

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

The MacWilliams Identity for Quantum Convolutional Codes

Ching-Yi Lai

Centre for Quantum Computation & Intelligent Systems
 Faculty of Engineering and Information Technology
 University of Technology, Sydney
 New South Wales, Australia 2007
 Email: ChingYi.Lai@uts.edu.au

Min-Hsiu Hsieh

Centre for Quantum Computation & Intelligent Systems
 Faculty of Engineering and Information Technology
 University of Technology, Sydney
 New South Wales, Australia 2007
 Email: Min-Hsiu.Hsieh@uts.edu.au

Abstract—In this paper, we propose a definition of the dual code of a quantum convolutional code, with or without entanglement assistance. We then derive a MacWilliams identity for quantum convolutional codes. Along the way, we obtain a direct proof of the MacWilliams identity, first found by Gluesing-Luerssen and Schneider, in the setting of classical convolutional codes.

I. INTRODUCTION

In classical coding theory, a well-known duality result is the MacWilliams identity for block codes, which gives a relation between the weight enumerators of a code and its dual [1]. However, due to the difficulty of defining weight enumerators that are invariant for classical convolutional codes, the MacWilliams identity was not believed to exist [2]. It was conjectured that the weight adjacency matrix, defined by a state space description of the encoder, could play the role of weight enumeration for convolutional codes [3]. Recently Gluesing-Luerssen and Schneider answered the conjecture on the positive side by deriving a MacWilliams identity for the weight adjacency matrices of a convolutional code and its dual in the *controller canonical form* [4], [5]. Later on, Forney proposed a more general MacWilliams theorem for convolutional codes (up to a scalar) by the normal factor graph duality theorem [6].

Quantum convolutional codes are a technique to protect a stream of quantum information in quantum communication [7], [8], [9], [10], [11]. It is unknown whether a MacWilliams identity exists for quantum convolutional codes and the notion of the dual code of a quantum convolutional code is unclear. For a quantum stabilizer code defined by a stabilizer group [12], [13], its dual stabilizer code does not exist since the orthogonal group of a stabilizer group is not a stabilizer group. (The notion of orthogonality will be clear after we define an inner product later.) However, if shared-entanglement between the sender and receiver is allowed [14], [15], the dual code of a stabilizer code is an entanglement-assisted quantum error-correcting (EAQEC) code [16], [17]. The MacWilliams theorem exists for quantum codes with or without entanglement assistance [18], [19], [20], [16].

In this article, we provide a direct proof of the MacWilliams identity for classical convolutional codes using the Dirac bracket notation, and then apply it to the quantum case. The scalar that is missing in Forney's result [6] is explicitly given in our proof. We will define the dual code of a quantum convolutional

code within the framework of entanglement-assisted quantum (EAQ) convolutional codes [21], [22], [23]. Our notion of duality coincides with the normal factor graph duality theorem, which details how one can obtain the dual of a code from its normal realization [24], [6], [25], [26].

II. REVIEW OF QUANTUM ERROR-CORRECTING CODES

We use the Dirac notation that $|\psi\rangle$ is a vector in a vector space V . Let $\langle\psi| = |\psi\rangle^\dagger$ be the adjoint of $|\psi\rangle$ and let $\langle\psi|\phi\rangle$ and $|\psi\rangle\langle\phi|$ denote the inner product and the outer product of $|\psi\rangle, |\phi\rangle \in V$, respectively. The tensor product $|\psi_1\rangle \otimes |\psi_2\rangle$ is a vector in the vector space $V_1 \otimes V_2$ for $|\psi_1\rangle \in V_1$ and $|\psi_2\rangle \in V_2$, where the tensor product $A \otimes B$ for an $s \times t$ matrix $A = [a_{i,j}]$ and an $s' \times t'$ matrix $B = [b_{i,j}]$ is

$$\begin{bmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,t}B \\ a_{2,1}B & a_{2,2}B & \cdots & a_{2,t}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{s,1}B & a_{s,2}B & \cdots & a_{s,t}B \end{bmatrix}.$$

Let \mathcal{H} be the state space of a single qubit with an (ordered) orthonormal basis $\{|0\rangle, |1\rangle\}$. The state space of n qubits is the tensor product of n single qubit state space \mathcal{H} and is denoted by $\mathcal{H}^{\otimes n}$. Let $\mathcal{G}_n = \mathcal{G}_1^{\otimes n}$ denote the n -fold Pauli group, where $\mathcal{G}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$. Note that $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, and $Y = iZX$ form a basis of the space of the linear operators on \mathcal{H} . The weight $\text{wt}(g)$ of $g \in \mathcal{G}_n$ is the number of components of g that are not the identity operator. For $g_1, g_2 \in \mathcal{G}_n$, we define the inner product $*$ in \mathcal{G}_n by

$$g_1 * g_2 = \begin{cases} 0, & \text{if } [g_1, g_2] = 0 \\ 1, & \text{if } \{g_1, g_2\} = 0, \end{cases}$$

where $[g_1, g_2] = g_1g_2 - g_2g_1$ and $\{g_1, g_2\} = g_1g_2 + g_2g_1$.

Suppose \mathcal{S} is an Abelian subgroup of \mathcal{G}_n with a set of $n - k$ independent generators $\{g_1, g_2, \dots, g_{n-k}\}$ and \mathcal{S} does not include $-I$. An $[[n, k]]$ quantum stabilizer code $C(\mathcal{S})$ is defined to be the 2^k -dimensional subspace of $\mathcal{H}^{\otimes n}$ fixed by \mathcal{S} . That is,

$$C(\mathcal{S}) = \{|\psi\rangle \in \mathcal{H}^{\otimes n} : g|\psi\rangle = |\psi\rangle, \forall g \in \mathcal{S}\}.$$

If the sender and receiver share c maximally-entangled pairs $|\Phi_+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ before communication, this coding scheme is called an EAQEC code [14], [15]. It is assumed

that the qubits held by the receiver before communication are error-free. Similarly, an $[[n, k; c]]$ EAQEC code is defined to be the 2^k -dimensional subspace of $\mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes c}$ fixed by a stabilizer group $\mathcal{S} \in \mathcal{G}_{n+c}$. We neglect the operators on the receiver's qubits since they are perfect. (The case that the qubits of the receiver are imperfect is addressed in [27]). In this case the simplified stabilizer group \mathcal{S}' is no longer Abelian. Suppose \mathcal{S}' has a set of independent generators $\{g_1, \dots, g_{n-k}, h_1, \dots, h_c\}$ so that they satisfy the following commutation relation: $g_i * h_i = 1$, and $g_i * h_j = 0$, $g_i * g_j = 0$, and $h_i * h_j = 0$ for $i \neq j$. The c pairs of $\{g_i, h_i\}$ for $i = 1, \dots, c$ are called symplectic partners, corresponding to the c maximally-entangled states. The rest $n-k-c$ generators $\{g_{c+1}, \dots, g_{n-k}\}$ commute with everything in \mathcal{S}' .

III. THE MACWILLIAMS IDENTITY ON THE EXACT WEIGHT GENERATING FUNCTIONS

Suppose \mathcal{A} is a vector space of dimension n over a finite field \mathbb{F}_q , where $q = p^r$ is a power of a prime p . We define a Hilbert space $\mathcal{H}_{\mathcal{A}}$ corresponding to \mathcal{A} such that for all $a \in \mathcal{A}$, $|a\rangle$ is a unit vector in $\mathcal{H}_{\mathcal{A}}$ and $\{|a\rangle\}$ forms an orthonormal basis of $\mathcal{H}_{\mathcal{A}}$ so that $\langle a|a'\rangle = \delta_{a,a'}$, where $\delta_{a,a'}$ is the Kronecker delta function. Below we define the *exact weight generating function* (EWGF) of a subset of \mathcal{A} as a linear combination of orthonormal vectors, rather than the usual multivariate polynomial [1].

Definition 1. The EWGF $g_{\mathcal{C}}^E$ of a set $\mathcal{C} \subset \mathcal{A}$ is defined as $g_{\mathcal{C}}^E = \sum_{c \in \mathcal{C}} |c\rangle$.

Suppose $\hat{\mathcal{A}}$ is a dual space of \mathcal{A} of the same dimension that consists of homomorphisms that map \mathcal{A} to \mathbb{Z}_p . We define an "inner product" $\langle \hat{a}, a \rangle = \hat{a}(a)$ for $\hat{a} \in \hat{\mathcal{A}}$, and $a \in \mathcal{A}$. The Fourier transform operator $\mathcal{F}_{\mathcal{A}}$ is defined as

$$\mathcal{F}_{\mathcal{A}} = \sum_{\hat{a} \in \hat{\mathcal{A}}} \sum_{a \in \mathcal{A}} \omega^{\langle \hat{a}, a \rangle} |\hat{a}\rangle \langle a|,$$

where $\omega = e^{2\pi i/p}$ is a primitive complex p -th root of unity.

Theorem 2. Suppose \mathcal{C} is a subspace of \mathcal{A} with EWGF $g_{\mathcal{C}}^E = \sum_{c \in \mathcal{C}} |c\rangle$. The EWGF of its orthogonal space \mathcal{C}^{\perp} in $\hat{\mathcal{A}}$ with respect to an inner product $\langle \cdot, \cdot \rangle$ between $\hat{\mathcal{A}}$ and \mathcal{A} is

$$g_{\mathcal{C}^{\perp}}^E = \frac{1}{|\mathcal{C}|} \mathcal{F}_{\mathcal{A}} g_{\mathcal{C}}^E.$$

Proof.

$$\begin{aligned} \frac{1}{|\mathcal{C}|} \mathcal{F}_{\mathcal{A}} g_{\mathcal{C}}^E &= \frac{1}{|\mathcal{C}|} \sum_{\hat{a} \in \hat{\mathcal{A}}} \sum_{a \in \mathcal{A}} \omega^{\langle \hat{a}, a \rangle} |\hat{a}\rangle \langle a| \sum_{c \in \mathcal{C}} |c\rangle \\ &= \frac{1}{|\mathcal{C}|} \sum_{\hat{a} \in \hat{\mathcal{A}}} \sum_{c \in \mathcal{C}} \omega^{\langle \hat{a}, c \rangle} |\hat{a}\rangle \\ &= \sum_{\hat{a} \in \mathcal{C}^{\perp}} |\hat{a}\rangle = g_{\mathcal{C}^{\perp}}^E, \end{aligned}$$

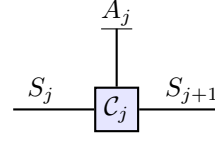


Fig. 1. The normal graph of a conventional state realization.

where the last equality follows from

$$\frac{1}{|\mathcal{C}|} \sum_{c \in \mathcal{C}} \omega^{\langle \hat{a}, c \rangle} = \begin{cases} 1, & \hat{a} \in \mathcal{C}^{\perp}; \\ 0, & \hat{a} \notin \mathcal{C}^{\perp}. \end{cases}$$

The above equation is obvious for $\hat{a} \in \mathcal{C}^{\perp}$. For $\hat{a} \notin \mathcal{C}^{\perp}$, there exists $c' \in \mathcal{C}$ such that $\langle \hat{a}, c' \rangle \neq 0$. Since $c' + \mathcal{C} = \mathcal{C}$, we have $\sum_{c \in \mathcal{C}} \omega^{\langle \hat{a}, c \rangle} = \sum_{c \in \mathcal{C}} \omega^{\langle \hat{a}, c+c' \rangle} = \omega^{\langle \hat{a}, c' \rangle} \sum_{c \in \mathcal{C}} \omega^{\langle \hat{a}, c \rangle}$, which implies $\sum_{c \in \mathcal{C}} \omega^{\langle \hat{a}, c \rangle} = 0$. \square

It is straightforward to derive the MacWilliams identity for the usual weight generators of linear block codes by applying a map $\gamma : |v\rangle \mapsto W^{\text{wt}(v)}$ on the EWGFs and the above theorem, where W is transcendental over \mathbb{C} and $\text{wt}(v)$ is the Hamming weight of v . We omit the details,

Next we show how to obtain the MacWilliams identity for the weight adjacency matrices of a classical convolutional code and its dual. Suppose we have a rate k/n convolutional code \mathcal{C} over \mathbb{F}_q with m memories. The normal graph of the state realization of \mathcal{C} is shown in Fig. 1, where S_j and S_{j+1} denote the memory space at time j and $j+1$, respectively, and A_j is the output space of the convolutional code. (For more details please refer to [6].) The *constraint code* \mathcal{C}_j is an $[n+2m, k+m]$ linear block code over \mathbb{F} defined as follows. Let $a : b$ be the concatenation of vectors a and b . A vector $(m_j : a_j : m_{j+1})$ belongs to \mathcal{C}_j if there is a path from state m_j to state m_{j+1} with output a_j in the trellis diagram of the convolutional code \mathcal{C} . According to Definition 1, the EWGF of \mathcal{C}_j is

$$g_{\mathcal{C}_j}^E = \sum_{m_j \in S_j} \sum_{m_{j+1} \in S_{j+1}} \sum_{\substack{v \in A_j: \\ (m_j : v : m_{j+1}) \in \mathcal{C}_j}} |m_j\rangle |v\rangle |m_{j+1}\rangle.$$

Definition 3. The *exact weight adjacency matrix* Λ_j^E of a convolutional constraint code \mathcal{C}_j is the matrix whose (m_j, m_{j+1}) entry is the EWGF of the output symbols of \mathcal{C}_j . That is,

$$\langle m_j | \Lambda_j^E | m_{j+1} \rangle = \sum_{\substack{v \in A_j: \\ (m_j : v : m_{j+1}) \in \mathcal{C}_j}} |v\rangle.$$

It can be directly verified or from the normal factor graph duality theorem that the constraint code $\hat{\mathcal{C}}_j$ of the dual \mathcal{C}^{\perp} has the codeword $(m_j : a_j : m_{j+1})$ if $(m_j : a_j : -m_{j+1})$ is in the dual code of \mathcal{C}_j .

Also, it is obvious that

$$\mathcal{F}_{\mathcal{A}} = \mathcal{F}_{\mathcal{A}_r} \otimes \mathcal{F}_{\mathcal{A}_s},$$

where \mathcal{A}_r and \mathcal{A}_s are r - and s -dimensional vector spaces over \mathbb{F}_q , respectively, so that $r + s = n$ and $\mathcal{A}_r \otimes \mathcal{A}_s = \mathcal{A}$. Combining these facts with Theorem 2, we have the

MacWilliams identity for the exact weight adjacency matrices of a convolutional code and its dual.

Theorem 4. The exact weight adjacency matrix $\hat{\Lambda}_j^E$ of the dual of \mathcal{C} is

$$\hat{\Lambda}_j^E = \frac{1}{|\mathcal{C}|} \sum_{m_j, m_{j'}} \left(\sum_{\substack{v \in \mathcal{A}_j \\ (m_j, v, m_{j'}) \in \mathcal{C}_j}} \mathcal{F}_{\mathcal{A}_j} |v\rangle \right) \mathcal{F}_{\mathcal{S}_j} |m_j\rangle \langle m_{j'} | \mathcal{F}_{\mathcal{S}_{j+1}}^\dagger.$$

The weight adjacency matrix Λ of a convolutional code \mathcal{C} is obtained by applying the map $\gamma : |v\rangle \mapsto W^{\text{wt}(v)}$ to its exact weight adjacency matrix. Consequently, the MacWilliams identity for the usual weight adjacency matrices of a convolutional code and its dual directly follows and is omitted here.

IV. THE DUAL CODE OF A QUANTUM CONVOLUTIONAL CODE

Poulin *et al.* devised a representation of quantum convolutional codes by a seed transformation and defined the associated state diagram [28], [7]. Entanglement-assisted version is developed in [29], [30]. We will use this representation to develop the duality in quantum convolutional codes.

An (n, k, c, m) EAQ convolutional code is specified by a *seed transformation* U , input parameters $(\mathcal{I}^M, \mathcal{I}^L, \mathcal{I}^A, \mathcal{I}^E)$, and output parameters $(\mathcal{I}^{M'}, \mathcal{I}^P)$, where $\mathcal{I}^M, \mathcal{I}^L, \mathcal{I}^A, \mathcal{I}^E, \mathcal{I}^{M'}$, and \mathcal{I}^P are the locations of the input memory qubits, logical qubits, ancilla qubits, entangled qubits, output memory qubits, and physical qubits, so that $|\mathcal{I}^M| = |\mathcal{I}^{M'}| = m$, $|\mathcal{I}^L| = k$, $|\mathcal{I}^A| = a$, $|\mathcal{I}^E| = c$, and $|\mathcal{I}^P| = n = k + a + c$.

Definition 5. A seed transformation U is a unitary Clifford operator on $n + m$ qubits so that $UZ_i U^\dagger = g_i \in \mathcal{G}_{n+m}$, $UX_i U^\dagger = h_i \in \mathcal{G}_{n+m}$, for $i = 1, \dots, n + m$ for a set of $(n + m)$ pairs of symplectic partners $\{g_1, \dots, g_{n+m}, h_1, \dots, h_{n+m}\}$, where $g_i * h_i = 1$, and $g_i * h_j = 0$, $g_i * g_j = 0$, and $h_i * h_j = 0$ for $i \neq j$.

An EAQ convolutional code has a state diagram, associated with the seed transformation U .

Definition 6. The state diagram associated with a seed transformation U and two sequences $(\mathcal{I}^M, \mathcal{I}^L, \mathcal{I}^A, \mathcal{I}^E)$ and $(\mathcal{I}^{M'}, \mathcal{I}^P)$ is a *directed* diagram with 4^m vertices, called memory states and labeled by an $M \in \mathcal{G}_m$. Two vertices M and M' are connected by an edge with label (L, P) if and only if there exist $L \in \mathcal{G}_k$, $P \in \mathcal{G}_n$, and $S^Z \in \{I, Z\}^{\otimes n-k}$ such that

$$M' \otimes P = U(M \otimes L \otimes S^Z \otimes I^{\otimes c}) U^\dagger.$$

In some cases we may relocate M' and P so that $P \otimes M' = U(M \otimes L \otimes S^Z \otimes I^{\otimes c}) U^\dagger$, and is equivalent to the above definition up to a rearrangement of qubits.

The dual code of an EAQ convolutional code is defined according to its seed transformation.

Definition 7. Suppose \mathcal{C} is a quantum convolutional code with a seed transformation U on the input sequence $(\mathcal{I}^M, \mathcal{I}^L, \mathcal{I}^A, \mathcal{I}^E)$. Then the dual code \mathcal{C}^\perp of \mathcal{C} has the seed

transformation U on the input parameters $(\mathcal{I}^M, \mathcal{I}^E, \mathcal{I}^A, \mathcal{I}^L)$ and the same output sets.

Remark: An EAQ convolutional code and its dual are uniquely defined up to a *unitary row operator* R that preserves the stabilizer group \mathcal{S} and its dual \mathcal{S}^\perp [31]. For example, UR is a seed transformation that defines the same EAQ convolutional code as U does if for all $g \in \mathcal{S}$ and $h \in \mathcal{S}^\perp$, $RgR^\dagger \in \mathcal{S}$ and $RhR^\dagger \in \mathcal{S}^\perp$, respectively.

Consider the normal factor graph of the quantum convolutional code (the same as Fig. 1). Its constraint code \mathcal{C}_j at time j is the $[[n + 2m, k; c]]$ EAQEC code defined by a simplified stabilizer group \mathcal{S}' with the following generators:

$$\begin{aligned} Z_i^M \otimes g_i, X_i^M \otimes h_i, & \quad \text{for } i \in \mathcal{I}^M; \\ I^M \otimes g_i, I^M \otimes h_i, & \quad \text{for } i \in \mathcal{I}^E; \\ I^M \otimes g_i, & \quad \text{for } i \in \mathcal{I}^A; \end{aligned}$$

where the superscripts M, L, A , and E denote the qubits that are operated. According to [16], the dual code \mathcal{C}_j^\perp with respect to the inner product $*$, defined in \mathcal{G}_{n+2m} , is the $[[n + 2m, c; k]]$ EAQEC code defined by a simplified stabilizer group with the following generators:

$$\begin{aligned} Z_i^M \otimes g_i, X_i^M \otimes h_i, & \quad \text{for } i \in \mathcal{I}^M; \\ I^M \otimes g_i, I^M \otimes h_i, & \quad \text{for } i \in \mathcal{I}^L; \\ I^M \otimes g_i, & \quad \text{for } i \in \mathcal{I}^A. \end{aligned}$$

Observe that the seed transformation U with the input parameters $(\mathcal{I}^M, \mathcal{I}^E, \mathcal{I}^A, \mathcal{I}^L)$ as in Definition 7 defines the dual constraint code \mathcal{C}_j^\perp . Following [6], this constraint code \mathcal{C}_j^\perp defines the dual graph of the normal factor graph of the original quantum convolutional code. Thus our definition of the dual code of a quantum convolutional code is justified.

Since the overall phase of a quantum state is not important, we always count in the quotient group $\bar{\mathcal{G}}_n = \mathcal{G}_n / \{\pm 1, \pm i\}$ for the weight distribution of a subgroup of \mathcal{G}_n . An element in $\bar{\mathcal{G}}_n$ is denoted by $[g]$, where $g \in \mathcal{G}_n$. Thus $[\]$ defines an equivalence class. If $[g] = [g']$ in $\bar{\mathcal{G}}_n$, then $gg' \in \{\pm I, \pm iI\}$. For $[g_1], [g_2] \in \bar{\mathcal{G}}_n$, we implicitly define the symplectic inner product $*$ by $[g_1] * [g_2] = g_1 * g_2$. The weight enumerator of a subgroup S of \mathcal{G}_n is a polynomial $D_S(W) = \sum_{w=0}^n d_w W^w$, where d_w is the number of element of $[S] = S / \{\pm 1, \pm i\}$ of weight w .

Definition 8. The *weight adjacent matrix* Λ associated with a state diagram is defined to be the matrix so that its (M_j, M_{j+1}) entry is the weight generating function of the set of physical output operators when the input and output memory operators are M_j and M_{j+1} , respectively.

In the case of the quotient Pauli group $\bar{\mathcal{G}}_1 = \langle [I], [X], [Y], [Z] \rangle$, the matrix representation of the Fourier

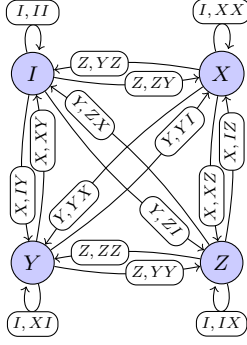


Fig. 2. The state diagram corresponding to the seed transformation U_1 .

transform operator in the order $|[I]\rangle, |[X]\rangle, |[Y]\rangle, |[Z]\rangle$ is

$$F = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

It can be verified that the Fourier transform matrix on the n -fold Pauli group \mathcal{G}_n is $F^{\otimes n}$.

Observe that Theorem 2 also applies to additive groups and the following theorem can be easily obtained from Theorem 4. Again, the proof is omitted.

Theorem 9. Suppose \mathcal{C} is an (n, k, c, m) EAQ convolutional code with a weight adjacency matrix Λ . The weight adjacency matrix $\hat{\Lambda}$ of its dual code in the sense of Definition 7 (with a given seed transformation U and associated parameters) is related to Λ by the following equation:

$$\hat{\Lambda} = 4^{-m} 4^{-k} 2^{-a} \mathbb{H} (F^{\otimes m} \Lambda F^{\otimes m}),$$

where F is the Fourier transform matrix defined above, and \mathbb{H} applies the following transformation on each entry of the input matrix:

$$f(W) \mapsto f\left(\frac{1-W}{1+3W}\right) (1+3W)^{\deg f}.$$

In the case of $m = 0$, it reduces to the case of EAQEC codes in [17], [16].

V. EXAMPLES

Wilde and Hsieh constructed an example of non-catastrophic and recursive ($m = 1, k = 1, a = 0, c = 1$) EAQ convolutional code with $\mathcal{I}^M = \{1\}$, $\mathcal{I}^{L'} = \{2\}$, $\mathcal{I}^E = \{3\}$, $\mathcal{I}^{M'} = \{1\}$, and $\mathcal{I}^P = \{2, 3\}$ [29]. The seed transformation U_1 is as follows:

$$\begin{array}{ccccccc} Z & I & I & & Z & I & X \\ I & Z & I & & X & Z & Y \\ I & I & Z & & X & Y & Z \\ X & I & I & \xrightarrow{U_1} & X & X & X \\ I & X & I & & Y & I & Y \\ I & I & X & & Y & X & Y \end{array},$$

and its state diagram is shown in Fig. 2. The seed transforma-

tion U_1 has an weight adjacent matrix

$$\Lambda = \begin{bmatrix} 1 & W^2 & W & W \\ W^2 & W^2 & W^2 & W^2 \\ W^2 & W & W & W^2 \\ W^2 & W & W^2 & W \end{bmatrix}.$$

(Unlike [29], this weight adjacency matrix include the path of the zero physical-weight cycle at the (1,1) entry.)

The dual of this EAQ convolutional code is obtained by switching the roles of the logical qubits and ebits and in this example $k = c = 1$. We found the state diagram of the dual code is the reversed graph of the original state diagram, and consequently it has a weight adjacency matrix $\hat{\Lambda} = \Lambda^T$. On the other hand, we can apply Theorem 9 to obtain the same result as well.

The MacWilliams identity holds for the EAQ convolutional codes, catastrophic or noncatastrophic, recursive or nonrecursive (see Refs [28], [30] for these definitions). For example, the seed transformation of a $(n = 2, k = 1, m = 1, a = 0, c = 1)$ catastrophic and non-recursive EAQ convolutional code U_2 is as follows:

$$\begin{array}{ccccccc} Z & I & I & & Z & I & I \\ I & Z & I & & Z & Z & I \\ I & I & Z & \xrightarrow{U_2} & I & Z & Z \\ X & I & I & & X & X & X \\ I & X & I & & I & X & X \\ I & I & X & & I & I & X \end{array}.$$

($\mathcal{I}^M = \{1\}$, $\mathcal{I}^{L'} = \{2\}$, $\mathcal{I}^E = \{3\}$, $\mathcal{I}^{M'} = \{1\}$, and $\mathcal{I}^P = \{2, 3\}$.) The dual pair of the weight adjacency matrices are

$$\Lambda = \begin{bmatrix} 1+W^2 & 0 & 0 & W+W^2 \\ 0 & 1+W^2 & W+W^2 & 0 \\ 0 & W+W^2 & 1+W^2 & 0 \\ W+W^2 & 0 & 0 & 1+W^2 \end{bmatrix},$$

and

$$\hat{\Lambda} = \begin{bmatrix} 1+W+2W^2 & 0 & 0 & 0 \\ 0 & W+3W^2 & 0 & 0 \\ 0 & 0 & W+3W^2 & 0 \\ 0 & 0 & 0 & 1+W+2W^2 \end{bmatrix}.$$

The third example is the ($m = 1, k = 1, a = 1$) quantum convolutional code constructed in [28] with the same seed transformation U_2 , but $\mathcal{I}^{M'} = \{3\}$ and $\mathcal{I}^P = \{1, 2\}$. The dual code of this quantum convolutional code is the ($m = 1, k = 0, a = 1, c = 1$) EAQ convolutional code. It is easier to construct the state diagram of this EAQ convolutional code, since it can be obtained by removing those edges of the original state diagram with nonzero logical weight. The weight adjacency matrix of the dual code is

$$\hat{\Lambda} = \begin{bmatrix} 1 & 0 & 0 & W \\ 0 & W^2 & W^2 & 0 \\ 0 & W^2 & W^2 & 0 \\ W & 0 & 0 & W^2 \end{bmatrix}.$$

The weight adjacency matrix of the original quantum convo-

lutional code can be obtained by the MacWilliams identity for convolutional codes as follows:

$$\Lambda = 4^{-m} 4^{-c} 2^{-a} \mathbb{H} \left(F^{\otimes m} \hat{\Lambda} F^{\otimes m} \right)$$

$$= \begin{bmatrix} 1 + W^2 & W + W^2 & W + W^2 & 2W \\ W + W^2 & 2W^2 & 2W^2 & W + W^2 \\ W + W^2 & 2W^2 & 2W^2 & W + W^2 \\ 2W & W + W^2 & W + W^2 & 1 + W^2 \end{bmatrix}.$$

VI. CONCLUSION

The main contribution of this work is a MacWilliams identity for the EAQ convolutional codes. Specifically, the MacWilliams identity is established for the weight adjacency matrices of a quantum convolutional code and its dual. Our definition of the dual code of an EAQ convolutional code is similar to that of an EAQEC code. On the other hand, we also provide a direct proof of the MacWilliams identity for the classical convolutional codes.

With the MacWilliam identity, one can then compute the distance spectrum polynomials of a quantum convolutional code and its dual, from the weight adjacency matrices. It will allow the comparison of the error performance of different quantum convolutional codes.

Unlike classical codes, QECCs can involve various different resources [32], [33]. Another interesting open question is how to quantify the *passive* error-correcting power of the quantum subsystem codes, particularly, using the weight generating functions. It is possible to define the dual codes of such QECCs and obtain various notions of MacWilliams identities. However, it remains unknown whether these quantum weight generating functions can be directly applied to the performance analysis for these codes. The main difficulty arises from a quantum effect, namely, quantum degeneracy.

For more details and results about the weight enumeration of classical and quantum convolutional codes, please refer to the complete version of our paper [34].

ACKNOWLEDGMENT

CYL was supported by the Australian Research Council under Grant DP120103776. MH was supported by the UTS Chancellors postdoctoral research fellowship and UTS Early Career Researcher Grants Scheme. MH acknowledges hospitality and support from Overseas Team Program of Academy of Mathematics and Systems Science, Chinese Academy of Science.

REFERENCES

- [1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
- [2] J. B. Shearer and R. J. McEliece, "There is no MacWilliams identity for convolutional codes," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 6, pp. 775–776, 1977.
- [3] H. Gluesing-Luerssen, "On the weight distribution of convolutional codes," *Linear Algebra and its Applications*, vol. 408, pp. 298–326, 2005.
- [4] H. Gluesing-Luerssen and G. Schneider, "On the MacWilliams identity for convolutional codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1536–1550, 2008.

- [5] —, "A MacWilliams identity for convolutional codes: The general case," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 2920–2930, 2009.
- [6] J. Forney, G.D., "Codes on graphs: Duality and MacWilliams identities," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1382–1397, 2011.
- [7] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Phys. Rev. Lett.*, vol. 91, p. 177902, Oct 2003.
- [8] G. Forney, M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 865–880, 2007.
- [9] M. Grassl and M. Rotteler, "Non-catastrophic encoders and encoder inverses for quantum convolutional codes," in *Proc. 2006 IEEE Intl. Symp. Inf. Theory*, 2006, pp. 1109–1113.
- [10] —, "Constructions of quantum convolutional codes," in *Proc. 2007 IEEE Intl. Symp. Inf. Theory*, 2007, pp. 816–820.
- [11] M. M. Wilde, "Quantum-shift-register circuits," *Phys. Rev. A*, vol. 79, p. 062325, Jun 2009.
- [12] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Institute of Technology, Pasadena, CA, 1997.
- [13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press, 2000.
- [14] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, pp. 436–439, 2006.
- [15] T. Brun, I. Devetak, and M.-H. Hsieh, "Catalytic quantum error correction," quant-ph/0608027, 2006.
- [16] C.-Y. Lai, T. A. Brun, and M. M. Wilde, "Duality in entanglement-assisted quantum error correction," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 4020–4024, 2013.
- [17] —, "Dualities and identities for entanglement-assisted quantum codes," *Quant. Inf. Proc.*, pp. 1–34, 2013.
- [18] P. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities for classical coding theory," *Phys. Rev. Lett.*, vol. 78, no. 8, pp. 1600–1602, Feb 1997.
- [19] E. M. Rains, "Quantum weight enumerators," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1388 – 1394, 1995.
- [20] A. Ashikhmin and S. Litsyn, "Upper bounds on the size of quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1206 – 1215, 1999.
- [21] M. M. Wilde and T. A. Brun, "Extra shared entanglement reduces memory demand in quantum convolutional coding," *Phys. Rev. A*, vol. 79, p. 032313, Mar 2009.
- [22] —, "Entanglement-assisted quantum convolutional coding," *Phys. Rev. A*, vol. 81, p. 042333, Apr 2010.
- [23] —, "Quantum convolutional coding with shared entanglement: general structure," *Quant. Inf. Proc.*, vol. 9, no. 5, pp. 509–540, 2010.
- [24] J. Forney, G.D., "Codes on graphs: normal realizations," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 520–548, 2001.
- [25] Y. Mao and F. Kschischang, "On factor graphs and the Fourier transform," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1635–1649, 2005.
- [26] A. Al-Bashabsheh and Y. Mao, "Normal factor graphs and holographic transformations," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 752–763, 2011.
- [27] C.-Y. Lai and T. A. Brun, "Entanglement-assisted quantum error-correcting codes with imperfect ebits," *Phys. Rev. A*, vol. 86, p. 032319, Sep 2012.
- [28] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2776–2798, 2009.
- [29] M. M. Wilde and M.-H. Hsieh, "Entanglement boosts quantum turbo codes," in *Proc. 2011 IEEE Intl. Symp. Inf. Theory*, 2011, pp. 445–449.
- [30] M. M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1203–1222, 2014.
- [31] C.-Y. Lai and T. A. Brun, "Entanglement increases the error-correcting ability of quantum error-correcting codes," *Phys. Rev. A*, vol. 88, p. 012320, Jul 2013.
- [32] I. Kremsky, M.-H. Hsieh, and T. A. Brun, "Classical enhancement of quantum error-correcting codes," *Phys. Rev. A*, vol. 78, p. 012341, 2008.
- [33] M.-H. Hsieh, I. Devetak, and T. A. Brun, "General entanglement-assisted quantum error-correcting codes," *Phys. Rev. A*, vol. 76, p. 062313, 2007.
- [34] C.-Y. Lai, M.-H. Hsieh, and H.-H. Lu, "On the MacWilliams identity for classical and quantum convolutional codes," 2014. [Online]. Available: <http://arxiv.org/abs/1404.5012>