MacWilliams identities and matroid polynomials

Thomas Britz
Department of Mathematical Sciences,
University of Aarhus, Denmark
britz@imf.au.dk

Submitted: December 12, 2001; Accepted: April 22, 2002
MR Subject Classifications: 05B35, 94B05

Abstract

We present generalisations of several MacWilliams type identities, including those by Kløve and Shiromoto, and of the theorems of Greene and Barg that describe how the Tutte polynomial of the vector matroid of a linear code determines the rth support weight enumerators of the code. One of our main tools is a generalisation of a decomposition theorem due to Brylawski.

1 Introduction

Since the 1963 article [8] by F. J. MacWilliams, coding theorists have paid considerable attention to the support (Hamming) weight distribution of linear codes. In later years, this interest has increased due to results such as those by Wei [16] on rth generalised Hamming weights, Kløve [6] and Simonis [13] on rth support (Hamming) weight distributions (effective length distributions in Simonis' terminology), and Shiromoto [11] on λ-ply weight enumerators. Section 2 of this paper introduces notation and the various enumerators, by presenting the MacWilliams identities [8] as well as their generalisations by Kløve [6] and Shiromoto [11]. The two main results of this section, Theorems 3 and 7, generalise these results. Proofs of these theorems appear in the later sections.

In Section 3, we generalise theorems due to Greene [5] and Barg [1] that describe how the Tutte polynomial of the vector matroid of a linear code determines the rth support weight enumerators of the code. We obtain two theorems which turn out to be equivalent to each other and to the 'Critical Theorem' by Crapo and Rota [4]. The main tool is a generalisation of the characterisation of Tutte-Groethendieck polynomials due to Brylawski [3]. As applications of these theorems, we prove Theorems 3 and 7 of Section 2.

In Section 4, an alternative proof of Theorem 7 is presented. This proof relies on coding-theoretical arguments rather than on matroid theory.

We assume a basic knowledge of matroid theory; for an excellent introduction to the topic, see [10, 17, 18].

2 Support enumerators of a linear code

Let $\mathbb{F}_q$ be the finite field over q elements and let E denote a set of $n \geq 1$ distinct elements. For purposes of readability throughout this paper, we will denote by $\{f_e\}_A$ any multiset $\{f_e \mid e \in A\}$ whose elements f_e are labeled by the elements e of $A \subseteq E$. A *linear code* on E over $\mathbb{F}_q$ is a subspace C of the vector space $\mathbb{F}_q^E$. If $v = \{v_e\}_E$ is a word of $\mathbb{F}_q^E$, then let the set $S(v) = \{e \in E \mid v_e \neq 0\}$ denote the *support* of v. The (Hamming) weight function $w(v) = |S(v)|$ of a word $v \in \mathbb{F}_q^E$ is equal to the number of non-zero coordinates of v.

For each $i = 0, 1, ...$ let A_i be the number of codewords in C with weight i. The *support weight enumerator*

$$A(z) = \sum_{i=0}^{n} A_i z^i$$

is the generating function of the sequence $\{A_i\}_{i \geq 0}$. J. MacWilliams [8] proved the following fundamental identity between the support weight enumerators of a linear code and its dual.

Theorem 1 (MacWilliams identity) *[8] If $A(z)$ and $B(z)$ are the support weight enumerators of a linear k-dimensional code $C \subseteq \mathbb{F}_q^E$ and of its dual $C^\perp$, then*

$$B(z) = \frac{1}{q^k}\big(1 + (q-1)z\big)^n A\Big(\frac{1-z}{1+(q-1)z}\Big).$$

A generalisation of the support weight enumerator is the *support enumerator* $A\big(\{z_e\}_E\big)$ given by

$$A\big(\{z_e\}_E\big) = \sum_{E' \subseteq E} A_{E'} \prod_{e \in E'} z_e$$

where $A_{E'}$ denotes the number of codewords whose support is $E' \subseteq E$. By setting $z_e = z$ for all $e \in E$, we obtain the weight enumerator. The following theorem is the MacWilliams identity for support enumerators. A proof will be provided in Section 4, but for now remark that it follows from an equivalent result, Proposition 2 in [14], or from stronger results such as Theorem 7 below or Theorem 14 in [9, Ch. 5. §6]. Note that we obtain the MacWilliams identity by setting $z_e = z$ for all $e \in E$.

Theorem 2 *Let $C \subseteq \mathbb{F}_q^E$ be a k-dimensional linear code. If $A\big(\{z_e\}_E\big)$ and $B\big(\{z_e\}_E\big)$ are the respective support enumerators of C and the dual code $C^\perp$, then*

$$B\big(\{z_e\}_E\big) = \frac{1}{q^k}\Big(\prod_{e \in E}\big(1 + (q-1)z_e\big)\Big) A\bigg(\Big\{\frac{1-z_e}{1+(q-1)z_e}\Big\}_E\bigg).$$

A further generalisation of the support weight enumerator is the *m-tuple support enumerator*

$$A^{[m]}(\{z_e\}_E) = \sum_{E' \subseteq E} A_{E'}^{[m]} \prod_{e \in E'} z_e$$

where $A^{[m]}_{E'}$ denotes the number of ordered m-tuples of codewords in C whose union of supports is E'. The corresponding MacWilliams identity for m-tuple support enumerators is as follows.

Theorem 3 *If $A^{[m]}\big(\{z_e\}_E\big)$ and $B^{[m]}\big(\{z_e\}_E\big)$ are the m-tuple support enumerators of a linear k-dimensional code $C \subseteq \mathbb{F}_q^E$ and of its dual $C^\perp$ for some $m \geq 0$, then*

$$B^{[m]}\big(\{z_e\}_E\big) = \frac{1}{q^{km}}\Big(\prod_{e\in E}\big(1+(q^m-1)z_e\big)\Big)A^{[m]}\bigg(\Big\{\frac{1-z_e}{1+(q^m-1)z_e}\Big\}_E\bigg).$$

We will prove this result in Section 3.

Corollary 4 *For each subset $E' \subseteq E$ it holds that*

$$\sum_{E''\subseteq E'} B^{[m]}_{E''} = (q^m)^{|E'|-k} \sum_{E''\subseteq E\setminus E'} A^{[m]}_{E''}.$$

Proof. Set $z_e = 1$ for each element $e \in E'$ and $z_e = 0$ for each element $e \notin E'$. Now apply Theorem 3. $\square$

Define the numbers $A^{[m]}_i = \sum_{E':|E'|=i} A^{[m]}_{E'}$ for $i = 0,\ldots,n$.

Let the *m-tuple support weight enumerator* of C be

given by the sum

$$A^{[m]}(z) = \sum_{i=0}^{n} A^{[m]}_i z^i.$$

Note that $A^{[m]}(z)$ may be obtained by setting all z_e equal to z in $A^{[m]}\big(\{z_e\}_E\big)$. As an immediate corollary of Theorem 3, we obtain the following generalisation of the MacWilliams identity by K. Shiromoto.

Theorem 5 *[11]*

If $A^{[m]}(z)$ and $B^{[m]}(z)$ are the m-tuple support weight enumerators of a linear k-dimensional code $C \subseteq \mathbb{F}_q^E$ and of its dual $C^\perp$ for some $m \geq 0$, then

$$B^{[m]}(z) = \frac{1}{q^{km}}\big(1+(q^m-1)z\big)^n A^{[m]}\Big(\frac{1-z}{1+(q^m-1)z}\Big).$$

A different generalisation of the support weight enumerator of a linear code C involves the *rth support weight distribution* $\{A^{(r)}_i \mid i \geq 0\}$ of C where

$$A^{(r)}_i = \Big|\{C' \mid C' \text{ is an } r\text{-dimensional subspace of } C \text{ and } \Big|\bigcup_{v\in C'} S(v)\Big| = i\}\Big|.$$

The *rth support weight enumerator* is the corresponding generating function

$$A^{(r)}(z) = \sum_{i\geq 0} A^{(r)}_i z^i.$$

The next theorem is the MacWilliams identity for the rth support weight enumerator, due to T. Kløve [6]. Shiromoto [12] proved the equivalence between this result and Theorem 5, and J. Simonis [13] has proved a result which is equivalent to both these results.

Let $[a]_b$ denote the product $\prod_{i=0}^{b-1}(q^a - q^i)$.

Theorem 6 *[6] If $A^{(r)}(z)$ and $B^{(r)}(z)$ are the rth support weight enumerators of a linear k-dimensional code $C \subseteq \mathbb{F}_q^E$ and of its dual $C^\perp$ for all r such that $0 \leq r \leq k$, then the following identity holds for all $m \geq 0$:*

$$\sum_{r=0}^{k}[m]_r B^{(r)}(z) = \frac{1}{q^{km}}\bigl(1+(q^m-1)z\bigr)^n \sum_{r=0}^{k}[m]_r A^{(r)}\Bigl(\frac{1-z}{1+(q^m-1)z}\Bigr).$$

To generalise the rth support weight enumerators, define the *rth support distribution* $\{A_{E'}^{(r)} \mid E' \subseteq E\}$ of C where

$$A_{E'}^{(r)} = \Bigl|\{C' \mid C' \text{ is an } r\text{-dimensional subspace of } C \text{ and } \bigcup_{v \in C'} S(v) = E'\}\Bigr|.$$

The *rth support enumerator* is the sum

$$A^{(r)}\bigl(\{z_e\}_E\bigr) = \sum_{E' \subseteq E} A_{E'}^{(r)} \prod_{e \in E'} z_e .$$

Note that the support enumerator $A\bigl(\{z_e\}_E\bigr)$ is given by the sum

$$A^{(0)}\bigl(\{z_e\}_E\bigr) + (q-1)A^{(1)}\bigl(\{z_e\}_E\bigr) = 1 + (q-1)A^{(1)}\bigl(\{z_e\}_E\bigr).$$

The following theorem generalises both Theorem 2 and Theorem 6. The former may be obtained by setting $m = 1$ and the latter may be obtained by setting $z_e = z$ for all $e \in E$.

Theorem 7 *If $A^{(r)}\bigl(\{z_e\}_E\bigr)$ and $B^{(r)}\bigl(\{z_e\}_E\bigr)$ are the rth support enumerators of a linear k-dimensional code $C \subseteq \mathbb{F}_q^E$ and of its dual $C^\perp$ for all r such that $0 \leq r \leq k$, then the following identity holds for all $m \geq 0$:*

$$\sum_{r=0}^{k}[m]_r B^{(r)}\bigl(\{z_e\}_E\bigr) =$$

$$\frac{1}{q^{km}}\Bigl(\prod_{e \in E}\bigl(1+(q^m-1)z_e\bigr)\Bigr) \sum_{r=0}^{k}[m]_r A^{(r)}\Bigl(\Bigl\{\frac{1-z_e}{1+(q^m-1)z_e}\Bigr\}_E\Bigr).$$

Theorem 3 and Theorem 7 are equivalent. This follows from the following oft-proved theorem (originally due to E. Landberg [7]).

Theorem 8 *Let C be an r-dimensional subspace of $\mathbb{F}_q^E$. The number of ordered m-tuples of vectors $(v_1, \ldots, v_m) \in C^m$ which span C is independent of the actual subspace C. Indeed, this number equals $[m]_r$.*

Let $C \subseteq \mathbb{F}_q^E$ be a linear code and let $E' \subseteq E$. The family of ordered m-tuples of vectors in C, whose union of supports is E', may be partitioned into $m+1$ blocks, according to the dimension r of the span of the m vectors. Furthermore, Theorem 8 stipulates that there are precisely $[m]_r$ m-tuples $(v_1, \ldots, v_m)$ of codewords of a fixed code C' of dimension r such that $v_1, \ldots, v_m$ span C'. Together, these two observations imply

Proposition 9 *For each subset $E' \subseteq E$ it holds that $A_{E'}^{[m]} = \sum_{r=0}^{k} [m]_r A_{E'}^{(r)}$. Hence, $A^{[m]}(\{z_e\}_E) = \sum_{r=0}^{k} [m]_r A^{(r)}(\{z_e\}_E)$.*

The equivalence of Theorems 3 and 7 now follows. By setting $m = 1$, the equivalence of Theorems 5 and 6 is therefore also re-proved.

3 The vector matroid of a linear code

Let G be a generator matrix for a linear code $C \subseteq \mathbb{F}_q^E$. The vector matroid $\mathcal{M}_C = \mathcal{M}[G]$ is the matroid over E whose independent sets are the linearly independent columns of G. The code C and the matroid $\mathcal{M}_C$ are quite closely related. For instance, it is easy to show that $\mathcal{M}_C$ is independent of the chosen generator matrix G and that the dual matroid corresponds to the dual code:

$\mathcal{M}_C^{\perp} = \mathcal{M}_{C^\perp}$. However, the code C contains more information than the matroid $\mathcal{M}_C$. Indeed, a matroid $\mathcal{M}$ may, over the same field, be the vector matroid of several linear codes which are not monomially equivalent. The results in this section demonstrate how some of the matroid's properties determine many properties of the codes, in particular the various enumerators mentioned in the previous section.

The *characteristic polynomial* $P(\mathcal{M}; \lambda)$ of a matroid $\mathcal{M}$ on the set E may defined by the sum

$$P(\mathcal{M}; \lambda) = \sum_{A \subseteq E} (-1)^{|A|} \lambda^{r(E)-r(A)}$$

where r is the rank function of $\mathcal{M}$. The *rank generating function* $R(\mathcal{M}; x, y)$ of $\mathcal{M}$ is defined by the sum

$$R(\mathcal{M}; x, y) = \sum_{A \subseteq E} x^{r(E)-r(A)} y^{|A|-r(A)}.$$

Note that $P(\mathcal{M}; \lambda) = (-1)^{r(E)} R(\mathcal{M}; -\lambda, -1)$. By an easy application of the identity $r(E) + r^*(A) = |A| + r(E \setminus A)$ one may show the duality identity

$$R(\mathcal{M}^*; x, y) = R(\mathcal{M}; y, x).$$

The following celebrated theorem by H. Crapo and G.-C. Rota describes the set of supports $S(C)$ of a linear code. We have restated the theorem slightly, in a manner similar to that of Greene [5].

Theorem 10 *[4] The m-tuple support enumerator of a linear code $C \subseteq \mathbb{F}_q^E$ is given by*

$$A^{[m]}\big(\{z_e\}_E\big) = \sum_{A \subseteq E} P(\mathcal{M}_C/(E \setminus A); q^m) \prod_{e \in A} z_e.$$

In particular, the following corollary is obtained by setting $m = 1$. This result has been derived independently in [2].

Corollary 11 *The support enumerator of a linear code $C \subseteq \mathbb{F}_q^E$ is given by*

$$A\big(\{z_e\}_E\big) = \sum_{A \subseteq E} P(\mathcal{M}_C/(E \setminus A); q) \prod_{e \in A} z_e.$$

The main importance of Theorem 10 and Corollary 11 is the fact that the matroid $\mathcal{M}_C$ determines the structure of the set of supports of C. In turn, this implies that the codes representing $\mathcal{M}$ over $\mathbb{F}_q$ share a common set of supports of codewords. Indeed, Theorems 16 and 17 below state that the m-tuple support enumerator and rth support enumerator of any linear code which represents $\mathcal{M}$ over $\mathbb{F}_q$ may be obtained by evaluating certain polynomials associated with $\mathcal{M}$.

C. Greene expresses the support weight enumerator $A(z)$ of a code C as an evaluation of the rank generating function $R(\mathcal{M}_C; x, y)$ of the matroid $\mathcal{M}_C$, as follows.

Theorem 12 *[5] Let $C \subseteq \mathbb{F}_q^E$ be a k-dimensional linear code. Then the support weight enumerator $A(z)$ of C is given by*

$$A(z) = (1-z)^k z^{n-k} R\Big(\mathcal{M}_C; \frac{qz}{1-z}, \frac{1-z}{z}\Big).$$

The application of the duality identity $R(\mathcal{M}_{C^\perp}; x, y) = R(\mathcal{M}_C; y, x)$ allows Greene to re-prove Theorem 1. This procedure is repeated by A. Barg [1] who expresses rth support weight enumerators $A^{(r)}(z)$ by the rank generating function and uses this to re-prove Theorem 6.

Theorem 13 *[1] Let $C \subseteq \mathbb{F}_q^E$ be a k-dimensional linear code. If $A^{(r)}(z)$ is the rth support weight enumerator of C where $0 \le r \le n$, then it holds for all $m \ge 0$ that*

$$\sum_{r=0}^{k} [m]_r A^{(r)}(z) = (1-z)^k z^{n-k} R\Big(\mathcal{M}_C; \frac{q^m z}{1-z}, \frac{1-z}{z}\Big).$$

We will also follow this method, in order to express the rth support enumerator in terms of matroid properties. For this purpose, we will generalise the rank generating function. Let R be a domain and let $R(X)$ be the ring of rational forms over R. Associate to each element $e \in E$ an indeterminate variable z_e over R. If g and h are functions on $R(X)$, then define a *generalised rank generating function* $R_{g,h}(\mathcal{M}; x, y, \{z_e\}_E)$ by the sum

$$\sum_{A \subseteq E} x^{r(E)-r(A)} y^{|A|-r(A)} \Big(\prod_{e \in A} g(z_e)\Big) \prod_{f \notin A} h(z_f).$$

Note that we obtain the usual rank generating function by letting g and h be the identity function, and setting $z_e = 1$ for all $e \in E$. L. Traldi [15] has independently investigated a closely related polynomial (a generalised Tutte polynomial for doubly weighted matroids).

Proposition 14 $R_{g,h}(\mathcal{M}^*; x, y, \{z_e\}_E) = R_{h,g}(\mathcal{M}; y, x, \{z_e\}_E)$.

Proof. We apply the identity $r(E) + r^*(A) = |A| + r(E \setminus A)$:

$$\begin{aligned}
& R_{g,h}(\mathcal{M}^*; x, y, \{z_e\}_E) \\
&= \sum_{A \subseteq E} x^{r^*(E)-r^*(A)} y^{|A|-r^*(A)} \Big(\prod_{e \in A} g(z_e)\Big) \prod_{f \notin A} h(z_f) \\
&= \sum_{A \subseteq E} x^{|E \setminus A|-r(E \setminus A)} y^{r(E)-r(E \setminus A)} \Big(\prod_{e \in A} g(z_e)\Big) \prod_{f \notin A} h(z_f) \\
&= \sum_{A \subseteq E} y^{r(E)-r(A)} x^{|A|-r(A)} \Big(\prod_{e \in A} h(z_e)\Big) \prod_{f \notin A} g(z_f) \\
&= R_{h,g}(\mathcal{M}; y, x, \{z_e\}_E).
\end{aligned}$$

□

The following theorem generalises the characterisation [3] of Tutte-Groethendieck polynomials of a matroid due to T. Brylawski. A result which is closely related to the first part of Theorem 15 appears in [15].

Theorem 15 *If g and h are functions in $R(X)$, then the generalised rank generating function $R_{g,h}$ is the unique function $f(\mathcal{M}, x, y, \{z_e\}_E)$ on a given minor-closed class $\mathcal{A}$ of matroids $\mathcal{M}$ and variables $x \cup y \cup \{z_e\}_E$ which satisfies the following conditions:*

1. *$f(U_{0,1}, x, y, z_e) = yg(z_e) + h(z_e)$ and*
   $f(U_{1,1}, x, y, z_e) = g(z_e) + xh(z_e)$;
2. *If e is a loop or a coloop of $\mathcal{M}$, then*
   $f(\mathcal{M}, x, y, \{z_{e'}\}_E) = f(\mathcal{M}(e), x, y, z_e) f(\mathcal{M} \setminus e, x, y, \{z_{e'}\}_{E-e})$
3. *If e is a neither a loop nor a coloop of $\mathcal{M}$, then*
   $f(\mathcal{M}, x, y, \{z_{e'}\}_E) =$
   $h(z_e) f(\mathcal{M} \backslash e, x, y, \{z_{e'}\}_{E-e}) + g(z_e) f(\mathcal{M}/e, x, y, \{z_{e'}\}_{E-e})$.

Furthermore, if $g(x)$ and $h(x)$ are functions in $R(X)$ such that $g(x), h(x) \neq 0'$, and $f(\mathcal{M}, x, y, \{z_e\}_E)$ is a function satisfying conditions 2 and 3, then for all $e \in E$ it holds that $f(\mathcal{M}, x, y, \{z_{e'}\}_E)$ is equal to

$$R_{g,h}(\mathcal{M}; \frac{f(U_{1,1}, x, y, z_e) - g(z_e)}{h(z_e)}, \frac{f(U_{0,1}, x, y, z_e) - h(z_e)}{g(z_e)}, \{z_{e'}\}_E).$$

Proof. The proof is straightforward.

$$\begin{aligned} R_{g,h}(U_{0,1}, x, y, z_e) &= x^{r(e)-r(\emptyset)} y^{|\emptyset|-r(\emptyset)} h(z_e) + x^{r(e)-r(e)} y^{|e|-r(e)} g(z_e) \\ &= h(z_e) + yg(z_e) \quad \text{and} \\ R_{g,h}(U_{1,1}, x, y, z_e) &= x^{r(e)-r(\emptyset)} y^{|\emptyset|-r(\emptyset)} h(z_e) + x^{r(e)-r(e)} y^{|e|-r(e)} g(z_e) \\ &= g(z_e) + xh(z_e) \end{aligned}$$

so $R_{g,h}$ satisfies condition 1. To show that $R_{g,h}$ also satisfies conditions 2 and 3, observe that

$$\begin{aligned} R_{g,h}(\mathcal{M}, x, y, \{z_{e'}\}_E) &= \sum_{A \subseteq E} x^{r(E)-r(A)} y^{|A|-r(A)} \Big(\prod_{e' \in A} g(z_{e'})\Big) \prod_{f \notin A} h(z_f) \\ &= \sum_{A \subseteq E-e} \Big(\prod_{e' \in A} g(z_{e'})\Big)\Big(\prod_{f \notin A \cup e} h(z_f)\Big) F(A)\,, \end{aligned}$$

where $F(A) = h(z_e) x^{r(\mathcal{M})-r(A)} y^{|A|-r(A)} + g(z_e) x^{r(\mathcal{M})-r(A\cup e)} y^{|A\cup e|-r(A\cup e)}$. In order to evaluate $F(A)$ further, we must distinguish between three cases: e is either a loop, a coloop, or neither of these. Suppose that e is a loop. Then $r(\mathcal{M}) = r(\mathcal{M}\backslash e)$ and $r_{\mathcal{M}}(A) = r_{\mathcal{M}}(A \cup e) = r_{\mathcal{M}\backslash e}(A)$ for all subsets $A \subseteq E - e$ so

$$\begin{aligned} F(A) &= yh(z_e) x^{r(\mathcal{M}\backslash e)-r_{\mathcal{M}\backslash e}(A)} y^{|A|-r_{\mathcal{M}\backslash e}(A)} + \\ &\quad\ yg(z_e) x^{r(\mathcal{M}\backslash e)-r_{\mathcal{M}\backslash e}(A)} y^{|A|-r_{\mathcal{M}\backslash e}(A)} \\ &= (h(z_e) + yg(z_e))(x^{r(\mathcal{M}\backslash e)-r_{\mathcal{M}\backslash e}(A)} y^{|A|-r_{\mathcal{M}\backslash e}(A)})\,. \end{aligned}$$

Since $h(z_e)+yg(z_e)=R_{g,h}(U_{0,1},x,y,z_e)=R_{g,h}(\mathcal{M}(e),x,y,z_e)$, we see that

$$R_{g,h}(\mathcal{M},x,y,\{z_{e'}\}_E)=R_{g,h}(\mathcal{M}(e),x,y,z_e)R_{g,h}(\mathcal{M}\setminus e,x,y,\{z_{e'}\}_{E-e}).$$

The two remaining cases are similar, and $R_{g,h}$ satisfies conditions 1 and 2. The conditions 1, 2, and 3 recursively define $R_{g,h}$, which proves the uniqueness of the function $R_{g,h}$.

Suppose that $g(x)$ and $h(x)$ are functions on $R(X)$ such that $g(x),h(x)\neq 0$, and that $f(\mathcal{M},x,y,\{z_{e'}\}_E)$ is a function which satisfies conditions 2 and 3 for all $\mathcal{M}\in\mathcal{A}$. Let F_0 and F_1 denote the terms

$$\frac{f(U_{0,1},x,y,z_e)-h(z_e)}{g(z_e)} \quad \text{and} \quad \frac{f(U_{1,1},x,y,z_e)-g(z_e)}{h(z_e)}\ ,$$

respectively.

First note that $f(\mathcal{M},x,y,\{z_{e'}\}_E)$ is equal to $R_{g,h}(\mathcal{M};F_1,F_0,\{z_{e'}\}_E)$ for $\mathcal{M}=U_{0,1},U_{1,1}$. Now let $\mathcal{M}\ \in\mathcal{A}$ be a given matroid on E, and let e be an element of E. Assume that $f(\mathcal{M}',x,y,\{z_{e'}\}_E)$ is equal to $R_{g,h}(\mathcal{M}';F_1,F_0,\{z_{e'}\}_E)$ for the minors $\mathcal{M}'=\mathcal{M}\backslash e'',\mathcal{M}/e''$ of $\mathcal{M}$ where $e''\neq e$ is some element of E. Suppose that e'' is a loop of $\mathcal{M}$. By assumption and by two applications of condition 2, it follows that

$$\begin{aligned}
& R_{g,h}(\mathcal{M};F_1,F_0,\{z_{e'}\}_E)\\
= \ & R_{g,h}(\mathcal{M}(e'');F_1,F_0,z_{e''})R_{g,h}(\mathcal{M}\backslash e'';F_1,F_0,\{z_{e'}\}_{E-e''})\\
= \ & f(\mathcal{M}(e'');F_1,F_0,z_{e''})f(\mathcal{M}\backslash e'';F_1,F_0,\{z_{e'}\}_{E-e''})\\
= \ & f(\mathcal{M};F_1,F_0,\{z_{e'}\}_E)\,.
\end{aligned}$$

The cases in which e'' is either a coloop or an element which is neither a loop nor a coloop are similar. The theorem now follows by induction on $|E|$. □

Let $C\subseteq\mathbb{F}_q^E$ be a linear code. A *puncturing* $C\setminus E'$ of C by the coordinate set $E'\subseteq E$ is the code obtained by deleting from each vector $v\in C$ the entries corresponding to E'. A *shortening* C/E' of C by the coordinate set $E'\subseteq E$ is the code obtained by first removing from C all vectors $v\in C$ whose support contain elements of E', and then shortening by E'. Note that $C\setminus E'$ and C/E' are subspaces of $\mathbb{F}_q^{E\setminus E'}$ and that

$$\mathcal{M}_{C\setminus E'}=\mathcal{M}_C\setminus E' \qquad \text{and} \qquad \mathcal{M}_{C/E'}=\mathcal{M}_C/E'.$$

Any code C' obtained from a linear code C by a sequence of shortenings and puncturings is a *minor* of C. The corresponding matroid $\mathcal{M}_{C'}$ is a minor of $\mathcal{M}_C$.

The following theorem generalises Theorem 12 for the m-tuple support enumerator.

Theorem 16 *Let $C\subseteq\mathbb{F}_q^E$ be a k-dimensional linear code. Then*

$$A^{[m]}\big(\{z_e\}_E\big)=R_{1-x,x}(\mathcal{M}_C;q^m,1,\{z_e\}_E).$$

In particular, $A\big(\{z_e\}_E\big)=R_{1-x,x}(\mathcal{M}_C;q,1,\{z_e\}_E)$.

Proof. Let $\mathcal{M}_{C'}$ be the support matroid of each minor C' of C. Consider the m-tuple support enumerators $A^{[m]}_{C'}\big(\{z_e\}_{E'}\big)$ as a function $A^{[m]}$ on the family of all minors C' of C. In order to apply Theorem 15, we must show that $A^{[m]}$ may be regarded as a function on the family of all minors $\mathcal{M}'$ of $\mathcal{M}_C$. First, note that

$$A^{[m]}_{U_{0,1}}(z_e) = 1 \quad \text{and} \quad A^{[m]}_{U_{1,1}}(z_e) = 1 + (q^m - 1)z_e \tag{3.1}$$

are well-defined since these are the only corresponding support enumerators of the minors C' of C which have only one coordinate.

Suppose that $C' \subseteq \mathbb{F}_q^{E'}$ is a minor of C and let E'' and e' be a subset and a member, respectively, of the set of coordinates E' of C'. If e' is a loop of $\mathcal{M}_{C'}$, then e' is not contained in any of the supports of C' so

$$A^{[m]}_{C'}\big(\{z_e\}_{E'}\big) = A^{[m]}_{C'\setminus e'}\big(\{z_e\}_{E'-e'}\big) = A^{[m]}_{U_{0,1}}(z_{e'})A^{[m]}_{C'\setminus e'}\big(\{z_e\}_{E'-e'}\big). \tag{3.2}$$

If e' is a coloop of $\mathcal{M}_{C'}$, then e' is the support of some codeword $v \in C'$. If e' is not contained in E'', then the number $A^{[m]}_{E''}$ is the same for C' as for C'/e. However, if e' is contained in E'', then consider an m-tuple $(v_1, \ldots, v_m)$ of codewords of $C' \setminus e'$ such that $\cup_{i=1}^m S(v_i) = E'' - e'$. By appending to each codeword v_i one of the q elements of $\mathbb{F}_q$ as the (e')th coordinate, q^m new m-tuples are formed, of which only one does not have a union of supports which contains e'. Conversely, any m-tuple $(v_1, \ldots, v_m)$ of codewords of C' such that $\cup_{i=1}^m S(v_i) = E''$ can be obtained in this manner. Note that $C'/e' = C' \setminus e'$ since e' is the support of some codeword. Hence,

$$\begin{aligned} A^{[m]}_{C'}\big(\{z_e\}_{E'}\big) &= A^{[m]}_{C'/e'}\big(\{z_e\}_{E'-e'}\big) + (q^m - 1)z_{e'}A^{[m]}_{C'\setminus e'}\big(\{z_e\}_{E'-e'}\big) \\ &= \big(1 + (q^m - 1)z_{e'}\big)A^{[m]}_{C'\setminus e'}\big(\{z_e\}_{E'-e'}\big) \\ &= A^{[m]}_{U_{1,1}}(z_{e'})A^{[m]}_{C'\setminus e'}\big(\{z_e\}_{E'-e'}\big)\,. \end{aligned} \tag{3.3}$$

Now, suppose that e' is neither a loop nor a coloop. If e' is not contained in E'', then the numbers of codewords whose support equals E' are identical for C' and for C'/e'. On the other hand, if e' is contained in E'', then the number of m-tuples of codewords of $C' \setminus e'$ whose union of supports equals $E'' - e'$ is equal to the number of m-tuples of codewords of C' whose union of supports equals either E'' or $E' - e'$.

From this, it follows that

$$A^{[m]}_{C'}\big(\{z_e\}_{E'}\big) = (1 - z_{e'})A^{[m]}_{C'/e'}\big(\{z_e\}_{E'-e'}\big) + z_{e'}A^{[m]}_{C'\setminus e'}\big(\{z_e\}_{E'-e'}\big). \tag{3.4}$$

By induction, the identities (3.1), (3.2), (3.3), and (3.4) show that

$A^{[m]}_{C'}\big(\{z_e\}_{E'}\big)$ depends only on the matroid $\mathcal{M}_{C'}$. Hence, condition 2 in Theorem 15 is satisfied by the identities (3.2) and (3.3), and identity (3.4) satisfies condition 3 in Theorem 15 for the functions $g : x \mapsto 1 - x$ and $h : x \mapsto x$ on $R(X)$. Theorem 15 concludes the proof. □

As an immediate application of Proposition 14 and Theorem 16, we may prove Theorem 3 as follows.

$$\begin{aligned}
&B^{[m]}\big(\{z_e\}_E\big)\\
&= R_{1-x,x}(\mathcal{M}_{C^\perp}; q^m, 1, \{z_e\}_E)\\
&= R_{x,1-x}(\mathcal{M}_C; 1, q^m, \{z_e\}_E) = \sum_{A\subseteq E} (q^m)^{|A|-r(A)}\Big(\prod_{e\in A} z_e\Big)\prod_{f\notin A}(1-z_e)\\
&= \frac{1}{q^{km}} \sum_{A\subseteq E} (q^m)^{r(E)-r(A)}\Big(\prod_{e\in A} q^m z_e\Big)\prod_{f\notin A}(1-z_e)\\
&= \frac{1}{q^{km}}\Big(\prod_{e\in E}\big(1+(q^m-1)z_e\big)\Big) R_{1-x,x}\Big(\mathcal{M}_C; q^m, 1, \Big\{\frac{1-z_e}{1+(q^m-1)z_e}\Big\}_E\Big)\\
&= \frac{1}{q^{km}}\Big(\prod_{e\in E}\big(1+(q^m-1)z_e\big)\Big) A^{[m]}\Big(\Big\{\frac{1-z_e}{1+(q^m-1)z_e}\Big\}_E\Big). \qquad \square
\end{aligned}$$

The support generalisation of Theorem 13 is described in the following theorem.

Theorem 17 *Let C be a k-dimensional subspace of $\mathbb{F}_q^E$. Then for each $m \geq 0$ it holds that*

$$\sum_{r=0}^{k} [m]_r A^{(r)}\big(\{z_e\}_E\big) = R_{1-x,x}(\mathcal{M}_C; q^m, 1, \{z_e\}_E).$$

Proof. Theorem 17 follows immediately from Proposition 9 and Theorem 16. □

Furthermore, Theorem 22 follows from Theorem 16, Theorem 17, and Lemma 21. In turn, Theorem 22 implies that Theorem 12 and Theorem 13 are equivalent.

Theorem 7 follows as an immediate corollary from Proposition 14 and Theorem 17.

To conclude, we prove that the two latter theorems are also equivalent to Theorem 10:

$$\begin{aligned}
&R_{1-x,x}(\mathcal{M}_C, q^m, 1, \{z_e\}_E)\\
=\;& \sum_{A\subseteq E} (q^m)^{r(E)-r(A)}\Big(\prod_{e\in A}(1-z_e)\Big)\prod_{f\notin A} z_f\\
=\;& \sum_{A\subseteq E} (q^m)^{r(E)-r(A)}\Big(\sum_{B\subseteq A}(-1)^{|B|}\prod_{e\in B} z_e\Big)\prod_{f\notin A} z_f\\
=\;& \sum_{A\subseteq E}\sum_{B\subseteq A}(-1)^{|B|}(q^m)^{r(E)-r(A)} \prod_{e\in B\cup(E\setminus A)} z_e\\
=\;& \sum_{A\subseteq E}\Big(\sum_{B\subseteq A}(-1)^{|B|}(q^m)^{(r(E)-r(E\setminus A))-(r(B\cup(E\setminus A))-r(E\setminus A))}\Big)\prod_{e\in A} z_e .
\end{aligned}$$

Hence,

$$R_{1-x,x}(\mathcal{M}_C, q^m, 1, \{z_e\}_E) = \sum_{A\subseteq E} P(\mathcal{M}_C/(E\setminus A); q^m)\prod_{e\in A} z_e . \qquad \square$$

4 An alternative proof of Theorem 7

This section contains an alternative proof of Theorem 7 which does not depend on matroid theory. The proof relies on Theorem 2 which, as mentioned in Section 2, follows easily from a number of results. To make this section self-contained, however, a direct proof of Theorem 2 is provided.

It is perhaps of interest to note that these proofs differ only very slightly, in an obvious way, from one of the two original proofs [8] of the MacWilliams identity, and from Kløve's proof [6] of Theorem 6.

Proof of Theorem 2. Let χ be a non-trivial character of $\mathbb{F}_q$ and define $g(u)$ for $u \in \mathbb{F}_q^E$ by the sum

$$\sum_{v\in\mathbb{F}_q^E} \chi\big(\langle u,v\rangle\big) \prod_{e\in S(v)} z_e\,.$$

We will now express the sum $\sum_{u\in C} g(u)$ in two different ways and then identify the support enumerators $A\big(\{z_e\}_E\big)$ and $B\big(\{z_e\}_E\big)$. The first expression:

$$\begin{aligned}\sum_{u\in C} g(u) &= \sum_{u\in C}\sum_{v\in\mathbb{F}_q^E} \chi\big(\langle u,v\rangle\big) \prod_{e\in S(v)} z_e \\ &= \sum_{v\in\mathbb{F}_q^E}\Big(\prod_{e\in S(v)} z_e\Big)\sum_{u\in C}\chi\big(\langle u,v\rangle\big)\,.\end{aligned}$$

If $v \in C^\perp$, then the inner sum equals $|C|$. On the other hand, if $v \notin C^\perp$,

then $\langle u,v\rangle$ assumes all values of $\mathbb{F}_q$ an equal number of times, whence the inner sum is 0. Therefore,

$$\sum_{u\in C} g(u) = |C| \sum_{v\in C^\perp}\prod_{e\in S(v)} z_e = |C|\cdot B\big(\{z_e\}_E\big)\,. \tag{4.1}$$

For the second expression, consider $g(u)$:

$$\begin{aligned}g(u) &= \sum_{v\in\mathbb{F}_q^E} \chi\big(\langle u,v\rangle\big) \prod_{e\in S(v)} z_e \\ &= \sum_{v\in\mathbb{F}_q^E}\prod_{e\in S(v)} \chi(u_e v_e) z_e \\ &= \prod_{e\in E}\Big(1 + \sum_{v_e\in\mathbb{F}_q-0} \chi(u_e v_e) z_e\Big)\,.\end{aligned}$$

If $u_e = 0$, then the inner sum equals $(q-1)z_e$. Otherwise, the inner sum equals $z_e \cdot \sum\limits_{a\in\mathbb{F}_q-0} \chi(a) = -z_e$. Hence,

$$
\begin{aligned}
\sum_{u\in C} g(u) &= \sum_{u\in C}\Big(\prod_{e\notin S(u)}\big(1+(q-1)z_e\big)\Big)\prod_{e\in S(u)}(1-z_e)\\
&= \Big(\prod_{e\in E}\big(1+(q-1)z_e\big)\Big)\sum_{u\in C}\prod_{e\in S(u)}\frac{1-z_e}{1+(q-1)z_e}\\
&= \Big(\prod_{e\in E}\big(1+(q-1)z_e\big)\Big)A\Big(\Big\{\frac{1-z_e}{1+(q-1)z_e}\Big\}_E\Big).
\end{aligned}
$$

By noting that $|C| = q^k$, we may combine the above expression of $\sum_{u\in C} g(u)$ with the expression (4.1) to obtain the identity stated in the theorem. $\square$

In order to prove Theorem 7, a few initial lemmas are required. Let G be a generator matrix for C of rank k and for all l let $\mathcal{F}_l$ denote the family of l-dimensional subspaces of $\mathbb{F}_q^k$. Any r-dimensional subspace D of C may be represented by a generator matrix of the form MG where M is a $r \times k$ matrix of rank r which is uniquely determined up to row operations. Conversely, any such matrix MG generates a r-dimensional subspace D of C. Therefore, if U_D denotes the subspace of $\mathbb{F}_q^k$ which is dual to the row space of M, then

Lemma 18 *For any $r \leq k$, the map $D \mapsto U_D$ defines a bijection between the r-dimensional subspaces of C and $\mathcal{F}_{k-r}$.*

Let G_e and $(MG)_e$ denote the column of G and MG,
respectively, which corresponds to the element e. Define for each set $U \subseteq \mathbb{F}_q^k$ a corresponding set $s(U) = \{e \mid G_e \in U\}$.

Lemma 19 *If D is a subspace of C, then $\displaystyle\bigcup_{v\in D} S(v) = E\backslash s(U_D)$.*

Proof. $\displaystyle E\backslash\bigcup_{v\in D} S(v) = \{e \mid (MG)_e = 0\} = \{e \mid M(G_e) = 0\} = s(U_D)$. $\square$

Let $C^{(m)} = \{vG \mid v \in \mathbb{F}_{q^m}^k\}$ be the code generated by G over $\mathbb{F}_{q^m}$.

Lemma 20 *The support enumerator for $C^{(m)}$ is*

$$
A_m\big(\{z_e\}_E\big) = \sum_{r=0}^{k}[m]_{k-r}\sum_{U\in\mathcal{F}_{k-r}}\prod_{e\notin s(U)} z_e.
$$

Proof. Let $\hat{U} = \{y \in \mathbb{F}_{q^m}^k \mid \forall x \in \mathbb{F}_q^k : \langle x, y\rangle = 0 \text{ if and only if } x \in U\}$.

If $y \in \hat{U}$, then $S(yG) = \{e \mid y(G_e) \neq 0\} = E \backslash s(U)$. Note also that if $U \in \mathcal{F}_r$, then $|\hat{U}| = [m]_{k-r}$. Since $\{\hat{U} \mid U \text{ is a subspace of } \mathbb{F}_q^k\}$ partitions $\mathbb{F}_{q^m}^k$, it follows that

$$\begin{aligned}
A_m\big(\{z_e\}_E\big) &= \sum_{v \in C^{(m)}} \prod_{e \in S(v)} z_e = \sum_{x \in \mathbb{F}_{q^m}^k} \prod_{e \in S(xG)} z_e \\
&= \sum_{r=0}^{k} \sum_{U \in \mathcal{F}_r} \sum_{y \in \hat{U}} \prod_{e \in s(yG)} z_e = \sum_{r=0}^{k} \sum_{U \in \mathcal{F}_r} \sum_{y \in \hat{U}} \prod_{e \notin s(U)} z_e \\
&= \sum_{r=0}^{k} [m]_{k-r} \sum_{U \in \mathcal{F}_r} \prod_{e \notin s(U)} z_e. \qquad \square
\end{aligned}$$

From Lemmas 18, 19, and 20, we obtain the following lemma.

Lemma 21 *The support enumerator for $C^{(m)}$ is*

$$A_m\big(\{z_e\}_E\big) = \sum_{r=0}^{k} [m]_r A^{(r)}\big(\{z_e\}_E\big).$$

Note that Proposition 9 may be extended by Lemma 21 as follows.

Theorem 22 $A^{[m]}\big(\{z_e\}_E\big) = A_m\big(\{z_e\}_E\big) = \sum_{r=0}^{k} [m]_r A^{(r)}\big(\{z_e\}_E\big).$

Theorem 22 also follows from Theorem 16, Theorem 17, and Lemma 21.

Also note that Theorem 17 may be re-proved without the (indirect) use of Theorem 8. Since the matroids $\mathcal{M}_C$ and $\mathcal{M}_{C^{(m)}}$ are identical, and $C^{(m)}$ is a code over $\mathbb{F}_{q^m}$, it follows from Theorem 16 and Lemma 21 that

$$\begin{aligned}
\sum_{r=0}^{k} [m]_r A^{(r)}\big(\{z_e\}_E\big) &= A_m\big(\{z_e\}_E\big) \\
&= R_{1-x,x}(\mathcal{M}_{C^{(m)}}; q^m, 1, \{z_e\}_E) \\
&= R_{1-x,x}(\mathcal{M}_C; q^m, 1, \{z_e\}_E)\,.
\end{aligned}$$

Proof of Theorem 7. We apply Theorem 2 and Lemma 21:

$$\begin{aligned}
\sum_{r=0}^{k} [m]_r B^{(r)}\big(\{z_e\}_E\big) &= B_m\big(\{z_e\}_E\big) \\
&= \frac{1}{q^{km}} \Big(\prod_{e \in E} \big(1 + (q^m - 1) z_e\big) \Big) A_m\bigg(\Big\{ \frac{1 - z_e}{1 + (q^m - 1) z_e} \Big\}_E \bigg) \\
&= \frac{1}{q^{km}} \Big(\prod_{e \in E} \big(1 + (q^m - 1) z_e\big) \Big) \sum_{r=0}^{k} [m]_r A^{(r)} \bigg(\Big\{ \frac{1 - z_e}{1 + (q^m - 1) z_e} \Big\}_E \bigg). \qquad \square
\end{aligned}$$

Acknowledgements

I thank Peter Cameron for his valuable suggestions and advice.

I also thank Alexander Barg, Alan Sokal, and the anonymous referee for their helpful comments.

References

[1] A. Barg, The matroid of supports of a linear code, *Appl. Algebra Engrg. Comm. Comput.* **8** (1997), 165–172.

[2] R. A. Brualdi, V. S. Pless, and J. S. Beissinger,

On the MacWilliams identities for linear codes, *Linear Algebra Appl.* **107** (1988), 191–189.

[3] T. Brylawski, A decomposition for combinatorial geometries, *Trans. Am. Math. Soc.* **171** (1972), 235–282.

[4] H. Crapo and G.-C. Rota, *On the Foundations of Combinatorial Theory: Combinatorial Geometries (Preliminary edition)*, The M.I.T. Press, Cambridge, Mass.-London, 1970.

[5] C. Greene, Weight enumeration and the geometry of linear codes, *Studies in Appl. Math.* **55** (1976), 119–128.

[6] T. Kløve, Support weight distribution of linear codes, *Discrete Math.* **106/107** (1992), 311–316.

[7] E. Landberg, Über eine Anzahlbestimmung und eine damit zusammenhängende Reihe, *J. Reine Angew. Math.* **111** (1893), 78–88.

[8] F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell System Tech. J.* **42** (1963), 79–94.

[9] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, Amsterdam, 1978.

[10] J. Oxley, *Matroid Theory*, The Clarendon Press, New York, 1992.

[11] K. Shiromoto, A new MacWilliams type identity for linear codes, *Hokkaido Math. Journal* **25** (1996), 651–656.

[12] K. Shiromoto, The weight enumerator of linear codes over $GF(q^m)$ having generator matrix over $GF(q)$, *Des. Codes and Cryptogr.* **16** (1999), 87–92.

[13] J. Simonis, The effective length of subcodes, *Appl. Algebra Eng. Com. Comp.* **5** (1994), 371–377.

[14] J. Simonis, MacWilliams identities and coordinate partitions, *Linear Algebra Appl.* **216** (1995), 81–91.

[15] L. Traldi, Series and parallel reductions for the Tutte polynomial, *Discrete Math.* **220** (2000), 291–297.

[16] V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory* **37** (1991), 1412–1418.

[17] D. J. A. Welsh, *Matroid Theory*, Academic Press, London-New York, 1976.

[18] N. White, *Theory of Matroids*, Encyclopedia of Mathematics and its Applications, 26. Cambridge University Press, Cambridge-New York, 1986.