MacWilliams identities for codes on graphs

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>As Published</td>
<td><a href="http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5351248">http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5351248</a></td>
</tr>
<tr>
<td>Publisher</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>Version</td>
<td>Final published version</td>
</tr>
<tr>
<td>Accessed</td>
<td>Wed Oct 17 03:21:17 EDT 2018</td>
</tr>
<tr>
<td>Citable Link</td>
<td><a href="http://hdl.handle.net/1721.1/59361">http://hdl.handle.net/1721.1/59361</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.</td>
</tr>
<tr>
<td>Detailed Terms</td>
<td></td>
</tr>
</tbody>
</table>
Abstract—The MacWilliams identity for linear time-invariant convolutional codes that has recently been found by Gluesing-Luerssen and Schneider is proved concisely, and generalized to arbitrary group codes on graphs. A similar development yields a short, transparent proof of the dual sum-product update rule.

I. INTRODUCTION

Finding a MacWilliams-type identity for convolutional codes is a problem of long standing. Recently Gluesing-Luerssen and Schneider (GLS) have formulated [1] and proved [2] such an identity involving the (Hamming) weight adjacency matrix (WAM) of a linear time-invariant convolutional code over a finite field and the WAM of its orthogonal code.

The purpose of this note is to provide a concise group-theoretic proof of this identity, and to generalize it to arbitrary group codes defined on graphs. We use first the general duality code over a finite field and the WAM of its orthogonal code.

Let $\mathcal{C} \subseteq \mathcal{A}$ be a group or linear code involving certain subsets of the symbol and state variables. The full behavior of the realization is the set $\mathcal{B} = (a, s)$ of all configurations of symbol variables $a \in \mathcal{A}$ and state variables $s \in \mathcal{S} = \bigcap_{j \in \mathcal{I}_S} S_j$ such that all constraints are satisfied. The code generated by the realization is the projection $\mathcal{C} = \mathcal{B}|\mathcal{A}$ of $\mathcal{B}$ onto $\mathcal{A}$; i.e., the set of all symbol configurations $a \in \mathcal{A}$ that appear in some $(a, s) \in \mathcal{B}$.

For example, in a conventional state realization of a linear code $\mathcal{C}$ over a finite field $\mathbb{F}$, the symbol index set $\mathcal{I}_A$ is a conventional discrete time axis, namely the set of integers $\mathbb{Z}$, or a subinterval of $\mathbb{Z}$. The state index set $\mathcal{I}_S$ may be thought of as the set of times that occur between consecutive pairs of times in $\mathcal{I}_A$, and the state time preceding symbol time $k \in \mathcal{I}_A$ is conventionally also denoted by $k \in \mathcal{I}_S$. The constraint codes $\{\mathcal{C}_k, k \in \mathcal{I}_A\}$ are linear codes indexed by the symbol index set $\mathcal{I}_A$, and specify the set of all valid $(s_k, a_k, s_{k+1})$ transitions; i.e., for each $k \in \mathcal{I}_A$, $\mathcal{C}_k$ is a subspace of the Cartesian product vector space $S_k \times A_k \times S_{k+1}$. The full behavior $\mathcal{B}$ of the realization is the set of all symbol/state trajectories $(a, s)$ such that $(s_k, a_k, s_{k+1})$ is a valid transition in $\mathcal{C}_k$ for all $k \in \mathcal{I}_A$. The code $\mathcal{C}$ generated by the realization is the set of all symbol trajectories $a$ that appear in some $(a, s) \in \mathcal{B}$.

A normal realization is defined as a generalized state realization in which every symbol variable is involved in precisely one constraint code, and every state variable is involved in precisely two constraint codes. Thus a conventional state realization is normal. It is shown in [3] that any generalized state realization may be straightforwardly converted to a normal realization by introducing replication constraints, without essentially increasing the complexity of the realization.

A normal realization has a natural graphical model, in which each constraint code $\mathcal{C}_i$ corresponds to a vertex, each state variable $S_j$ (which by definition is involved in two constraints) corresponds to an edge connecting the two corresponding constraint vertices, and each symbol variable $A_k$ (which by definition is involved in one constraint) corresponds to a leaf or “half-edge” connected to the corresponding constraint vertex.

For example, Figure 1 shows the graph corresponding to a conventional state realization, which is a simple chain graph. Here vertices are represented by square boxes, and the “half-
III. DUAL NORMAL REALIZATIONS

The central duality result of [3] is the following: given a normal realization of a code $C$, the dual normal realization generates the dual code $C^\perp$. For simplicity of exposition, we will explain this result only for the case where $C$ is a linear code over a finite field $F$, but it holds also in the group case; see [3]. In the linear case, the dual code $C^\perp$ is the usual orthogonal code to $C$ under the usual symbolwise inner product.

We have seen that a normal realization for $C$ is defined by a set of symbol variables $\{A_k, k \in I_A\}$, a set of state variables $\{S_j, j \in I_S\}$, and a set of constraint codes $\{C_i, i \in I_C\}$, where each symbol variable is involved in one constraint code, and each state variable is involved in two constraint codes.

The definition of a dual normal realization is slightly simpler in the case of a linear code $C$ over the binary field $F_2$ than in the general case, so we discuss the binary case first. Then the dual normal realization is defined by the same sets of symbol and state variables, and by the set of orthogonal constraint codes $\{C^\perp_i, i \in I_C\}$, each involving the same variables as in the primal realization. The graph of the dual realization is thus the same as the graph of the primal realization, except that each constraint code $C_i$ is replaced by its orthogonal code $C^\perp_i$.

Example 1. Consider the rate-1/2 binary linear time-invariant convolutional code $C$ generated by the degree-2 generators $(1 + D^2, 1 + D + D^2)$, in standard $D$-transform notation. In other words, $C$ is the set of all output sequences of the single-input, two-output linear time-invariant system over $F_2$ whose impulse response is $(11, 01, 11, 00, \ldots)$. This system has a conventional four-state realization as in Figure 1 in which each symbol variable $A_k$ may be taken as $(F_2)^2$, each state variable $S_k$ may also be taken as $(F_2)^2$, and each constraint code $C_k$ is the $(6, 3)$ binary linear block code generated by the three generators

$$
\begin{array}{c|c|c}
00 & 11 & 10 \\
10 & 01 & 01 \\
01 & 11 & 00 \\
\end{array}
$$

which represent the three nontrivial (state, symbol, next-state) transitions in the impulse response of the system. The orthogonal code $C^\perp_k$ may easily be seen to be the $(6, 3)$ binary linear block code generated by the three generators

$$
\begin{array}{c|c|c}
00 & 11 & 01 \\
01 & 10 & 10 \\
10 & 11 & 00 \\
\end{array}
$$

which represent the three nontrivial (state, symbol, next-state) transitions in the impulse response of the system. The orthogonal code $C^\perp_k$ may easily be seen to be the $(6, 3)$ binary linear block code generated by the three generators

$$
\begin{array}{c|c|c}
00 & 11 & 01 \\
01 & 10 & 10 \\
10 & 11 & 00 \\
\end{array}
$$

which represent the three nontrivial (state, symbol, next-state) transitions in the impulse response of the system. The orthogonal code $C^\perp_k$ may easily be seen to be the $(6, 3)$ binary linear block code generated by the three generators

$$
\begin{array}{c|c|c}
00 & 11 & 01 \\
01 & 10 & 10 \\
10 & 11 & 00 \\
\end{array}
$$

which represent the three nontrivial (state, symbol, next-state) transitions in the impulse response of the system. The orthogonal code $C^\perp_k$ may easily be seen to be the $(6, 3)$ binary linear block code generated by the three generators

$$
\begin{array}{c|c|c}
00 & 11 & 01 \\
01 & 10 & 10 \\
10 & 11 & 00 \\
\end{array}
$$

which represent the three nontrivial (state, symbol, next-state) transitions in the impulse response of the system. The orthogonal code $C^\perp_k$ may easily be seen to be the $(6, 3)$ binary linear block code generated by the three generators

$$
\begin{array}{c|c|c}
00 & 11 & 01 \\
01 & 10 & 10 \\
10 & 11 & 00 \\
\end{array}
$$

which represent the three nontrivial (state, symbol, next-state) transitions in the impulse response of the system. The orthogonal code $C^\perp_k$ may easily be seen to be the $(6, 3)$ binary linear block code generated by the three generators

$$
\begin{array}{c|c|c}
00 & 11 & 01 \\
01 & 10 & 10 \\
10 & 11 & 00 \\
\end{array}
$$

which represent the three nontrivial (state, symbol, next-state) transitions in the impulse response of the system. The orthogonal code $C^\perp_k$ may easily be seen to be the $(6, 3)$ binary linear block code generated by the three generators

$$
\begin{array}{c|c|c}
00 & 11 & 01 \\
01 & 10 & 10 \\
10 & 11 & 00 \\
\end{array}
$$

which represent the three nontrivial (state, symbol, next-state) transitions in the impulse response of the system. The orthogonal code $C^\perp_k$ may easily be seen to be the $(6, 3)$ binary linear block code generated by the three generators

$$
\begin{array}{c|c|c}
00 & 11 & 01 \\
01 & 10 & 10 \\
10 & 11 & 00 \\
\end{array}
$$

which represent the three nontrivial (state, symbol, next-state) transitions in the impulse response of the system. The orthogonal code $C^\perp_k$ may easily be seen to be the $(6, 3)$ binary linear block code generated by the three generators

$$
\begin{array}{c|c|c}
00 & 11 & 01 \\
01 & 10 & 10 \\
10 & 11 & 00 \\
\end{array}
$$

which represent the three nontrivial (state, symbol, next-state) transitions in the impulse response of the system. The orthogonal code $C^\perp_k$ may easily be seen to be the $(6, 3)$ binary linear block code generated by the three generators

$$
\begin{array}{c|c|c}
00 & 11 & 01 \\
01 & 10 & 10 \\
10 & 11 & 00 \\
\end{array}
$$
in the impulse response of a conventional state realization of a single-input, three-output linear system over \( \mathbb{F}_q \), with sign inverters as in Figure 2, whose impulse response is \((010, 202, 111, 000, \ldots)\), or \((2D + D^2, 1 + D^2, 2D + D^2)\) in \( D \)-transform notation. (Note the unconventional basis of the dual state space.) This is indeed the generator of the orthogonal convolutional code \( \mathbb{C}^\perp \) under our symbolwise definition of the inner product. (For the more usual sequence-wise definition of the inner product, we need to take the time-reversal of \( \mathbb{C}^\perp \), which in this case is the code generated by \((1 + 2D, 1 + D^2, 1 + 2D)\).)

IV. MacWilliams Identities

Given these duality results, various MacWilliams-type identities may be obtained in a more or less standard manner. We follow the development in [4].

Every finite abelian group \( T \) is a direct product of cyclic groups. In particular, every finite field \( T \) has \( q = p^m \) elements for some prime \( p \) and is isomorphic as an additive group to \((\mathbb{Z}_p)^m\), and every vector space over a finite field \( \mathbb{F}_p^m \) of dimension \( d \) is isomorphic to \((\mathbb{Z}_p)^{md} \). Thus, for some integer \( n \), we may take \( T = (\mathbb{Z}_p)^n \), the set of \( n \)-tuples of elements of \( \mathbb{Z}_p \).

Given a complex-valued function \( \{ x : T \to \mathbb{C}, t \mapsto x(t) \} \) defined on \( T = (\mathbb{Z}_p)^n \), its (Fourier) transform is the complex-valued function \( \{ X : \mathbb{F} \to \mathbb{C}, f \mapsto X(f) \} \) defined on \( \mathbb{F} = (\mathbb{Z}_p)^n \) by

\[
X(f) = \sum_{t \in T} x(t) \omega^{f \cdot t}, \quad f \in \mathbb{F},
\]

where \( \omega \) is a primitive complex \( p \)-th root of unity, and \( f \cdot t \in \mathbb{Z}_p \) is the ordinary dot product between the \( n \)-tuples \( f \in (\mathbb{Z}_p)^n \) and \( t \in (\mathbb{Z}_p)^n \) over \( \mathbb{Z}_p \). If we view \( x = \{ x(t), t \in T \} \) as a vector indexed by \( T \), and similarly \( X = \{ X(f), f \in \mathbb{F} \} \) as a vector indexed by \( \mathbb{F} \), then the transform can be expressed in matrix form as

\[
X = \mathcal{H}x,
\]

where \( \mathcal{H} \) is the transform matrix. Note that \( \mathcal{H}^T = \mathcal{H} \), where \( \mathcal{H}^T \) denotes the transpose of \( \mathcal{H} \).

From the orthogonality relation

\[
\sum_{f} \omega^{f \cdot t} = \begin{cases} |\mathbb{F}|, & t = 0; \\ 0, & t \neq 0, \end{cases}
\]

we obtain the matrix equation

\[
\mathcal{H}^* = [\mathbb{F}]_I[|\mathbb{F}|],
\]

where \( \mathcal{H}^* = \{ \omega^{f \cdot t}, f \in \mathbb{F}, t \in T \}, |\mathbb{F}| = |T| = p^n \), and \( I[|\mathbb{F}|] \) is the \([|\mathbb{F}| \times |\mathbb{F}|] \) identity matrix. In other words, the inverse of \( \mathcal{H} \) is \( \mathcal{H}^{-1} = [\mathbb{F}]^{-1} \mathcal{H}^* \). Thus we obtain the inverse transform

\[
x = \mathcal{H}^{-1}X = \frac{\mathcal{H}^*X}{|\mathbb{F}|}.
\]

We say that \( x \) and \( X \) are a transform pair.

We may extend these definitions to a set of indeterminates \( \mathbf{z} = \{ z(t), t \in T \} \) indexed by \( T \), rather than a complex-valued function. The transform of this set is then a set of indeterminates \( \mathbf{Z} = \{ Z(f), f \in \mathbb{F} \} \) indexed by \( \mathbb{F} \), where

\[
Z = \mathcal{H}z.
\]

Again, we have the inverse transform relationship

\[
z = \mathcal{H}^{-1}Z = \frac{\mathcal{H}^*Z}{|\mathbb{F}|},
\]

and we say that \( z \) and \( Z \) are a transform pair.

For example, if \( T = \mathbb{Z}_2 \), then \( Z(0) = z(0) + z(1) \) and \( Z(1) = z(0) - z(1) \); similarly, \( z(0) = \frac{1}{2}(Z(0) + Z(1)) \), and \( z(1) = \frac{1}{2}(Z(0) - Z(1)) \).

Now let us consider weight enumerators, initially for the case of a conventional state realization over a finite field \( \mathbb{F} \) as in Figure 1. We define the complete weight adjacency matrix (CWAM) of each constraint code \( \mathbb{C} \subseteq S_k \times A_k \times S_{k+1} \) as follows.

If \( A_k = \mathbb{F}^n \), then define the complete weight enumerator of the \( n \)-tuple \( a = (a_1, \ldots, a_n) \in \mathbb{F}^n \) as the product \( w(a) = \prod_{1 \leq i \leq n} w(a_i) \), where \( w = \{ w(a), a \in \mathbb{F} \} \) is a set of indeterminates indexed by \( \mathbb{F} \). Then the CWAM of \( \mathbb{C} \) is the matrix \( \Lambda(w) = \{ \Lambda(s_k, s_{k+1})(w), (s_k, s_{k+1}) \in S_k \times S_{k+1} \} \) defined by

\[
\Lambda(s_k, s_{k+1})(w) = \sum_{C(s_k, s_{k+1})} w(a_k),
\]

where \( C(s_k, s_{k+1}) = \{ a_k \mid (s_k, a_k, s_{k+1}) \in \mathbb{C} \} \). Thus each entry \( \Lambda(s_k, s_{k+1})(w) \) is a homogeneous integer polynomial of degree \( n \) in the \( \mathbb{F} \) indeterminates \( w = \{ w(a), a \in \mathbb{F} \} \).

Now let \( y = \{ y(s_k), s_k \in S_k \} \) and \( z = \{ z(s_{k+1}), s_{k+1} \in S_{k+1} \} \) be sets of indeterminates indexed by the state variables \( S_k \) and \( S_{k+1} \), respectively, and define a generating function \( g_{\Lambda(w)}(y, z) \), a polynomial in the sets of indeterminates \( y \) and \( z \), as follows:

\[
g_{\Lambda(w)}(y, z) = y^T \Lambda(w) z = \sum_{S_k \times S_{k+1}} y(s_k) \Lambda(s_k, s_{k+1})(w) z(s_{k+1}).
\]

From the definition \( C(s_k, s_{k+1}) = \{ a_k \mid (s_k, a_k, s_{k+1}) \in \mathbb{C} \} \), it follows that

\[
g_{\Lambda(w)}(y, z) = \sum_{(s_k, a_k, s_{k+1}) \in \mathbb{C}} y(s_k) w(a_k) z(s_{k+1}).
\]

Example 1 (cont.). The constraint code of Example 1 has the eight codewords \( 00000000, 00111010, 10101110, 01010001, 11001011, 01000100, 11101101, 11110111 \), corresponding to the eight possible (state, symbol, next-state) transitions. Writing \( \{ w_0, w_1 \} \) instead of \( \{ w(0), w(1) \} \), we see that we may write the CWAM of this constraint code in matrix form
As
\[
\Lambda(w) = \begin{array}{cccccc}
0 & 10 & 01 & 11 \\
00 & w_0^2 & 0 & 0 \\
10 & 0 & 0 & w_0 w_1 \\
01 & w_1^2 & w_0^2 & 0 \\
11 & 0 & 0 & w_0 w_1 \\
\end{array}
\]

Equivalently, its generating function \(g_{\Lambda(w)}(y, z)\) is
\[
g_{\Lambda(w)}(y, z) = w_0^2(y_00 z_{00} + y_01 z_{10}) + w_1^2(y_00 z_{10} + y_10 z_{00}) + w_0 w_1(y_01 z_{01} + y_{11} z_{11}).
\]

The key duality relation for MacWilliams identities is the Poisson summation formula, which says that “the sum of a function over a linear space is equal to the sum of the Fourier transform of the function over the dual space” \([5]\). For our case, this formula may be stated as follows:

**Poisson summation formula.** Let \(x\) and \(X\) be a transform pair defined on \(T = (\mathbb{Z}_p)^n\) and \(F = (\mathbb{Z}_p)^n\), respectively, and let \(C\) and \(C^\perp\) be orthogonal subgroups of \(T\) and \(F\), respectively. Then
\[
\sum_{t \in C} x(t) = \frac{1}{|C^\perp|} \sum_{f \in C^\perp} X(f).
\]

Now, applying this formula to the equation above for \(g_{\Lambda(w)}(y, z)\), we obtain
\[
g_{\Lambda(w)}(y, z) = \sum_{c_k} y(s_k) w(a_k) z(s_{k+1}) = \frac{1}{|C_k^\perp|} \sum_{c_k} Y(\hat{s}_k) W(\hat{a}_k) Z(-\hat{s}_{k+1}).
\]

Here we use the fact that the transform of a product is the product of their transforms, where \(Y = \mathcal{H}_y Y\), \(W = \mathcal{H}_w W\), and \(Z = \mathcal{H}_z Z\). Note that \(W\) is itself a product transform. Also, since the elements of \(H_z\) are \(H_z(s_k + 1, -s_k + 1) = \omega^{-s_k + 1} s_{k+1}\), the matrix \(H_z\) is the conjugate of the usual transform matrix over \(S_{k+1}\).

If we define the CWAM \(\Lambda(W)\) of \(C_k^\perp\) and its generating function \(g_{\Lambda(W)}(Y, Z)\) similarly to the analogous quantities for \(C_k\), then we obtain
\[
g_{\Lambda(W)}(Y, Z) = \sum_{c_k} Y(\hat{s}_k) W(\hat{a}_k) Z(-\hat{s}_{k+1}).
\]

Using inverse transforms, we thus obtain
\[
g_{\Lambda(W)}(Y, Z) = |C_k^\perp| g_{\Lambda(w)}(y, z) = |C_k^\perp| \mathbf{y}^T \hat{\Lambda}(W) \mathbf{Z}
\]

This MacWilliams identity shows how the generating function for the CWAM \(\Lambda(W)\) of \(C_k^\perp\) may be obtained from that for \(C_k\), or vice versa.

Alternatively, since
\[
g_{\Lambda(W)}(Y, Z) = \mathbf{y}^T \hat{\Lambda}(W) \mathbf{Z}
\]

we may simply write
\[
\hat{\Lambda}(W) = |C_k^\perp| \mathbf{y}^T \hat{\Lambda}(\mathcal{H}_w^{-1} W) \mathcal{H}_z^{-1} \mathbf{Z},
\]

a MacWilliams identity that shows how the CWAM of \(C_k^\perp\) may be obtained from the CWAM of \(C_k\).

**Example 1 (cont.)**. Given the CWAM \(\Lambda(w)\) of the constraint code \(C_k\) of Example 1, the CWAM \(\Lambda(W)\) of the orthogonal constraint code \(C_k^\perp\) is given by the matrix equation at the top of the next page, where we have substituted the dual indeterminates \(W_0\) and \(W_1\) for \(w_0 + w_1\) and \(w_0 - w_1\).

The Hamming weight adjacency matrix (HWAM) \(\Lambda_H\) of a constraint code \(C_k\) is obtained by substituting 1 for \(w(0)\) and \(w\) for each \(w(a)\), \(a \neq 0\). Thus each element \(\Lambda_H(s_k, s_{k+1})(w)\) becomes a polynomial of degree \(n\) in the single indeterminate \(w\). The dual indeterminates become \(W(0) = 1 + ([F] - 1)w\) and \(W(a) = 1 - w, a \neq 0\), which scale to 1 and \(W = (1 - w)/(1 + ([F] - 1)w)\), respectively. Substituting in the above MacWilliams-type identities for CWAMs, we obtain MacWilliams-type identities for HWAMs. This yields the main result of \([1]\), \([2]\). \(^2\)

**Example 2 (cont.)**. For a worked-out example of the HWAM \(\Lambda(W)\) of the orthogonal code \(C_k^\perp\) to the constraint code of Example 2, see \([2]\).

Although our development has focussed on conventional state realizations of linear time-invariant convolutional codes, it may be straightforwardly extended to obtain MacWilliams identities for any generalized state realization of any finite abelian group code defined on an arbitrary graph, because constraint code duality holds in the general case.

**V. DUALIZING THE SUM-PRODUCT UPDATE RULE**

Another duality result in \([3]\) is a general method for dualizing the sum-product update rule, which among other things yields the “tanh rule” of APP decoding. The approach of this paper yields a cleaner derivation of this result.

Again, for simplicity we restrict attention to conventional state realizations, in which each constraint code \(C_k\) specifies the state transitions in \(S_k \times A_k \times S_{k+1}\) that can possibly occur. Let the (right-going) message be any real- or complex-valued function \(m_w = \{m_k(s_k), s_k \in S_k\}\) of the state variable \(S_k\), and let \(f_k = \{f_k(a_k), a_k \in A_k\}\) be any real- or complex-valued weight function of the symbol variable \(A_k\). Then the sum-product update rule associated with constraint code \(C_k\) is
\[
m_{k+1}(s_{k+1}) = \sum_{c_k(s_k+1)} m_k(s_k) f_k(a_k),
\]

\(^2\)The MacWilliams identity of \([1]\), \([2]\) is stated in terms of the HWAM for a minimal realization of a linear time-invariant convolutional code \(C\) in controller canonical form, and the HWAM of some minimal encoder for the orthogonal code \(C^\perp\). Our results apply to the CWAM or HWAM of any state realization, and the CWAM or HWAM of its dual realization, because in our development, by constraint code duality, the basis of the dual state space representation is fixed as soon as the basis of the primal state space is fixed.
where \( \mathcal{C}(s_{k+1}) = \{(s_k, a_k) \in S_k \times A_k \mid (s_k, a_k, s_{k+1}) \in \mathcal{C}\} \). In other words, if we define a set of indeterminates
\[
\mathbf{x} = \{x(s_{k+1}), s_{k+1} \in S_{k+1}\},
\]
then \( m_{k+1}(s_{k+1}) \) is the coefficient of \( x(s_{k+1}) \) in the homogeneous degree-1 multivariate generating function \( g_{k+1}(\mathbf{x}) \) defined by
\[
g_{k+1}(\mathbf{x}) = m^T_{k+1} \mathbf{x} = \sum_{s_{k+1}} m_{k+1}(s_{k+1}) x(s_{k+1}).
\]
From the definition of \( \mathcal{C}(s_{k+1}) \), it follows that
\[
g_{k+1}(\mathbf{x}) = \sum_{\mathbf{c}_k} m_k(\mathbf{s}_k) f_k(\mathbf{a}_k) x(s_{k+1}).
\]
Using the Poisson summation formula, we obtain
\[
g_{k+1}(\mathbf{x}) = \sum_{\mathbf{c}_k} m_k(s_k) f_k(a_k) x(s_{k+1})
\]
\[
= \frac{1}{|\mathcal{C}_k|} \sum_{\mathbf{c}_k} M_k(\mathbf{s}_k) F_k(\mathbf{a}_k) X(-\mathbf{s}_{k+1})
\]
\[
= \frac{\hat{g}_{k+1}(\mathbf{X})}{|\mathcal{C}_k|},
\]
where we again use the fact that the transform of a product is the product of their transforms, and define transformed functions or indeterminates by corresponding capitalized functions or indeterminates. The left side of this equation is the generating function \( g_{k+1}(\mathbf{x}) \) of the message \( \{m_{k+1}\} \), and the right side is (up to scale) the generating function \( \hat{g}_{k+1}(\mathbf{X}) \) of the message \( M_{k+1} \) obtained by performing the sum-product update algorithm for \( \mathcal{C}_k \) upon the message \( M_k \) and the weight function \( F_k \). Moreover, the messages \( m_k \) and \( M_k \) form a transform pair.

Consequently, we have the following recipe for performing the sum-product update rule for \( \mathcal{C}_k \):

1) Transform the incoming messages \( m_k \) and \( f_k \) to \( M_k \) and \( F_k \);
2) Perform the sum-product update rule for \( \mathcal{C}_k \) to generate an output message \( M_{k+1} \);
3) Inverse transform \( M_{k+1} \) to obtain the message \( m_{k+1} \), up to the scale factor \( |\mathcal{C}_k| \).

Since the complexity of performing the sum-product update rule for \( \mathcal{C}_k \) is proportional to \( |\mathcal{C}_k| \), this dual computation may be attractive if \( |\mathcal{C}_k| < |\mathcal{C}_k| \).

**Example 3 ("tanh rule").** Let \( S_k, A_k \) and \( S_{k+1} \) be binary variables taking values in \( \mathbb{F}_2 \), and let \( \mathcal{C}_k \) be the \((3, 2)\) single-parity-check code consisting of the four codewords \((000, 011, 101, 110)\); then \( \mathcal{C}_k^\perp \) is the \((3, 1)\) repetition code consisting of the two codewords \((000, 111)\). Let the incoming message and weight function be \( m_k = (m_0, m_1) \) and \( f_k = (f_0, f_1) \); then the transformed message and weight function are \( M_k = (M_0 = m_0 + m_1, M_1 = m_0 - m_1) \) and \( F_k = (F_0 = f_0 + f_1, F_1 = f_0 - f_1) \). Using two multiplications, the sum-product update equation then produces the message \( M_{k+1} = (M_{k+1}(0) = (m_0 + m_1)(f_0 + f_1), M_{k+1}(1) = (m_0 - m_1)(f_0 - f_1)) \). Thus, up to scale, the message \( m_{k+1} \) is
\[
m_{k+1}(0) = M_{k+1}(0) + M_{k+1}(1) \propto m_0 f_0 + m_1 f_1;
\]
\[
m_{k+1}(1) = M_{k+1}(0) - M_{k+1}(1) \propto m_0 f_1 + m_1 f_0;
\]
which is evidently the message that would have been computed by a direct computation of the sum-product update rule for \( \mathcal{C}_k \), which requires four multiplications.

Again, although our development has focussed on a constraint code of a conventional linear state realization, it may be straightforwardly extended to obtain a dual sum-product update rule for an arbitrary constraint code over any finite abelian group.

**ACKNOWLEDGMENT**

For comments on an earlier version of this paper, I am grateful to H. Gluesing-Luerssen.

**REFERENCES**


