A Complete MacWilliams Theorem for Convolutional Codes

Ching-Yi Lai, Min-Hsiu Hsieh
Centre for Quantum Computation and 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@uts.edu.au

Hsiao-feng Lu
Department of Electrical and Computer Engineering
National Chiao Tung University
HsinChu 30010, Taiwan.
Email: francis@mail.nctu.edu.tw

***Abstract*—In this paper, we prove a MacWilliams identity for the weight adjacency matrices based on the constraint codes of a convolutional code (CC) and its dual. Our result improves upon a recent result by Gluesing-Luerssen and Schneider, where the requirement of a minimal encoder is assumed. We can also establish the MacWilliams identity for the input-parity weight adjacency matrices of a systematic CC and its dual. Most importantly, we show that a type of Hamming weight enumeration functions of all codewords of a CC can be derived from the weight adjacency matrix, which thus provides a connection between these two very different notions of weight enumeration functions in the convolutional code literature. Finally, the relations between various enumeration functions of a CC and its dual are summarized in a diagram. This explains why no MacWilliams identity exists for the free-distance enumerators.**

I. Introduction

The free-distance enumerator of a convolutional code (CC) that counts the weight distribution of fundamental paths in the full trellis diagram has been shown to have no MacWilliams identity [1] by Shearer and McEliece in 1977 [2]. On the contrary, a recent result by Gluesing-Luerssen and Schneider proved a MacWilliams identity for the enumeration matrices, the weight adjacency matrices (WAMs), of a CC and its dual [3]. A fundamental question thus arises: What information in a WAM is missing in the corresponding free-distance enumerator? Moreover, is there any relationship between the two very different notions of weight enumeration functions?

In this paper, we provide positive answers to the above questions. We adopt the concept of constraint codes of a CC introduced by Forney in his normal factor graph duality theorem [4]. We further define the dual of a CC from the constraint codes. Within this framework, we obtain a straightforward proof of the MacWilliams identity for the WAMs based on the constraint codes of a CC and its dual. Using constraint codes allows us to generalize the result obtained in Ref. [3] because different generator matrices (or encoders) of a constraint code generate the same code space of the constraint code. Thus the MacWilliams identity for CCs derived from the constraint codes is unique. In other words, the encoders need not be minimal in our proof.

We next define a Hamming weight enumeration of all codewords of a CC, $W_{\mathcal{C}}(y,D)$, in equation (11). While no MacWilliams identity exists for this weight enumeration, we can establish relations between $W_{\mathcal{C}}(y,D)$ and $W_{\mathcal{C}^\perp}(y,D)$ through the WAMs of a CC and its dual. We also show that this weight enumeration function is related to the free-distance enumerator of the CC. Finally, we illustrate the complete relations of various weight enumeration functions in a diagram, which summarizes the MacWilliams theorem for CCs.

II. Preliminary

Definition 1. Let $\mathcal{C}$ be an (n,k,m) convolutional code over $\mathbb{F}_q$ with a polynomial generator matrix $G(D)\in\mathbf{M}_{k\times n}\left(\mathbb{F}_q[D]\right)$ for some indeterminate D. Then $\mathcal{C}$ is a rank-k submodule of $\mathcal{M}=\left(\mathbb{F}_q[D]\right)^n$ given by

$$\mathcal{C}=\left\{G^\top(D)\underline{m}(D):\underline{m}(D)\in\left(\mathbb{F}_q[D]\right)^k\right\}.$$

The dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ is defined as

$$\mathcal{C}^\perp:=\left\{\underline{u}(D)\in\mathcal{M}:\underline{u}(D^{-1})^\top\underline{c}(D)=0,\ \text{for all }\underline{c}(D)\in\mathcal{C}\right\}.$$

The constraint code $\mathcal{C}_{(j)}$ for $\mathcal{C}$ is a $[2m+n,m+k]$ linear block code over $\mathbb{F}_q$, consisting of images of the map $(\underline{w}_j,\underline{\ell}_j)\mapsto(\underline{w}_j,\underline{p}_j,\underline{w}_{j+1})$, where $\underline{w}_j\in\mathbb{F}_q^m$ represents the state, $\underline{\ell}_j\in\mathbb{F}_q^k$ is the input message vector, and $\underline{p}_j\in\mathbb{F}_q^n$ is the output code vector, all at time instant j. The constraint code $\hat{\mathcal{C}}_{(j)}$ for $\mathcal{C}^\perp$ is a $[2m+n,m+n-k]$ linear code over $\mathbb{F}_q$ given by

$$\begin{aligned}\hat{\mathcal{C}}_{(j)}=\Big\{\left[\underline{u}_j^\top\ \underline{v}^\top\ \underline{u}_{j+1}^\top\right]^\top\in\mathbb{F}_q^{2m+n}:&\\ \underline{u}_j^\top\underline{w}_j+\underline{v}^\top\underline{p}_j-\underline{u}_{j+1}^\top\underline{w}_{j+1}=0,&\\ \text{for all }\left[\underline{w}_j^\top\ \underline{p}_j^\top\ \underline{w}_{j+1}^\top\right]^\top\in\mathcal{C}_{(j)}\Big\}.&\end{aligned}\qquad(1)$$

Furthermore, the above defines the dual code $\mathcal{C}_{(j)}^\perp$ for $\mathcal{C}_{(j)}$ in the usual sense as

$$\mathcal{C}_{(j)}^\perp=\left\{\left[\underline{u}_j^\top\ \underline{v}^\top\ -\underline{u}_{j+1}^\top\right]^\top:\left[\underline{u}_j^\top\ \underline{v}^\top\ \underline{u}_{j+1}^\top\right]^\top\in\hat{\mathcal{C}}_{(j)}\right\}.$$

Let $\mathcal{V}$ be a vector space over $\mathbb{F}_q$ and assume char$(\mathbb{F}_q)=p$. The group character $\chi_{\underline{u}}\in\text{Hom}(\mathcal{V},U(1))$ for some $\underline{u}\in\mathcal{V}$ is a group homomorphism from $\mathcal{V}$ to $U(1)$, the unitary group in $\mathbb{C}$. Below we will focus on a specific kind of group character $\chi_{\underline{u}}:\underline{v}\mapsto\zeta^{\text{tr}(\underline{u}^\top\underline{v})}$, where tr : $\mathbb{F}_q\to\mathbb{F}_p$ is the usual trace linear map for fields, and ζ is a primitive p-th root of unity in $\mathbb{C}$.

III. Weight Enumeration of the Constraint Code

Let $\mathcal{V} = \mathbb{F}_q^{2m+n}$ and f be any function defined on $\mathcal{V}$. The classical MacWilliams identity is simply

$$\sum_{\underline{v}\in\mathcal{C}_{(j)}^{\perp}} f\left(\underline{v}\right) \;=\; \frac{1}{\left|\mathcal{C}_{(j)}\right|}\sum_{\underline{u}\in\mathcal{C}_{(j)}} F\left(\underline{u}\right), \tag{2}$$

where F is the Fourier transform of f over $\mathcal{V}$ with respect to kernel $\chi_{\underline{u}}(\underline{v})$.

A. Enumerate in Multivariate Polynomial

For any $(\underline{v}_1, \underline{v}_2, \underline{v}_3) \in \mathbb{F}_q^m \times \mathbb{F}_q^n \times \mathbb{F}_q^m \cong \mathcal{V}$, in this subsection we consider the following weight function

$$f\left(\underline{v}_1, \underline{v}_2, \underline{v}_3\right) = \left[\prod_{i=1}^{m}\prod_{j=1}^{q} x_{i,j}^{\mathrm{wt}_j(v_{1,i})}\right] y^{\mathrm{wt}\left(\underline{v}_2\right)} \left[\prod_{i=1}^{m}\prod_{j=1}^{q} z_{i,j}^{\mathrm{wt}_j(v_{3,i})}\right]$$

for some indeterminates $x_{i,j}$, y, and $z_{i,j}$, where $\underline{v}_1, \underline{v}_3 \in \mathbb{F}_q^m$, $\underline{v}_2 \in \mathbb{F}_q^n$, and wt : $\mathbb{F}_q^n \to \mathbb{Z}^+$ is the usual Hamming weight metric. Say $\mathbb{F}_q = \{\omega_1, \dots, \omega_q\}$, wt_j is an indicator function given by $\mathrm{wt}_j(a) := \mathbf{1}(a = \omega_j)$.

The weight enumerator for $\mathcal{C}_{(j)}$ based on weight function f is

$$\begin{aligned} &W_{\mathcal{C}_{(j)}}\left(x_{1,1}, \dots, x_{m,q}, y, z_{1,1}, \dots, z_{m,q}\right) \\ &\qquad = \sum_{\left[\underline{w}_j^\top \;\, \underline{p}_j^\top \;\, \underline{w}_{j+1}^\top\right]^\top \in\mathcal{C}_{(j)}} f\left(\underline{w}_j, \underline{p}_j, \underline{w}_{j+1}\right). \end{aligned} \tag{3}$$

The Fourier transform of f over $\mathcal{V}$ with respect to kernel $\chi_{\underline{u}}(\underline{v})$ with $\underline{u} = (\underline{u}_1, \underline{u}_2, \underline{u}_3)$ is given in (4).

Thus we obtain the following theorem.

Theorem 2. The weight enumerators for $\mathcal{C}_{(j)}^{\perp}$ and $\hat{\mathcal{C}}_{(j)}$ are given by

$$\begin{aligned} &W_{\mathcal{C}_{(j)}^{\perp}}\left(x_{1,1}, \dots, x_{m,q}, y, z_{1,1}, \dots, z_{m,q}\right) \\ &= \frac{(1+(q-1)y)^n}{q^{m+k}} W_{\mathcal{C}_{(j)}}\left(\mathfrak{x}_{1,1}, \dots, \mathfrak{x}_{m,q}, \mathfrak{y}, \mathfrak{z}_{1,1}, \dots, \mathfrak{z}_{m,q}\right), \end{aligned}$$

where

$$\begin{aligned} \mathfrak{x}_{i,\ell} &= \sum_{j=1}^{q} \zeta^{-\mathrm{tr}(\omega_\ell\omega_j)} x_{i,j}, \\ \mathfrak{y} &= \frac{1-y}{1+(q-1)y}, \\ \mathfrak{z}_{i,\ell} &= \sum_{j=1}^{q} \zeta^{-\mathrm{tr}(\omega_\ell\omega_j)} z_{i,j}; \end{aligned}$$

and

$$\begin{aligned} &W_{\hat{\mathcal{C}}_{(j)}}\left(x_{1,1}, \dots, x_{m,q}, y, z_{1,1}, \dots, z_{m,q}\right) \\ &= \frac{(1+(q-1)y)^n}{q^{m+k}} W_{\mathcal{C}_{(j)}}\left(\mathfrak{x}_{1,1}, \dots, \mathfrak{x}_{m,q}, \mathfrak{y}, \hat{\mathfrak{z}}_{1,1}, \dots, \hat{\mathfrak{z}}_{m,q}\right), \end{aligned}$$

where $\hat{\mathfrak{z}}_{i,\ell} = \sum_{j=1}^{q} \zeta^{+\mathrm{tr}(\omega_\ell\omega_j)} z_{i,j}$.

If $\mathcal{C}_{(j)}$ is systematic, the above result can be extended to the input-parity weight enumerator by further splitting the weights for $\underline{p}_j$ (or equivalently $\underline{v}_2$) as a two-split in y_I and y_P for inputs and parities as in [5], [6]. In other words, say $\underline{v}_2 = \left[\underline{v}_{2,I}^\top \;\, \underline{v}_{2,P}^\top\right]^\top$ and redefine the weight function as

$$\begin{aligned} &f_{\mathrm{IP}}\left(\underline{v}_1, \underline{v}_{2,I}, \underline{v}_{2,P}, \underline{v}_3\right) \\ &= \left[\prod_{i=1}^{m}\prod_{j=1}^{q} x_{i,j}^{\mathrm{wt}_j(v_{1,i})}\right] y_I^{\mathrm{wt}\left(\underline{v}_{2,I}\right)} y_P^{\mathrm{wt}\left(\underline{v}_{2,P}\right)} \left[\prod_{i=1}^{m}\prod_{j=1}^{q} z_{i,j}^{\mathrm{wt}_j(v_{3,i})}\right]. \end{aligned}$$

Then the following corollary is immediate.

Corollary 3. The input-parity weight enumerator for $\hat{\mathcal{C}}_{(j)}$ is

$$\begin{aligned} &W_{\hat{\mathcal{C}}_{(j)}}\left(x_{1,1}, \dots, x_{m,q}, y_I, y_P, z_{1,1}, \dots, z_{m,q}\right) \\ &\qquad = K \times W_{\mathcal{C}_{(j)}}\left(\mathfrak{x}_{1,1}, \dots, \mathfrak{x}_{m,q}, \mathfrak{y}_I, \mathfrak{y}_P, \mathfrak{z}_{1,1}, \dots, \mathfrak{z}_{m,q}\right), \end{aligned}$$

where $\mathfrak{y}_I = \frac{1-y_I}{1+(q-1)y_I}, \mathfrak{y}_P = \frac{1-y_P}{1+(q-1)y_P}$, and

$$K = \frac{(1+(q-1)y_I)^k(1+(q-1)y_P)^{n-k}}{q^{m+k}}. \tag{5}$$

B. Enumerate in Matrix: Weight Adjacency Matrix

We may also enumerate the codewords in $\mathcal{C}_{(j)}$ in a matrix form. To this end, we index the entries of a matrix $A \in \mathbf{M}_{q^m}(\mathbb{Z}[y])$ by $(\underline{v}_1, \underline{v}_3) \in \mathbb{F}_q^m \times F_q^m$. Let $\underline{e}_{\underline{v}} \in \{0,1\}^{q^m}$ be a length-q^m vector in $\mathbb{R}^{q^m}$ such that $\left(\underline{e}_{\underline{v}}\right)_i = 1$ if the index i is associated with vector $\underline{v} \in \mathbb{F}_q^m$, and $\left(\underline{e}_{\underline{v}}\right)_i = 0$, otherwise. With the above, for any $(\underline{v}_1, \underline{v}_2, \underline{v}_3) \in \mathbb{F}_q^m \times \mathbb{F}_q^n \times \mathbb{F}_q^m$, we consider the following weight function

$$f_{\mathrm{mat}}\left(\underline{v}_1, \underline{v}_2, \underline{v}_3\right) = y^{\mathrm{wt}\left(\underline{v}_2\right)} \underline{e}_{\underline{v}_1} \underline{e}_{\underline{v}_3}^\top. \tag{6}$$

Definition 4. The weight adjacency matrix for $\mathcal{C}_{(j)}$ is the weight enumerator for $\mathcal{C}_{(j)}$ based on weight function f_{mat}, i.e.,

$$\Lambda_{\mathcal{C}_{(j)}}\left(y\right) = \sum_{\left[\underline{w}_j^\top \;\, \underline{p}_j^\top \;\, \underline{w}_{j+1}^\top\right]^\top \in\mathcal{C}_{(j)}} f_{\mathrm{mat}}\left(\underline{w}_j, \underline{p}_j, \underline{w}_{j+1}\right). \tag{7}$$

The Fourier transform of f_{mat} over $\mathcal{V}$ with respect to kernel $\chi_{\underline{u}}(\underline{v})$ is given by

$$\begin{aligned} &F_{\mathrm{mat}}(\underline{u}_1, \underline{u}_2, \underline{u}_3) \\ &= \sum_{(\underline{v}_1, \underline{v}_2, \underline{v}_3)\in\mathcal{V}} y^{\mathrm{wt}\left(\underline{v}_2\right)} \underline{e}_{\underline{v}_1} \underline{e}_{\underline{v}_3}^\top \zeta^{-\sum_{i=1}^{3}\mathrm{tr}\left(\underline{u}_i^\top \underline{v}_i\right)} \\ &= \left(\sum_{\underline{v}_1\in\mathbb{F}_q^m} \zeta^{-\mathrm{tr}\left(\underline{u}_1^\top \underline{v}_1\right)} \underline{e}_{\underline{v}_1}\right) \left[\sum_{\underline{v}_2\in\mathbb{F}_q^n} y^{\mathrm{wt}\left(\underline{v}_2\right)} \zeta^{-\mathrm{tr}\left(\underline{u}_2^\top \underline{v}_2\right)}\right] \\ &\quad \left(\sum_{\underline{v}_3\in\mathbb{F}_q^m} \zeta^{-\mathrm{tr}\left(\underline{u}_3^\top \underline{v}_3\right)} \underline{e}_{\underline{v}_3}^\top\right). \end{aligned} \tag{8}$$

In particular, let $\mathfrak{F}_{q^m}$ be the standard q^m-point FFT matrix given by

$$\mathfrak{F}_{q^m} \;:=\; \sum_{\underline{u}\in\mathbb{F}_q^m}\sum_{\underline{v}\in\mathbb{F}_q^m} \zeta^{-\mathrm{tr}\left(\underline{u}^\top \underline{v}\right)} \underline{e}_{\underline{v}} \underline{e}_{\underline{u}}^\top;$$

$$\begin{aligned}
&F(\underline{u}_1,\underline{u}_2,\underline{u}_3) \qquad\qquad (4)\\
&= \sum_{(\underline{v}_1,\underline{v}_2,\underline{v}_3)\in\mathcal{V}} f\left(\underline{v}_1,\underline{v}_2,\underline{v}_3\right)\left[\chi_{\underline{u}}(\underline{v})\right]^*\\
&= \sum_{(\underline{v}_1,\underline{v}_2,\underline{v}_3)\in\mathcal{V}} \left[\prod_{i=1}^{m}\prod_{j=1}^{q} x_{i,j}^{\mathrm{wt}_j(\underline{v}_1)}\right] y^{\mathrm{wt}\left(\underline{v}_2\right)} \left[\prod_{i=1}^{m}\prod_{j=1}^{q} z_{i,j}^{\mathrm{wt}_j(\underline{v}_3)}\right] \zeta^{-\sum_{i=1}^{3}\mathrm{tr}(\underline{u}_i^\top\underline{v}_i)}\\
&= \left[\prod_{i=1}^{m}\left(\sum_{j=1}^{q}\zeta^{-\mathrm{tr}(u_{1,i}\omega_j)}x_{i,j}\right)\right](1+(q-1)y)^{n-\mathrm{wt}\left(\underline{u}_2\right)}(1-y)^{\mathrm{wt}\left(\underline{u}_2\right)}\left[\prod_{i=1}^{m}\left(\sum_{j=1}^{q}\zeta^{-\mathrm{tr}(u_{3,i}\omega_j)}z_{i,j}\right)\right]\\
&= \left[\prod_{i=1}^{m}\prod_{\ell=1}^{q}\left(\sum_{j=1}^{q}\zeta^{-\mathrm{tr}(\omega_\ell\omega_j)}x_{i,j}\right)^{\mathrm{wt}_\ell(u_{1,i})}\right](1+(q-1)y)^{n-\mathrm{wt}\left(\underline{u}_2\right)}(1-y)^{\mathrm{wt}\left(\underline{u}_2\right)}\left[\prod_{i=1}^{m}\prod_{\ell=1}^{q}\left(\sum_{j=1}^{q}\zeta^{-\mathrm{tr}(\omega_\ell\omega_j)}z_{i,j}\right)^{\mathrm{wt}_\ell(u_{3,i})}\right].
\end{aligned}$$

then (8) can be rewritten as

$$\begin{aligned}
&F_{\mathrm{mat}}(\underline{u}_1,\underline{u}_2,\underline{u}_3)\\
&= (1+(q-1)y)^{n-\mathrm{wt}\left(\underline{u}_2\right)}(1-y)^{\mathrm{wt}\left(\underline{u}_2\right)}\mathfrak{F}_{q^m}\underline{e}_{\underline{u}_1}\underline{e}_{\underline{u}_3}^\top\mathfrak{F}_{q^m}^\top.
\end{aligned}$$

Substituting the above into (2) yields the following result.

Theorem 5. The weight adjacency matrices for $\mathcal{C}_{(j)}^\perp$ and $\hat{\mathcal{C}}_{(j)}$ are given respectively by

$$\begin{aligned}
\Lambda_{\mathcal{C}_{(j)}^\perp}(y) &= \frac{(1+(q-1)y)^n}{q^{m+k}}\mathfrak{F}_{q^m}\Lambda_{\mathcal{C}_{(j)}}(\mathfrak{y})\,\mathfrak{F}_{q^m}^\top\\
\Lambda_{\hat{\mathcal{C}}_{(j)}}(y) &= \frac{(1+(q-1)y)^n}{q^{m+k}}\mathfrak{F}_{q^m}\Lambda_{\mathcal{C}_{(j)}}(\mathfrak{y})\,\mathfrak{F}_{q^m}^\dagger
\end{aligned}$$

where $\mathfrak{y} = \frac{1-y}{1+(q-1)y}$.

Same as before, when $\mathcal{C}_{(j)}$ is systematic, we can split the weights of $\underline{v}_2$ to formulate the following weight function

$$f_{\text{mat,IP}}\left(\underline{v}_1,\underline{v}_{2,I},\underline{v}_{2,P},\underline{v}_3\right) = y_I^{\mathrm{wt}\left(\underline{v}_{2,I}\right)}y_P^{\mathrm{wt}\left(\underline{v}_{2,P}\right)}\underline{e}_{\underline{v}_1}\underline{e}_{\underline{v}_3}^\top. \qquad (9)$$

This leads to the following duality for input-parity weight enumerators.

Corollary 6.

$$\begin{aligned}
\Lambda_{\mathcal{C}_{(j)}^\perp}(y_I,y_P) &= K\mathfrak{F}_{q^m}\Lambda_{\mathcal{C}_{(j)}}(\mathfrak{y}_I,\mathfrak{y}_P)\,\mathfrak{F}_{q^m}^\top,\\
\Lambda_{\hat{\mathcal{C}}_{(j)}}(y_I,y_P) &= K\mathfrak{F}_{q^m}\Lambda_{\mathcal{C}_{(j)}}(\mathfrak{y}_I,\mathfrak{y}_P)\,\mathfrak{F}_{q^m}^\dagger.
\end{aligned}$$

where $\mathfrak{y}_I = \frac{1-y_I}{1+(q-1)y_I}, \mathfrak{y}_P = \frac{1-y_P}{1+(q-1)y_P}$ and K is given in (5).

IV. Weight Enumeration for Convolutional Code $\mathcal{C}$

Let $\mathcal{C}$ be an (n,k,m) convolutional code over field $\mathbb{F}_q$. Recall that every codeword $\underline{c}\in\mathcal{C}$ is of the following form

$$\underline{c} \;=\; \sum_{i=0}^{d}\underline{c}_i D^i$$

for some $0\leq d<\infty$, with $\underline{c}_i\in\mathbb{F}_q^n$ and $\underline{c}_d\neq\underline{0}$. We will say that the degree of $\underline{c}$ is d, denoted by $\deg(\underline{c}) = d$. The Hamming weight of $\underline{c}\in\mathcal{C}$ is given by a linear extension of the usual Hamming weight function to module $\mathcal{M}$, i.e.

$$\mathrm{wt}\left(\underline{c}\right) \;=\; \sum_{i=0}^{\deg(\underline{c})}\mathrm{wt}\left(\underline{c}_i\right).$$

Similarly, the weight function of codewords $\underline{c}\in\mathcal{C}$ is given by the following in indeterminates y and D

$$f_D(\underline{c}) \;:=\; y^{\mathrm{wt}(\underline{c})}D^{\deg(\underline{c})}. \qquad (10)$$

Thus, the weight enumeration of all codewords $\underline{c}\in\mathcal{C}$ is

$$W_{\mathcal{C}}(y,D) \;=\; \sum_{\underline{c}\in\mathcal{C}} f_D(\underline{c}). \qquad (11)$$

The following lemma is almost trivial from the definition of constraint code $\mathcal{C}_{(j)}$ as well as the states $\underline{w}_j$.

Lemma 7.

$$W_{\mathcal{C}}(y,D) \;=\; \underline{e}_{\underline{0}}^\top\left(\mathtt{I}-\Lambda_{\mathcal{C}_{(j)}}(y)D\right)^{-1}\underline{e}_{\underline{0}}. \qquad (12)$$

Proof. Note that any codeword $\underline{c}\in\mathcal{C}$ with $\deg(\underline{c}) = d$ must satisfy states $\underline{w}_0 = \underline{0}$ and $\underline{w}_j = \underline{0}$ for all $j\geq d+1$. Hence

$$\sum_{\substack{\underline{c}\in\mathcal{C}\\ \deg(\underline{c})\leq d}} f_D(\underline{c}) \;=\; \sum_{i=0}^{d}\underline{e}_{\underline{0}}^\top\left(\Lambda_{\mathcal{C}_{(j)}}(y)\right)^i D^i\underline{e}_{\underline{0}}.$$

Take $d\to\infty$ and the result follows. □

Applying Theorem 5 to the above lemma gives the following corollary.

Corollary 8.

$$\begin{aligned}
&W_{\mathcal{C}^\perp}(y,D)\\
&\quad= \frac{1}{q^m}\,\underline{\mathbf{1}}^\top\left[\mathtt{I}-\frac{(1+(q-1)y)^n}{q^k}\Lambda_{\mathcal{C}_{(j)}}(\mathfrak{y})\,D\right]^{-1}\underline{\mathbf{1}}
\end{aligned}$$

where $\underline{\mathbf{1}}$ denotes the all-one vector of length q^m, and $\mathfrak{y} =$

$\frac{1-y}{1+(q-1)y}$.

Proof. It follows from definition of $W_{\mathcal{C}^\perp}(y,D)$ and Theorem 5 that

$$\begin{aligned}&W_{\mathcal{C}^\perp}(y,D)\\&=\underline{e}_{\underline{0}}^\top\left(\mathtt{I}-\Lambda_{\hat{\mathcal{C}}_{(j)}}(y)D\right)^{-1}\underline{e}_{\underline{0}}\\&=\underline{e}_{\underline{0}}^\top\left[\mathtt{I}-\frac{(1+(q-1)y)^n}{q^{m+k}}\mathfrak{F}_{q^m}\Lambda_{\mathcal{C}_{(j)}}(\mathfrak{y})\,\mathfrak{F}_{q^m}^\dagger D\right]^{-1}\underline{e}_{\underline{0}}\\&=\frac{1}{q^m}\underline{e}_{\underline{0}}^\top\mathfrak{F}_{q^m}\left[\mathtt{I}-\frac{(1+(q-1)y)^n}{q^k}\Lambda_{\mathcal{C}_{(j)}}(\mathfrak{y})\,D\right]^{-1}\mathfrak{F}_{q^m}^\dagger\underline{e}_{\underline{0}}.\end{aligned}$$

□

While Corollary 8 does not show the duality between $W_\mathcal{C}(y,D)$ and $W_{\mathcal{C}^\perp}(y,D)$, we may reconsider enumerating walks on the full trellis diagram[1] of $\mathcal{C}$ in a matrix, i.e.,

$$\Lambda_\mathcal{C}(y,D)\ :=\ \left(\mathtt{I}-\Lambda_{\mathcal{C}_{(j)}}(y)D\right)^{-1}=\sum_{d\geq 0}\left(\Lambda_{\mathcal{C}_{(j)}}(y)\right)^d D^d$$

whose $(\underline{w},\underline{w}')$th entry of matrix $\left(\Lambda_{\mathcal{C}_{(j)}}(y)\right)^d$ is the enumeration of the Hamming weights of length-d walks that begin at state $\underline{w}$ at time 0 and end at state $\underline{w}'$ at time d on the full trellis diagram of $\mathcal{C}$. Clearly, we have $W_\mathcal{C}(y,D)=\underline{e}_{\underline{0}}^\top\Lambda_\mathcal{C}(y,D)\underline{e}_{\underline{0}}$. It then follows from the proof of Corollary 8 that

$$\Lambda_{\mathcal{C}^\perp}(y,D)\ =\ \frac{1}{q^m}\mathfrak{F}_{q^m}\Lambda_\mathcal{C}\left(\mathfrak{y},\ \frac{(1+(q-1)y)^n}{q^k}D\right)\mathfrak{F}_{q^m}^\dagger$$

and $W_{\mathcal{C}^\perp}(y,D)=\underline{e}_{\underline{0}}^\top\Lambda_{\mathcal{C}^\perp}(y,D)\underline{e}_{\underline{0}}$.

Let $\mathcal{C}$ be a systematic convolutional code. For any codeword $\underline{c}\in\mathcal{C}$, let the weight function of $\underline{c}$ be

$$f_{D,\mathrm{IP}}(\underline{c})=y_I^{\sum_{i=0}^{\deg(\underline{c})}\mathrm{wt}\left(\underline{c}_{i,I}\right)}y_P^{\sum_{i=0}^{\deg(\underline{c})}\mathrm{wt}\left(\underline{c}_{i,P}\right)}D^{\deg(\underline{c})}$$

where $\underline{c}_i\ =\ \left[\underline{c}_{i,I}^\top\ \underline{c}_{i,P}^\top\right]^\top$ defined as before, and let $W_\mathcal{C}(y_I,y_P,D)$ (resp. $\Lambda_\mathcal{C}(y_I,y_P,D)$) be the input-parity weight enumerator (resp. input-parity weight adjacency matrix) for codewords of $\mathcal{C}$ (resp. walks on the full trellis diagram of $\mathcal{C}$) defined with respect to the above weight function. Let $\mathcal{C}^\perp$ be the dual code of $\mathcal{C}$. Finally, we state the duality result for input-parity weight enumerator for a systematic convolutional code $\mathcal{C}$ in the following theorem.

Theorem 9.

$$\Lambda_{\mathcal{C}^\perp}(y_I,y_P,D)=\frac{1}{q^m}\mathfrak{F}_{q^m}\Lambda_\mathcal{C}\left(\mathfrak{y}_I,\mathfrak{y}_P,K'D\right)\mathfrak{F}_{q^m}^\dagger,\qquad(13)$$

where

$$K'=\ \frac{(1+(q-1)y_I)^k(1+(q-1)y_P)^{n-k}}{q^k}.$$

Furthermore,

$$\begin{aligned}W_\mathcal{C}(y_I,y_P,D)&=&\underline{e}_{\underline{0}}^\top\Lambda_\mathcal{C}(y_I,y_P,D)\underline{e}_{\underline{0}}\\W_{\mathcal{C}^\perp}(y_I,y_P,D)&=&\underline{e}_{\underline{0}}^\top\Lambda_{\mathcal{C}^\perp}(y_I,y_P,D)\underline{e}_{\underline{0}}.\end{aligned}$$

V. Some Remarks on the Free-Distance Enumerator

Definition 10. Let $\mathcal{C}$ be an (n,k,m) convolutional code. The set $\mathcal{C}_{\text{free}}$ consists of codewords $\underline{c}$ whose state begins at $\underline{w}_0=\underline{0}$ and merges back into $\underline{0}$ at some smallest time instant d. More precisely,

$$\mathcal{C}_{\text{free}}\ =\ \left\{\sum_{d\geq 0}\sum_{j=0}^{d}\underline{p}_jD^j\ :\ \begin{array}{l}\left[\underline{w}_j^\top\ \underline{p}_j^\top\ \underline{w}_{j+1}^\top\right]^\top\in\mathcal{C}_{(j)},j=0,\ldots,d,\\ \underline{w}_0=\underline{w}_{d+1}=\underline{0},\underline{w}_j\neq\underline{0}\text{ for }j=1,\ldots,d\end{array}\right\}.\qquad(14)$$

Clearly, as an $\mathbb{F}_q[D]$-module, the code $\mathcal{C}$ is generated by $\mathcal{C}_{\text{free}}$ over $\mathbb{F}_q[D]$. But it should be noted that $\mathcal{C}_{\text{free}}$ is not necessarily linear independent over $\mathbb{F}_q[D]$ nor a submodule of $\mathcal{M}$.

Following the notation in the previous section, we can define the free-distance enumerator that enumerates the codewords in $\mathcal{C}_{\text{free}}$ as

$$W_{\mathcal{C}_{\text{free}}}(y,D)\ =\ \sum_{\underline{c}\in\mathcal{C}_{\text{free}}}f_D(\underline{c}).\qquad(15)$$

It should be noted that the above enumerator differs from the conventional transfer function for convolutional codes in the sense that the zero element $\underline{0}\in\mathcal{M}$ is excluded in the latter.

The weight enumerator $W_{\mathcal{C}_{\text{free}}}(y,D)$ can be easily determined by the weight adjacency matrix of the constraint code $\mathcal{C}_{(j)}$.

Proposition 11. Let $\Lambda_{\mathcal{C}_{(j)}}(y)$ be the $q^m\times q^m$ weight adjacency matrix for the constraint code $\mathcal{C}_{(j)}$. Then

$$W_{\mathcal{C}_{\text{free}}}(y,D)\ =\ \underline{e}_{\underline{0}}^\top\left[\mathtt{I}-\left(\Lambda_{\mathcal{C}_{(j)}}(y)-\underline{e}_{\underline{0}}\underline{e}_{\underline{0}}^\top\right)D\right]^{-1}\underline{e}_{\underline{0}}.\qquad(16)$$

Proof. Straightforward. □

Remark: The conventional transfer function of convolutional codes is given by $W_{\mathcal{C}_{\text{free}}}(y,D)-f_D(\underline{0})=W_{\mathcal{C}_{\text{free}}}(y,D)-1$. Secondly, the minimal free-distance d_{free} of $\mathcal{C}$ can be obtained by a power-series expansion of $W_{\mathcal{C}_{\text{free}}}(y,D)$ in y, that is,

$$W_{\mathcal{C}_{\text{free}}}(y,D)\ =\ 1+\sum_{i\geq d_{\text{free}}}\lambda_i\ y^i$$

for some rational function $\lambda_i\in\mathbb{F}_q(D)$ with $\lambda_{d_{\text{free}}}\neq 0$.

Note that the weight enumerator for codewords $\underline{c}\in\mathcal{C}$ is given by $W_\mathcal{C}(y,D)\ =\ \underline{e}_{\underline{0}}^\top\left(\mathtt{I}-\Lambda_{\mathcal{C}_{(j)}}(y)D\right)^{-1}\underline{e}_{\underline{0}}$. Also, by rewriting (16) as

$$W_{\mathcal{C}_{\text{free}}}(y,D)\ =\ \underline{e}_{\underline{0}}^\top\left[\left(\mathtt{I}-\Lambda_{\mathcal{C}_{(j)}}(y)D\right)+\underline{e}_{\underline{0}}\underline{e}_{\underline{0}}^\top D\right]^{-1}\underline{e}_{\underline{0}}$$

and applying the Woodbury identity to the middle matrix, we can relate $W_{\mathcal{C}_{\text{free}}}(y,D)$ to $W_\mathcal{C}(y,D)$ as shown in the following corollary.

[1] By the full trellis diagram of $\mathcal{C}$ we mean the trellis diagram of $\mathcal{C}$ with arbitrary beginning and ending states.

Corollary 12.

$$\begin{aligned} W_{\mathcal{C}_{\text{free}}}(y,D) &= \frac{W_{\mathcal{C}}(y,D)}{1+W_{\mathcal{C}}(y,D)D} \\ W_{\mathcal{C}}(y,D) &= \frac{W_{\mathcal{C}_{\text{free}}}(y,D)}{1-W_{\mathcal{C}_{\text{free}}}(y,D)D} \end{aligned}$$

Proof. By Woodbury identity for matrix inverse we have

$$\begin{aligned} & \left[\left(\mathtt{I}-\Lambda_{\mathcal{C}_{(j)}}(y)D\right)+\underline{e}_{\underline{0}}\underline{e}_{\underline{0}}^{\top}D\right]^{-1} \\ = \; & \left(\mathtt{I}-\Lambda_{\mathcal{C}_{(j)}}(y)D\right)^{-1}-\frac{D}{1+\underline{e}_{\underline{0}}^{\top}\left(\mathtt{I}-\Lambda_{\mathcal{C}_{(j)}}(y)D\right)^{-1}\underline{e}_{\underline{0}}D} \\ \times \; & \left(\mathtt{I}-\Lambda_{\mathcal{C}_{(j)}}(y)D\right)^{-1}\underline{e}_{\underline{0}}\underline{e}_{\underline{0}}^{\top}\left(\mathtt{I}-\Lambda_{\mathcal{C}_{(j)}}(y)D\right)^{-1}, \end{aligned}$$

which in turn gives

$$\begin{aligned} W_{\mathcal{C}_{\text{free}}}(y,D) &= W_{\mathcal{C}}(y,D)-\frac{\left(W_{\mathcal{C}}(y,D)\right)^2 D}{1+W_{\mathcal{C}}(y,D)D} \\ &= \frac{W_{\mathcal{C}}(y,D)}{1+W_{\mathcal{C}}(y,D)D}. \end{aligned}$$

The second expression is then immediate. □

Remark: A much simpler way to prove Corollary 12 is to show the second expression directly. Note that $\mathcal{C}$ is generated by $\mathcal{C}_{\text{free}}$ over $\mathbb{F}_q[D]$, hence the result follows from the standard argument in enumerative combinatorics.

Let $\mathcal{C}^{\perp}_{\text{free}}$ be the set consisting of the zero-path diverging codewords in $\mathcal{C}^{\perp}$ and let $W_{\mathcal{C}^{\perp}_{\text{free}}}(y,D)=\sum_{\underline{c}\in\mathcal{C}^{\perp}_{\text{free}}} f_D(\underline{c})$ be the corresponding weight enumerator. Then by Corollary 12 we get

$$W_{\mathcal{C}^{\perp}_{\text{free}}}(y,D) = \frac{W_{\mathcal{C}^{\perp}}(y,D)}{1+W_{\mathcal{C}^{\perp}}(y,D)D}.$$

One implication of the above is the following. There is a one-one correspondence, i.e. a duality, between $\Lambda_{\mathcal{C}}(y,D)$ and $\Lambda_{\mathcal{C}^{\perp}}(y,D)$ but not for $W_{\mathcal{C}}(y,D)$ and $W_{\mathcal{C}}^{\perp}(y,D)$ since $W_{\mathcal{C}}(y,D)$ corresponds only to the entry of $\Lambda_{\mathcal{C}}(y,D)$ associated with $(\underline{0},\underline{0})$ as shown in Lemma 7. Thus, there is no one-one correspondence between $W_{\mathcal{C}_{\text{free}}}(y,D)$ and $W_{\mathcal{C}^{\perp}_{\text{free}}}(y,D)$ as observed by Shearer and McEliece more than 40 years ago. On the other hand, let

$$\Lambda_{\mathcal{C}_{\text{free}}}(y,D) = \left[\left(\mathtt{I}-\Lambda_{\mathcal{C}_{(j)}}(y)D\right)+\underline{e}_{\underline{0}}\underline{e}_{\underline{0}}^{\top}D\right]^{-1} \tag{17}$$

and

$$\Lambda_{\mathcal{C}^{\perp}_{\text{free}}}(y,D) = \left[\left(\mathtt{I}-\Lambda_{\mathcal{C}^{\perp}_{(j)}}(y)D\right)+\underline{e}_{\underline{0}}\underline{e}_{\underline{0}}^{\top}D\right]^{-1} \tag{18}$$

denote the enumerations of length-d walks from state $\underline{w}$ to $\underline{w}'$ without immediate loops at state $\underline{0}$ in the full trellis diagrams of $\mathcal{C}$ and $\mathcal{C}^{\perp}$, respectively. Clearly,

$$\begin{aligned} W_{\mathcal{C}_{\text{free}}}(y,D) &= \underline{e}_{\underline{0}}^{\top}\Lambda_{\mathcal{C}_{\text{free}}}(y,D)\underline{e}_{\underline{0}} \\ W_{\mathcal{C}^{\perp}_{\text{free}}}(y,D) &= \underline{e}_{\underline{0}}^{\top}\Lambda_{\mathcal{C}^{\perp}_{\text{free}}}(y,D)\underline{e}_{\underline{0}}. \end{aligned}$$

Most importantly, there is indeed a one-one correspondence between $\Lambda_{\mathcal{C}_{\text{free}}}(y,D)$ and $\Lambda_{\mathcal{C}^{\perp}_{\text{free}}}(y,D)$ implied by (IV). We summarize the above in the Figure 1. Potentially, we can also obtaining an explicit formula connecting $\Lambda_{\mathcal{C}_{\text{free}}}(y,D)$ and $\Lambda_{\mathcal{C}^{\perp}_{\text{free}}}(y,D)$, however, it of less significance in combinatorial mathematics.

$$\begin{tikzcd}
\Lambda_{\mathcal{C}_{\text{free}}}(y,D) \arrow[r, leftrightarrow] \arrow[ddr, bend right] & \Lambda_{\mathcal{C}}(y,D) \arrow[r, leftrightarrow] \arrow[d] & \Lambda_{\mathcal{C}^{\perp}}(y,D) \arrow[r, leftrightarrow] \arrow[d] & \Lambda_{\mathcal{C}^{\perp}_{\text{free}}}(y,D) \arrow[ddl, bend left] \\
 & W_{\mathcal{C}}(y,D) \arrow[d, leftrightarrow] & W_{\mathcal{C}^{\perp}}(y,D) \arrow[d, leftrightarrow] & \\
 & W_{\mathcal{C}_{\text{free}}}(y,D) & W_{\mathcal{C}^{\perp}_{\text{free}}}(y,D) &
\end{tikzcd}$$

Fig. 1. Relations diagram of various weight enumerations. A relation $A \to B$ means that B can be derived given A.

VI. Discussion and Conclusion

The main achievement in this paper is the relationship between various notions of weight functions studied in the classical convolutional code literature, summarized in Fig. 1. As opposed to the classical coding theory, there is a growing interest in investigating these fundamental questions in quantum coding theory [7], [8]. Indeed, the MacWilliams identities have recently been established for quantum error-correcting codes [9], [10] and quantum convolutional codes [11].

The next question to ask from here is whether the MacWilliams identity can be established for turbo codes, and if so, is there any benefit?

A complete version of this work is available in Ref. [12].

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 and G. Schneider, “On the MacWilliams identity for convolutional codes,” *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1536–1550, 2008.

[4] J. Forney, G.D., “Codes on graphs: Duality and MacWilliams identities,” *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1382–1397, 2011.

[5] H.-F. Lu, P. Kumar, and E. hui Yang, “On the input-output weight enumerators of product accumulate codes,” *IEEE Communications Letters*, vol. 8, no. 8, pp. 520–522, Aug 2004.

[6] M.-C. Chiu and H.-F. Lu, “Accumulate codes based on 1+D convolutional outer codes,” *Communications, IEEE Transactions on*, vol. 57, no. 2, pp. 311–314, February 2009.

[7] T. A. Brun, I. Devetak, and M.-H. Hsieh, “Correcting quantum errors with entanglement,” *Science*, vol. 314, pp. 436–439, 2006.

[8] T. A. Brun, I. Devetak, and M.-H. Hsieh, “Catalytic Quantum Error Correction,” to appear in *IEEE Trans. Inf Theory*, 2014. (doi = 10.1109/TIT.2014.2313559).

[9] 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.

[10] 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.

[11] C.-Y. Lai and M.-H. Hsieh, “The Macwilliams identity for quantum convolutional codes,” in *to appear in Proc. IEEE ISIT 2014*.

[12] C.-Y. Lai, M.-H. Hsieh, and H.-F. Lu., “On the Macwilliams identity for classical and quantum convolutional codes,” 2014. [Online]. Available: http://arxiv.org/abs/1404.5012