 0 \ 0 \ 0 \ 0 \ 0)$, ..., $x_{2k-1} = (1 \ 0 \ 0 \ 0 \ 0 \ 0)$ and $x_{2k} = (0 \ 0 \ 0 \ 0 \ 0 \ 0)$. The matrix $A_f$
is given by

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

Hence, we can also see that the second property is satisfied. Hence, we have constructed a \(((2m, 4m^2 - 1), 2)\) 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 \(f(v) = v_1v_2v_3 + v_2v_4v_5 + v_2v_5v_6 + v_1v_2v_5 + v_1v_4v_5 + v_1v_2v_4v_5\). 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 \((x_1, \ldots, x_{10})\) to be \((6, 12, 24, 17, 3, 14, 31, 28, 26, 22)\) and form the matrix

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

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 \(A_f = \begin{pmatrix}1, 2, \ldots, x_{k-1}, x_k, x_{k+1}, x_{k+2}, \ldots, x_{2k-1}, 2^{k+1} + 2^k + x_{2k}, 2^k + x_{2k}, 2^{k+1} + x_{2k}\end{pmatrix}\).
- If there exists a \(((k, M))\) 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, \ldots, 31\}. The matrix \(A_f\) is given by

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

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 \(\rho_A \otimes \rho_B \oplus \mathbb{O} \subset \mathbb{B}_B\) 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 non-trivial 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 \(((k, M, d))\)-QECC as above, we take \(MN\) basis vectors, say \(g_1, g_2, \ldots, g_{MN}\) 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 \(((k, M, d))\)-OQEC 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 \(\rho_B\) (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 \(g_1, g_2, \ldots, g_6\).

Let

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

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

Also, quantum state \(\rho_A\) is encoded as \(\rho_A \otimes \rho_B \oplus \mathbb{0}^{C_L} =
\begin{pmatrix}
a & b & 0 & c & 0 \\
0 & a & 0 & b & 0 \\
0 & 0 & 0 & e & f \\
0 & d & 0 & 0 & 0 \\
g & 0 & h & 0 & i \\
0 & g & 0 & h & 0
\end{pmatrix}
\)
for arbitrary \(j, k, l\) and \(m\). This operator is w.r.t. basis formed by \(g_1, g_2, \ldots, g_6\). At the receiver, from the corrupted version of \(\rho_A \otimes \rho_B \oplus \mathbb{0}^{C_L}\), we can recover \(\rho_A\) (we need just \(\rho_A\) 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 QOEC is given in [15] which provides a method of constructing the stabilizer QOEC. 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 \(P_n = \langle i, X_1, Z_1, \ldots, X_n, Z_n \rangle\). The first step in constructing a stabilizer code is to choose a set of \(2^n\) operators \(\{X_j, Z_j\}\) for \(j = 1, \ldots, n\) that is Clifford isomorphic to the set of single-qubit Pauli operators \(\{X_j, Z_j\}\) for \(j = 1, \ldots, n\) in terms of the rules that the primed and unprimed operators obey the same commutation relations among themselves. The operators \(\{X_j', Z_j'\}\) for \(j = 1, \ldots, n\) 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 QEC corresponding to a \(2^s\) dimensional subspace, say \(C\) by the above framework of boolean functions. This means that \(f(v) = v_{s+1}v_{s+2}\ldots v_k\), 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 \(Z'_1, \ldots, Z'_{2^s}\) 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 \(S = < Z'_1, Z'_2, \ldots, Z'_{2^s} >\). If we want to construct a \(((k, 2^s, 2^t, d))\)-QOEC, 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) \(G = < S, X'_{k+1}, g_{k+1}, Z'_{k+1}, \ldots, X'_{k+t}, Z'_{k+t} >\) and the logical group \(L = < X'_{k+t+1}, g_{k+t+1}, \ldots, X'_{k+2t}, Z'_{k+2t} >\), the action of any \(l \in L\) and \(g \in G\) restricted to the code subspace \(C\) is given by
\[
gP = I_A \otimes gB
\]
\[lP = l^t \otimes I_B\]
for some \(l'A\), \(gB\) 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 constructed a construction of additive and non-additive ((\(2m\), \(4m-1, 2\)) codes, the original ((\(6,2\)) 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**


