TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 356, Number 10, Pages 3841–3868
S 0002-9947(03)03367-1
Article electronically published on July 24, 2003

LATROIDS AND THEIR REPRESENTATION BY CODES OVER MODULES

DIRK VERTIGAN

Dedicated in memory of William T. Tutte, 1917-2002

Abstract. It has been known for some time that there is a connection between linear codes over fields and matroids represented over fields. In fact a generator matrix for a linear code over a field is also a representation of a matroid over that field. There are intimately related operations of deletion, contraction, minors and duality on both the code and the matroid. The weight enumerator of the code is an evaluation of the Tutte polynomial of the matroid, and a standard identity relating the Tutte polynomials of dual matroids gives rise to a MacWilliams identity relating the weight enumerators of dual codes. More recently, codes over rings and modules have been considered, and MacWilliams type identities have been found in certain cases.

In this paper we consider codes over rings and modules with code duality based on a Morita duality of categories of modules. To these we associate latroids, defined here. We generalize notions of deletion, contraction, minors and duality, on both codes and latroids, and examine all natural relations among these.

We define generating functions associated with codes and latroids, and prove identities relating them, generalizing above-mentioned generating functions and identities.

1. Introduction

It has been known for some time (since the 1970's) that there is a connection between linear codes over fields and matroids represented over fields. The connection was explored in [8]; see also [6, 7, 19]. In fact a generator matrix for a linear code over a field is also a representation of a matroid over that field. There are intimately-related operations of deletion, contraction, minors and duality on both the code and the matroid. The weight enumerator of the code is an evaluation of the Tutte polynomial of the matroid, and a standard identity relating the Tutte polynomials of dual matroids gives rise to a MacWilliams identity [12, 13] relating the weight enumerators of dual codes.

More recently, codes over rings and modules have been considered, and MacWilliams type identities have been found in certain cases; see for example [9, 10,

Received by the editors July 15, 2002 and, in revised form, April 3, 2003.
2000 *Mathematics Subject Classification.* Primary 05B35; Secondary 94B05, 16D90.
Key words and phrases. Linear code, ring, Artinian ring, finite ring, module, matroid, polymatroid, latroid, minor, minor class, duality, Morita duality, weight enumerator, Tutte polynomial, generating function, MacWilliams identity.
The author's research was partially supported by the National Security Agency, grant number MDA904-01-0014.

11, 14, 22]. In particular [22] suggests using *Morita duality* (see [1] or below) and finds a MacWilliams identity in the case of finite *Frobenius* rings and a certain type of duality.

However, at least at the time this research was started, the literature generalizing results about linear codes over fields to results about linear codes over rings, seemed to contain no mention of matroid-like objects. From the author's point of view, the interesting questions were related to natural generalizations of the topic of matroid representation over fields. (Somewhat in this vein, Semple and Whittle have represented matroids over *partial* fields [16, 20, 21] which we will relate to our results in later work.) Others [4] had independently asked the author about the possibility of matroid-like objects arising from linear codes over rings.

In this paper we define generalizations of matroids, which we call *latroids*. We essentially generalize some results of [8] to the case of linear codes over modules with appropriate restrictions that ensure that everything is well defined.

In Section 2 we summarize the relevant results of Greene [8], as well as some classical results for matroids and linear codes over fields.

Sections 3-7 develop a generalization of matroid representation theory. In Section 3 we briefly discuss lattices. In Section 4 we discuss what we mean by codes, and their minors. In Section 5 we define latroids and their minors and duals, and we relate them. We discuss the connection between codes and latroids, and we relate their minors. In Section 6 we discuss code duality in terms of Morita duality and its connection to latroid duality, and the interaction of duality with minors. In Section 7 we discuss and illustrate how to interpret minors and duality of codes in the context of categories of modules.

In Sections 8, 9, and 10 we define certain generating functions for latroids generalizing the Tutte polynomial, and for codes we define various weight enumerators and show some identities relating these.

A paper such as this, bringing together several topics, is confronted with some diverse and sometimes conflicting notation, and some decisions must be made. For a matroid ρ its dual will be denoted $\rho^\perp$, since the superscript * is needed for another duality. The forward slash '/', is used for both contraction in matroids and 'modding out' in groups, rings and modules.

For a set E, let 2^E denote its power set and let $|E|$ denote its cardinality. For a set K, let K^E denote the set of all functions from E to K, or equivalently, all vectors with entries in K, indexed by E. If K is some algebraic object, then K^E inherits the appropriate algebraic structure in the natural way.

For a family or vector $\mathbf{L} = (L_e : e \in E)$ and $A \subseteq E$, the product $\prod_{e\in A} L_e$ is denoted $\mathbf{L}^A$ for any well-defined type of product.

For a positive integer k we denote $[k] = \{1, \dots, k\}$.

For a vector $\mathbf{x} = (x_i : i \in [k])$ and vector $a = (a_i : i \in [k])$, we define $\mathbf{x}^a$ by $\mathbf{x}^a = \prod_{i\in[k]} x_i^{a_i}$ whenever such an expression is well defined.

All rings considered in this paper have a multiplicative identity.

2. Linear codes, matroids and the Tutte polynomial

In this section we summarize the relevant results of Greene [8], which build on earlier work [6, 7] (see also Chapter 15, especially Section 15.7, of [19] for an exposition). We also summarize some other standard results for matroids and linear codes over fields [19]. These are the results that will be generalized.

Let K be a field and E be a finite set. A *code over K on the ground set E* is a subspace C of K^E.

The *dual code* $C^\perp$ is defined by

$$C^\perp = \{y \in K^E : x \cdot y = 0 \text{ for all } x \in C\} \tag{1}$$

and $C^\perp$ is also a code over K on the ground set E.

A *matroid* (ρ, E) *on ground set* E is a function $\rho : 2^E \to \mathbb{Z}$ satisfying the following three axioms:

(i) ρ is *normalized*, that is, $\rho(\emptyset) = 0$,
(ii) ρ is *bounded increasing*, that is, $0 \leq \rho(B) - \rho(A) \leq |B| - |A|$ for all $A \subseteq B \subseteq E$,
(iii) ρ is *submodular*, that is, $\rho(A)+\rho(B) \geq \rho(A\cap B)+\rho(A\cup B)$ for all $A, B \subseteq E$.

Actually ρ is the *rank function of* a matroid, but in this paper we will simply say that ρ *is* the matroid.

For $A \subseteq E$ we denote the *complement* $\overline{A} = E - A$. The *dual* of ρ is the matroid $\rho^\perp : 2^E \to \mathbb{Z}$ on the same ground set E where, giving two equivalent definitions, for all $A \subseteq E$,

$$\begin{array}{rcl} \rho^\perp(A) & = & |A| - (\rho(E) - \rho(\overline{A})), \\ \rho^\perp(\overline{A}) & = & |\overline{A}| - (\rho(E) - \rho(A)). \end{array} \tag{2}$$

Observe that

$$\begin{array}{rcl} \rho^{\perp\perp} & = & \rho, \\ C^{\perp\perp} & = & C. \end{array} \tag{3}$$

Note that the standard matroid notation for the dual of ρ is ρ^* rather than $\rho^\perp$. However we will use the superscript '*' in relation to Morita duality between categories of modules (see Section 6), and C^* and $C^\perp$ will denote two different modules.

Let X be a matrix with columns indexed by the set E. The matroid ρ_X represented by X has ground set E and has $\rho_X(A)$ equalling the rank of the set of columns indexed by A for every $A \subseteq E$. Let $\mathrm{rsp}(X)$ denote the rowspace of X. The dual spaces $\mathrm{rsp}(X)$ and $(\mathrm{rsp}(X))^\perp$ are called a *cocycle space* and a *cycle space*, respectively, of ρ_X, for reasons clarified below. In fact, the dual pair of codes $\mathrm{rsp}(X)$ and $(\mathrm{rsp}(X))^\perp$ uniquely determine the dual pair of matroids ρ_X and $(\rho_X)^\perp$.

Unfortunately there are two equally valid and natural conventions for designating *which* of the two matroids goes with *which* of the two codes. Both conventions are used in the literature. Instead of simply choosing one of the two conventions, we will first provide notation and terminology to distinguish the two, and *then* we will choose one.

To this end, we will require that for any subspace C of K^E we will explicitly designate that it is to be regarded either as a *cycle space* or as a *cocycle space*. Essentially, if $\mathcal{L}(K^E)$ is the lattice of all subspaces of K^E, we are making *two* copies of $\mathcal{L}(K^E)$ and simply calling all the elements of one copy 'cycle spaces' and all the elements of the other copy 'cocycle spaces'.

So, a code C determines a matroid in one of two ways, depending on whether C is regarded as a cycle space or a cocycle space. In this section we will adopt the cycle space convention, and the generalizations in later sections will be consistent with that choice.

The *circuits* and *cocircuits* of a matroid ρ on ground set E are defined in [19]. The *circuits* of ρ are the minimal subsets $A \subseteq E$ such that $\rho(A) < |A|$. The *cocircuits* of ρ are the *circuits* of $\rho^\perp$, or equivalently, the minimal subsets $A \subseteq E$ such that $\rho(\overline{A}) < \rho(E)$.

A *generator matrix* and a *parity check matrix* of a code C on ground set E are defined in [13]. A *generator matrix* of C is any matrix whose row space is C. A *parity check matrix* of C is any matrix whose row space is $C^\perp$.

For a vector $c \in K^E$ its *support* is $\mathrm{supp}(c) = \{e \in E : c(e) \neq 0\}$. For $A \subseteq E$, we denote the restriction of $c : E \to K$ to A, by $c|_A$.

2.1. **Definition.** Cycle space convention: If the subspace C of K^E is designated to be a cycle space, then the matroid *with cycle space* C, is denoted by ρ_C^{cyc}, or ρ_C for short, and is given by any of the following equivalent definitions:

(a) for every $A \subseteq E$ it holds that $\rho_C(A) = |A| - \dim\{c|_A : c \in C, c|_{\overline{A}} = 0\}$,
(b) the *circuits* of ρ_C are precisely the minimal non-empty supports of vectors in C,
(c) ρ_C is represented by any *parity check matrix* X of the code C, that is, any X with $C = (\mathrm{rsp}(X))^\perp$.

2.2. **Definition.** Cocycle space convention: If the subspace C of K^E is designated to be a cocycle space, then the matroid *with cocycle space* C, is denoted by ρ_C^{cocyc}, or ρ_C for short, and is given by any of the following equivalent definitions:

(a) for every $A \subseteq E$ it holds that $\rho_C(A) = \dim\{c|_A : c \in C\}$,
(b) the *cocircuits* of ρ_C are precisely the minimal non-empty supports of vectors in C,
(c) ρ_C is represented by any *generator matrix* X of the code C, that is, any X with $C = \mathrm{rsp}(X)$.

We may *delete* and/or *contract* elements from the ground set E of a code or matroid to obtain *minors*. Let ρ be a matroid on the ground set E.

For $F \subseteq E$, the *restriction* of ρ to F or the *deletion* of $\overline{F}$ from ρ is the matroid on the ground set F denoted by $\rho|F : 2^F \to \mathbb{Z}$ or $\rho\backslash\overline{F} : 2^F \to \mathbb{Z}$ and defined by

$$(\rho|F)(A) = (\rho\backslash\overline{F})(A) = \rho(A) \text{ for all } A \subseteq F. \tag{4}$$

The *contraction* of ρ to F or the *contraction* of $\overline{F}$ from ρ is the matroid on the ground set F denoted by $\rho \cdot F : 2^F \to \mathbb{Z}$ or $\rho/\overline{F} : 2^F \to \mathbb{Z}$ and defined by

$$(\rho \cdot F)(A) = (\rho/\overline{F})(A) = \rho(A \cup \overline{F}) - \rho(\overline{F}) \text{ for all } A \subseteq F. \tag{5}$$

Let C be a code on the ground set E, designated to be a cycle space.

The *restriction* of C to F or the *deletion* of $\overline{F}$ from C is the code on the ground set F denoted by $C|F$ or $C\backslash\overline{F}$ and defined by

$$C|F = C\backslash\overline{F} = \{c|_F \subseteq K^F : c \in C,\ c|_{\overline{F}} = 0\}. \tag{6}$$

Coding theorists call this operation *shortening*.

The *contraction* of C to F or the *contraction* of $\overline{F}$ from C is the code on the ground set F denoted by $C \cdot F$ or $C/\overline{F}$ and defined by

$$C \cdot F = C/\overline{F} = \{c|_F \subseteq K^F :\ c \in C\}. \tag{7}$$

Coding theorists call this operation *puncturing*. We will not use the terms shortening and puncturing here.

If code C is designated to be a cocycle space, then the roles of deletion and contraction are reversed. That will not concern us here, but it further emphasizes the need to make the choice of convention clear and explicit.

For any disjoint $A, B \subseteq E$ we say $(\rho\backslash A)/B$ is a *minor* of ρ and $(C\backslash A)/B$ is a *minor* of C, each on the ground set $E-(A\cup B)$. The sets A and B are allowed to be empty.

For disjoint sets $A_1, B_1, A_2, B_2 \subseteq E$,

$$\begin{array}{rcl} (((\rho\backslash A_1)/B_1)\backslash A_2)/B_2 & = & (\rho\backslash(A_1\cup A_2))/(B_1\cup B_2), \\ (((C\backslash A_1)/B_1)\backslash A_2)/B_2 & = & (C\backslash(A_1\cup A_2))/(B_1\cup B_2). \end{array} \tag{8}$$

In other words, deletions and contractions can be done in any order without changing the minor obtained, so we may omit the parentheses, and any sequence of deletions and contractions gives a minor.

Also for disjoint $A, B \in E$, duality swaps the roles of deletion and contraction, that is,

$$\begin{array}{rcl} (\rho\backslash A/B)^\perp & = & \rho^\perp/A\backslash B, \\ (C\backslash A/B)^\perp & = & C^\perp/A\backslash B. \end{array} \tag{9}$$

Observe that $\dim(C\cap(K^A\times\{0\}^{\overline{A}})) = \rho(C|A) = \rho(C\backslash\overline{A})$, so ρ_C tells us precisely the dimension of every intersection of C with the 'coordinate subspace' corresponding to each $A \subseteq E$.

The mapping $C \mapsto \rho_C$ respects the operations of deletion, contraction and duality in the following sense: for disjoint $A, B \in E$,

$$\begin{array}{rcl} \rho_{(C\backslash A/B)} & = & (\rho_C)\backslash A/B, \\ \rho_{(C^\perp)} & = & (\rho_C)^\perp. \end{array} \tag{10}$$

Note that this would also be true for the cocycle space convention, but again, with the roles of deletion and contraction the opposite for cocycle spaces to what they are for cycle spaces.

There are generating functions associated with both C and ρ_C; these were related in [8]. Recall that for a vector $c \in K^E$ its *support* is $\operatorname{supp}(c) = \{e \in E : c(e) \neq 0\}$. Its *Hamming weight* is $\operatorname{wt}(c) = |\operatorname{supp}(c)|$.

The *weight enumerator* W_C of a code C over a finite field $K \cong GF(q)$ is a polynomial in the variable z and is defined to be

$$W_C(z) = W(C; z) = \sum_{c\in C} z^{\operatorname{wt}(c)}. \tag{11}$$

The Tutte polynomial was originally defined for graphs [18] and then generalized to matroids [3, 5]. The Tutte polynomial T_ρ of a matroid ρ is a polynomial in variables x and y, defined to be

$$T_\rho(x, y) = T(\rho; x, y) = \sum_{A\subseteq E} (x-1)^{\rho(E)-\rho(A)}(y-1)^{|A|-\rho(A)}. \tag{12}$$

Some readers may wonder why $x-1$ and $y-1$ were used on the right-hand side instead of just x and y. It turns out that the coefficient of each monomial $x^i y^j$ is non-negative and combinatorially understood in terms of counting certain objects, and it is indeed natural. However, in later sections we will use a generalization of the Tutte-Whitney rank generating function denoted and defined by

$$R(\rho; x, y) = T(\rho; x+1, y+1) = \sum_{A\subseteq E} x^{\rho(E)-\rho(A)} y^{|A|-\rho(A)}. \tag{13}$$

An element $e \in E$ is a *loop* of a matroid ρ if and only if $\rho(e) = 0$. An element $e \in E$ is a *coloop* of ρ if and only if it is a loop of $\rho^\perp$. The *deletion-contraction formula* defines the Tutte polynomial recursively as follows. Here $\emptyset$ denotes the empty matroid.

$$\begin{array}{rcl} T(\emptyset; x, y) & = & 1, \\ \text{if } e \text{ is a loop,} \quad T(\rho; x, y) & = & yT(\rho\backslash e; x, y), \\ \text{if } e \text{ is a coloop,} \quad T(\rho; x, y) & = & xT(\rho/e; x, y), \\ \text{otherwise} \quad T(\rho; x, y) & = & T(\rho\backslash e; x, y) + T(\rho/e; x, y). \end{array} \tag{14}$$

The following important identities follow directly from (2), (12), (13) (or from (9), (13), (14)):

$$\begin{array}{rcl} T(\rho^\perp; x, y) & = & T(\rho; y, x), \\ R(\rho^\perp; x, y) & = & R(\rho; y, x). \end{array} \tag{15}$$

Greene [8] related the weight enumerator and the Tutte polynomial as follows:

$$W(C; z) = z^{|E|-\dim(C)}(1-z)^{\dim(C)} T\left(\rho_C; \frac{1}{z}, \frac{1+(q-1)z}{1-z}\right). \tag{16}$$

By the change of variables in (13), this is equivalent to

$$W(C; z) = z^{|E|-\dim(C)}(1-z)^{\dim(C)} R\left(\rho_C; \frac{1-z}{z}, \frac{qz}{1-z}\right). \tag{17}$$

The proof [8] is by induction, using the deletion-contraction formula (14), but it can just as well be proved using other techniques, as we do later with the generalization.

In [8], equations (15) and (16) were combined to give a new proof of a MacWilliams identity, namely, for any code C over a finite field $K \cong GF(q)$ on a finite ground set E,

$$W(C^\perp; z) = \frac{(1+(q-1)z)^{|E|}}{q^{\dim(C)}} W\left(C; \frac{1-z}{1+(q-1)z}\right). \tag{18}$$

Various more general weight enumerators have been defined and more general MacWilliams identities relate the weight enumerator of a code to that of its dual. These identities and enumerators may be made more general by involving more variables, for example the *exact weight enumerator* and associated MacWilliams identity; see Chapter 5 of [13]. More special identities are then obtained by making certain substitutions for the variables.

In another direction they may be generalized to a larger class of codes, for example to the class of codes over finite Frobenius rings; see [22].

We primarily generalize the results of this section in the second sense extending them to a much larger class of codes and making a corresponding extension of the class of matroids and their Tutte polynomials. However, while (11), (12), and (15) will generalize, there are some limitations on the generalization of (16) or (17), and hence of (18).

We also generalize in the first sense, by adding more variables.

3. Lattices

In a *complete lattice* $L = (L, \wedge, \vee, \leq)$, every subset has a join and meet. In particular, there is a unique minimal element called the *zero*, denoted $0 = 0_L$, and a unique maximal element called the *one*, denoted $1 = 1_L$. Every finite lattice

is complete. Throughout this paper every lattice is assumed to be complete and 'lattice' will mean 'complete lattice'.

For a lattice L, we say that a sublattice $\tilde{L}$ is a 0-1 *sublattice* of L provided that $0_L, 1_L \in \tilde{L}$, so that $0_{\tilde{L}} = 0_L$ and $1_{\tilde{L}} = 1_L$.

For a lattice L, and $l, m \in L$ with $l \leq m$, the *interval* $[l, m]_L$, or $[l, m]$ for short, is defined by $[l, m] = \{x \in L : l \leq x \leq m\}$. So l and m are respectively the zero and one of $[l, m]$.

For a module M, let $\mathcal{L}(M)$ denote the lattice of all submodules of M.

A lattice L has the *finite chain condition* (FCC) if every chain in L is finite. We say the module M has FCC if and only if the lattice $\mathcal{L}(M)$ has FCC.

4. Codes

In this section, we define what we mean by codes. The mathematical context is really categories of modules [1]. We first generalize the idea of dimension of a vector space in a fairly standard way, and for this we will need to impose certain 'finiteness' conditions.

Let rings R and S be respectively left- and right-Artinian rings, that is, ${}_RR$ and S_S have FCC. Let ${}_R\mathfrak{F}$ and $\mathfrak{F}_S$ be the categories of finitely generated left R-modules, right S-modules, respectively, so every module in each category has FCC. Any discussion of one of these transfers immediately to the other, so we will work mainly with $\mathfrak{F}_S$.

Suppose the simple right S-modules are $S_1, S_2, \ldots, S_k$ listed up to isomorphism without repetition. This list is finite since S is right Artinian. We arbitrarily order these k simple modules as $S_1, S_2, \ldots, S_k$, and then fix this ordering. A *composition series* of $M \in \mathfrak{F}_S$ is a chain of submodules $M = M_n > \ldots > M_2 > M_1 > M_0 = 0$ such that M_j/M_{j-1} is simple or equivalently M_{j-1} is a maximal proper submodule of M_j for every $j \in [n]$. Such a maximal chain exists since S is right Artinian and M is finitely generated; see [1] Theorem 15.21.

Define the *length* of $M \in \mathfrak{F}_S$, denoted by $\|M\|_S = \|M\| \in \mathbb{Z}^k$, to be the vector $\mathbf{r} = (r_1, r_2, \ldots, r_k)$, where the simple module S_i appears exactly r_i times up to isomorphism in the list $(M_j/M_{j-1} : j \in [n])$ for each $i \in [k]$. By the Jordan-Hölder Theorem [1], all composition series are *equivalent*, which by definition means that $\mathbf{r}$ is independent of the choice of composition series. So $\|M\| = \mathbf{r}$ is well defined. Note that the *scalar length* $n = \sum_{i=1}^k r_i$ is typically called the length of the composition series, but we define and use the more general vector $\mathbf{r} = (r_1, r_2, \ldots, r_k)$ as the length.

4.1. **Proposition.** (a) *For $M' \leq M \in \mathfrak{F}_S$ it holds that $\|M/M'\| = \|M\| - \|M'\|$.*

(b) *For any finite set E and any $M_e \in \mathfrak{F}_S$, $e \in E$, it holds that $\left\|\prod_{e\in E} M_e\right\| = \left\|\bigoplus_{e\in E} M_e\right\| = \sum_{e\in E} \|M_e\|$.*

(c) *For $M_1, M_2 \leq M \in \mathfrak{F}_S$ it holds that $\|M_1\|+\|M_2\| = \|M_1 \cap M_2\|+\|M_1+M_2\|$.*

These statements also hold for left modules, bimodules and Abelian groups, having FCC.

Proof. It is routine to generalize the proofs of the corresponding standard results for the scalar length $n = \sum_{i=1}^k r_i$ from [1] Section 11 to the vector length $\|M\| = \mathbf{r} = (r_1, r_2, \ldots, r_k)$. □

Recall that an *exact sequence* is a sequence of two or more homomorphisms,

$$\cdots \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow \cdots \tag{19}$$

where $\mathrm{Im}(f) = \mathrm{Ker}(g)$ for each successive pair.

Let E be a finite set, and for each $e \in E$, let $M_e \in \mathfrak{F}_S$. Denote the family $\mathbf{M} = (M_e : e \in E)$, and for $A \subseteq E$, denote $\mathbf{M}^A = \prod_{e\in A} M_e$. Since direct sums and direct products of *finitely* many modules are naturally isomorphic, we will use such sums and products interchangeably.

A *code C on the ground set E in $\mathbf{M}^E$* is a submodule of $\mathbf{M}^E$. Implicit in the description of any code are not only E and $\mathbf{M}^E$, but also the whole short exact sequence

$$0 \longrightarrow C \longrightarrow \mathbf{M}^E \longrightarrow \mathbf{M}^E/C \longrightarrow 0. \tag{20}$$

We call $\mathbf{M}^E/C$ the *cocode on the ground set E from $\mathbf{M}^E$, corresponding to C*. We also say that $\mathbf{M}^E$ is the *ambient module* of the code C and the *source module* of the cocode $\mathbf{M}^E/C$.

Now the product module $\mathbf{M}^E$ is, after all, just a module. There is essentially no change in generality if, for a module M, we alternatively define a *code in M* and a *cocode from M* to be the second and fourth terms in the short exact sequence

$$0 \longrightarrow C \longrightarrow M \longrightarrow M/C \longrightarrow 0. \tag{21}$$

Codes described the former way are said to be in *grounded format*, referring to the ground set E, while codes described the latter way are said to be in *generic format*. Results in one case can be translated to results in the other, without excessive difficulty.

The apparent loss of structure due to using M instead of $\mathbf{M}^E$ is more than made up for by introducing a lattice as follows. A generic code $C \leq M$ *with lattice L* is a pair (C, L), where the lattice L is a 0-1 sublattice of $\mathcal{L}(M)$.

We will now define code minors. There will also be discussion and illustration of how to interpret minors in the context of categories of modules in Section 7.

For a code C with lattice L, we obtain *minors* as follows. Given $l, m \in L$, with $l \leq m$, the *minor* of C obtained by *contracting* l and *deleting to* (or *restricting to*) m is the code denoted $(C|m)/l$ or $C{:}[l, m]$, *with* lattice denoted $L{:}[l, m]$ and ambient module m/l. It might seem natural to write $C\backslash m'/l$ for an appropriate m', instead of $(C|m)/l$, but there is not a clear and fully satisfactory choice of what m' should be.

$$\begin{aligned} C{:}[l, m] &= (m \cap C)/(l \cap C) \leq m/l, \\ L{:}[l, m] &= \{x/l : l \leq x \leq m\}. \end{aligned} \tag{22}$$

Observe that, as lattices, $[l, m] \cong L{:}[l, m]$ via $x \in [l, m] \mapsto x/l \in L{:}[l, m]$, and $L{:}[l, m]$ is a 0-1 sublattice of $\mathcal{L}(m/l)$.

For example, with a code $C \leq K^E$ as in Section 2, we obtain minors by taking the lattice L of all 'coordinate subspaces' $K^A \times 0^{\bar{A}}$ for all $A \subseteq E$.

We now provide similar definitions for codes in grounded format. A grounded code $C \subseteq \mathbf{M}^E$ *with lattice* $\mathbf{L}^E$ is a pair $(C, \mathbf{L}^E)$, where $\mathbf{L}^E$ is a product $\prod_{e\in E} L_e$ of lattices and each L_e is a 0-1 sublattice of $\mathcal{L}(M_e)$ for each $e \in E$. The elements of $\prod_{e\in E} L_e$ can be taken to be $|E|$-tuples $(x_e \in L_e : e \in E)$, with operations $\wedge$ and $\vee$ and relation $\leq$ defined componentwise in the natural way. We also treat $\mathbf{L}^E$ as a

0-1 sublattice of $\mathcal{L}(\mathbf{M})^E = \prod_{e\in E}\mathcal{L}(M_e)$, which in turn is a sublattice of $\mathcal{L}(\mathbf{M}^E)$, by identifying each $|E|$-tuple $(x_e : e \in E)$ with the module $\bigoplus_{e\in E} x_e = \prod_{e\in E} x_e$.

Note that we require $\mathbf{L}^E$ to be a product in this way, which is more restrictive than merely requiring $\mathbf{L}^E$ to be a 0-1 sublattice of $\mathcal{L}(\mathbf{M})^E$ (or the even bigger $\mathcal{L}(\mathbf{M}^E)$).

Minors are defined essentially as for the generic code case, but we spell out some details because of the presence of the ground set E. Suppose $\mathbf{l} = (l_e : e \in E)$ and $\mathbf{m} = (m_e : e \in E)$ are elements of $\mathbf{L}^E$ with $\mathbf{l} \le \mathbf{m}$ so that $l_e \le m_e$ for all $e \in E$. Essentially as before, *contracting* $\mathbf{l}$ and *restricting to* $\mathbf{m}$ gives the *minor* $C{:}[\mathbf{l},\mathbf{m}] = (\mathbf{m} \cap C)/(\mathbf{l} \cap C) \le \mathbf{m}/\mathbf{l}$. We also say that we contract l_e and restrict to m_e for each ground set element $e \in E$.

Now we identify $\mathbf{m}/\mathbf{l}$ with the product module $\prod_{e\in E}(m_e/l_e)$ so $C{:}[\mathbf{l},\mathbf{m}]$ is a code *in* the ambient module $\prod_{e\in E}(m_e/l_e)$. Moreover $C{:}[\mathbf{l},\mathbf{m}]$ is *with* the lattice $L{:}[\mathbf{l},\mathbf{m}]$ which we identify with the product $\prod_{e\in E}(L_e{:}[l_e, m_e])$.

So far, the minor has the same ground set E. But it could be for some $e \in E$ that $l_e = m_e$, so that the module m_e/l_e and lattice $L_e{:}[l_e, m_e]$ are both trivial (each having one element).

We say an element $e \in E$ is *trivial* in the code $C \le \mathbf{M}^E$ if $M_e = 0$. So e is trivial in the minor $C{:}[\mathbf{l},\mathbf{m}]$ if and only if $l_e = m_e$.

In a minor we shall allow the *removal* of any subset of trivial elements, that is, if $A \subseteq E$ is such that $l_e = m_e$ for all $e \in A$, then the minor $C{:}[\mathbf{l},\mathbf{m}] - A$ is a code which has ground set $E - A$, and is *in* the product $\prod_{e\in E-A}(m_e/l_e)$ and *with* lattice $\prod_{e\in E-A}(L_e{:}[l_e, m_e])$. Also, as a module, $C{:}[\mathbf{l},\mathbf{m}] - A$ is isomorphic to $C{:}[\mathbf{l},\mathbf{m}]$ via the natural isomorphism between $\prod_{e\in E-A}(m_e/l_e)$ and $\prod_{e\in E}(m_e/l_e)$.

Returning to the example, with a code $C \le K^E$ as in Section 2, and treating it as a grounded code, we have $L_e = \mathcal{L}(K) = \{0, K\}$, for each $e \in E$. So $\mathbf{L}^E$ is isomorphic to the Boolean lattice 2^E in the natural way. To delete $e \in E$, we choose $l_e = m_e = 0$ and we remove e. To contract $e \in E$, we choose $l_e = m_e = K$ and we remove e. Otherwise, we choose $l_e = 0$ and $m_e = K$. For such codes, the definition of minor is slightly more general in that we can produce a trivial element $e \in E$ (by choosing $l_e = m_e$) but we don't *have to* remove it, but this is of no great consequence.

5. Latroids

In this section we generalize matroids and polymatroids [19] to latroids.

5.1. **Definition.** An *ordered Abelian group* is a triple $(\mathbb{A}, +, \le)$, where $(\mathbb{A}, +)$ is an Abelian group, $(\mathbb{A}, \le)$ is a partial order and for all $a, b \in \mathbb{A}$,

(i) $a \le b \iff 0 \le b - a$ and
(ii) if $a \ge 0$ and $b \ge 0$, then $a + b \ge 0$.

5.2. **Example.** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ with the usual $+, \le$ are ordered Abelian groups.

5.3. **Example.** If $\mathbb{A}_1, \dots, \mathbb{A}_k$ are ordered Abelian groups, then define the ordered Abelian group $\prod_{i=1}^k \mathbb{A}_i$, where $(a_1, \dots, a_k) + (b_1, \dots, b_k) = (a_1 + b_1, \dots, a_k + b_k)$ and

$$(a_1, \dots, a_k) \le (b_1, \dots, b_k) \iff a_i \le b_i \text{ for all } i \in [k]. \tag{23}$$

5.4. **Definition.** Let L be a lattice and let $\mathbb{A}$ be an ordered Abelian group. A *free $\mathbb{A}$-latroid with length function $\|\cdot\|$ on lattice L* is a pair $(\|\cdot\|, L)$, where the function $\|\cdot\| : L \to \mathbb{A}$ satisfies the following three conditions:

(i) $\|\cdot\|$ is *normalized*, that is, $\|0_L\| = 0_{\mathbb{A}}$.
(ii) $\|\cdot\|$ is *strictly increasing*, that is, $\|l\| < \|m\|$ for all $l, m \in L$ with $l < m$.
(iii) $\|\cdot\|$ is *modular*, that is, $\|l\| + \|m\| = \|l \wedge m\| + \|l \vee m\|$ for all $l, m \in L$.

A lattice L is *modular* [17, 19] if

$$\forall x, y, z \in L \ : \ x \leq z \Longrightarrow x \vee (y \wedge z) = (x \vee y) \wedge z. \tag{24}$$

5.5. **Lemma.** (i) *For any module M, the lattice $\mathcal{L}(M)$ is modular.*
(ii) *Every sublattice of a modular lattice is modular.*
(iii) *Every product of modular lattices is modular.*
(iv) *If $(\|\cdot\|, L)$ is a free latroid, then L is a modular lattice.*

Proof. Parts (i), (ii) and (iii) are standard. Now suppose $x, y, z \in L$ and $x \leq z$. Combining the modularity equation (iii) of Definition 5.4, where (l, m) takes values (y, z), (x, y), $(x \vee y, z)$, $(x, y \wedge z)$, yields the equation $\|x \vee (y \wedge z)\| = \|(x \vee y) \wedge z\|$.

But in any lattice, if $x \leq z$, then $x \vee (y \wedge z) \leq (x \vee y) \wedge z$. Then (ii) of Definition 5.4 implies that $x \vee (y \wedge z) = (x \vee y) \wedge z$. □

5.6. **Definition.** Given $L, \mathbb{A}, \|\cdot\|$ as in Definition 5.4, an *$\mathbb{A}$-latroid with rank function ρ under length function $\|\cdot\|$ on lattice L*, is a triple $(\rho, \|\cdot\|, L)$, where the pair $(\|\cdot\|, L)$ is a *free $\mathbb{A}$-latroid on L* and the function $\rho : L \to \mathbb{A}$ satisfies the following three conditions:

(i) ρ is *normalized*, that is, $\rho(0_L) = 0_{\mathbb{A}}$.
(ii) ρ is *bounded increasing*, that is, $0 \leq \rho(m) - \rho(l) \leq \|m\| - \|l\|$ for all $l, m \in L$ with $l \leq m$.
(iii) ρ is *submodular*, that is, $\rho(l) + \rho(m) \geq \rho(l \wedge m) + \rho(l \vee m)$ for all $l, m \in L$.

We may also say that $(\|\cdot\|, \|\cdot\|, L)$ is a free latroid, regarding 'free' as an adjective specializing to the case $\rho = \|\cdot\|$. We omit reference to $\mathbb{A}$ if it is known from the context.

5.7. **Example.** If E is a finite set, $L = 2^E$ is the lattice of all subsets of E, and $|A|$ denotes the cardinality of $A \subseteq E$, then $(\rho, |\cdot|, 2^E)$ is a $\mathbb{Z}$-latroid if and only if (ρ, E) is a matroid.

More generally, for a positive integer j, $(\rho, j|\cdot|, 2^E)$ is a $\mathbb{Z}$-latroid, where $j|\cdot| : A \mapsto j|A|$ if and only if (ρ, E) is a *j-polymatroid*, that is, a function $\rho : 2^E \to \mathbb{Z}$, that is normalized, submodular and for which $\rho(B) - \rho(A) \leq j|B| - j|A|$ whenever $A \subseteq B \subseteq E$.

More generally still, a $\mathbb{Z}^k$-latroid $(\rho, \|\cdot\|, 2^E)$ can be regarded as a k-tuple of polymatroids, all on the ground set E.

We often use the isomorphism theorems ([1], Corollary 3.7), in particular for modules $l, C \leq M$,

$$l/(l \cap C) \cong (l + C)/C. \tag{25}$$

From a code C with lattice L we define a latroid.

5.8. **Example.** Let S be a right Artinian ring and suppose $C \leq M$ are finitely generated right S-modules. Suppose L is a 0-1 sublattice of $\mathcal{L}(M)$. (Note: $\wedge$ and

$\vee$ here are $\cap$ and $+$.) Let $\|\cdot\| : L \to \mathbb{Z}^k$ be the length function as defined in Section 4.

Define $\rho_C : L \to \mathbb{Z}^k$ in any of the following equivalent ways (see Proposition 4.1 and (25)):

$$\rho_C(l) = \|l\| - \|l \cap C\| = \|l/(l \cap C)\| = \|(l + C)/C\| = \|l + C\| - \|C\|. \tag{26}$$

Note that with the natural epimorphism $h : M \to M/C$, see (21), the image of $l \leq M$ under h is $h(l) = l/(l \cap C)$, which we may identify with $h(l+C) = (l+C)/C$. Thus we also have

$$\rho_C(l) = \|h(l)\| \tag{27}$$

and we may view the cocode $h(M) = M/C$, together with the image $h(l)$ of every $l \in L$, as a geometric realization of ρ_C.

5.9. **Lemma.** *With everything as in Example 5.8, $(\rho_C, \|\cdot\|, L)$ is a $\mathbb{Z}^k$-latroid determined by C and L, and similarly for finite Abelian groups and finitely generated left modules or bimodules over Artinian rings.*

Proof. By Proposition 4.1(c), $\|\cdot\|$ is modular. Abbreviate ρ_C to ρ. Trivially, ρ is normalized. Now for $l, m \in L$ with $l \leq m$,

$$\begin{aligned} \rho(m) - \rho(l) &= \|m\| - \|l\| - \|m \cap C\| + \|l \cap C\| \\ &= \|m/l\| - \|(m \cap C)/(l \cap C)\| \\ &= \|m/l\| - \|(m \cap C)/((m \cap C) \cap l)\| \\ &= \|m/l\| - \|((m \cap C) + l)/l)\| \quad \text{by (25)} \\ &= \|m\| - \|(m \cap C) + l\|. \end{aligned} \tag{28}$$

Clearly $l \leq (m \cap C) + l \leq m$, so it follows that ρ is bounded increasing under $\|\cdot\|$.

For $l, m \in L$, using $\rho(l) = \|l + C\| - \|C\|$ from (26),

$$\begin{aligned} & \rho(l) + \rho(m) - \rho(l \wedge m) - \rho(l \vee m) \\ = \; & \|l + C\| + \|m + C\| - \|(l \cap m) + C\| - \|(l + m) + C\| \\ = \; & \|l + C\| + \|m + C\| - \|(l + C) \cap (m + C)\| - \|(l + C) + (m + C)\| \\ & + \|(l + C) \cap (m + C)\| - \|(l \cap m) + C)\| \\ & \text{(noting that } (l + m) + C = (l + C) + (m + C)) \\ = \; & \|(l + C) \cap (m + C)\| - \|(l \cap m) + C)\| \text{ by Proposition 4.1(c)} \\ \geq \; & 0 \text{ by a distributive inequality, Theorem 15 (vii) of [17].} \end{aligned} \tag{29}$$

Hence ρ is submodular. □

We say that ρ_C is the latroid *represented* by the code with lattice (C, L), or for short, by the code C. While (C, L) uniquely determines ρ_C, there may be many other codes which also represent ρ_C.

For a latroid $\rho = (\rho, \|\cdot\|, L)$ and $l, m \in L$ with $l \leq m$, we define the *minor* of ρ obtained by *contracting* l and *deleting* (or *restricting*) *to* m as follows: It is denoted by the triple $(\rho{:}[l,m], \|\cdot\|_{[l,m]}, [l,m])$, abbreviated by $\rho{:}[l,m]$. It is defined by

$$\begin{aligned} \|x\|_{[l,m]} &= \|x\| - \|l\|, \\ (\rho{:}[l,m])(x) &= \rho(x) - \rho(l) \end{aligned} \tag{30}$$

for all $x \in [l, m]$.

5.10. **Lemma.** $(\rho{:}[l,m], \|\cdot\|_{[l,m]}, [l,m])$ *is indeed a latroid.*

Proof. The constant (with respect to x) terms $\|l\|$ and $\rho(l)$ subtracted on the right-hand side of (30) ensure that $\|\cdot\|_{[l,m]}$ and $\rho{:}[l,m]$ are normalized, while clearly preserving the other conditions. □

We now relate code minors to latroid minors, generalizing the first line of (10), after addressing one notational issue. Recall that the code minor $C{:}[l,m]$ is with the lattice $L{:}[l,m]$ which is isomorphic to $[l,m]$ via $\alpha : [l,m] \to L{:}[l,m]$, where $\alpha(x) = x/l$. Both the code minor $C{:}[l,m]$ and the latroid minor $\rho{:}[l,m]$ are determined by the interval sublattice, $[l,m]$. Now $[l,m]$, as an abstract lattice, can serve as the lattice for $\rho{:}[l,m]$. But for $C{:}[l,m]$, a code in the ambient module m/l, we need a concrete sublattice of $\mathcal{L}(m/l)$, which is why $L{:}[l,m]$ must be used, rather than $[l,m]$.

5.11. **Lemma.** *For a code $C \leq M$ with lattice L, and $l, m \in L$, $l \leq m$, we have*

$$\rho_{C:[l,m]} = (\rho_C){:}[l,m] \tag{31}$$

with the understanding that lattices $L{:}[l,m]$ and $[l,m]$ are identified via the isomorphism $\alpha : [l,m] \to L{:}[l,m]$, where $\alpha(x) = x/l$.

Proof. We wish to show equality of (31) as triples (rank, length, lattice). We have already identified the lattices. Now for $x/l \in L{:}[l,m]$, that is, for $l \leq x \leq m$ with $x \in L$,

$$\|x/l\|_{L:[l,m]} = \|x\| - \|l\| = \|x\|_{[l,m]}\,. \tag{32}$$

For the natural epimorphism $h : M \to M/C$ and $w \in M$ we shall identify $w/(w \cap C) = h(w) = (w + C)/C$, and similarly for the natural epimorphism from M to M/l. Now from (22) and (26)

$$\rho_{C:[l,m]}(x/l) = \|x/l\| - \|(x/l) \cap ((m \cap C)/(l \cap C))\| \tag{33}$$

but by (25), $(m \cap C)/(l \cap C) = ((m \cap C) + l)/l$ and $(x/l) \cap (((m \cap C) + l)/l) = (x \cap ((m \cap C) + l))/l$. Also, by using $l \leq x \leq m$ and lattice modularity (24) twice,

$$\begin{array}{rcl} x \cap ((m \cap C) + l) &=& x \cap (m \cap (C + l)) \\ &=& x \cap m \cap (C + l) \\ &=& x \cap (C + l) \\ &=& (x \cap C) + l \end{array} \tag{34}$$

and by (25), $((x \cap C) + l)/l = (x \cap C)/(l \cap C)$. So

$$\begin{array}{rcl} \rho_{C:[l,m]}(x/l) &=& \|x/l\| - \|(x \cap C)/(l \cap C)\| \\ &=& \|x\| - \|x \cap C\| - \|l\| + \|l \cap C\| \\ &=& \rho_C(x) - \rho_C(l) \\ &=& (\rho_C{:}[l,m])(x), \end{array} \tag{35}$$

as required. □

To generalize the second line of (10), we need to define code duality (done below in Section 6) and latroid duality, which we now consider.

5.12. **Definition.** The *dual* of a lattice L is the lattice denoted $L^\perp$ with elements denoted $L^\perp = \{x^\perp : x \in L\}$. The relation $\leq$, the operations $\vee$ and $\wedge$, and the 0

and 1 in lattice $L^\perp$ are given by

$$\begin{array}{rcl} x^\perp \le y^\perp & \iff & y \le x, \\ x^\perp \wedge y^\perp & = & (x \vee y)^\perp, \\ x^\perp \vee y^\perp & = & (x \wedge y)^\perp, \\ 0_{L^\perp} & = & (1_L)^\perp, \\ 1_{L^\perp} & = & (0_L)^\perp. \end{array} \tag{36}$$

We identify $x^{\perp\perp} = x$ and $L^{\perp\perp} = L$.

5.13. **Definition.** The dual of the latroid $\rho = (\rho, \|\cdot\|, L)$ is $\rho^\perp = (\rho^\perp, \|\cdot\|^\perp, L^\perp)$ where for $x^\perp \in L^\perp$,

$$\begin{array}{rcl} \left\|x^\perp\right\|^\perp & = & \|1_L\| - \|x\|, \\ \rho^\perp(x^\perp) & = & \left\|x^\perp\right\|^\perp - (\rho(1_L) - \rho(x)). \end{array} \tag{37}$$

A couple of convenient forms for the last equation are

$$\begin{array}{rcl} \left\|x^\perp\right\|^\perp - \rho^\perp(x^\perp) & = & \rho(1_L) - \rho(x), \\ \|x\| - \rho(x) & = & \rho^\perp(1_{L^\perp}) - \rho^\perp(x^\perp) \end{array} \tag{38}$$

and from (37) with $x = 0_L$ we observe that

$$\begin{array}{rcl} \|1_{L^\perp}\|^\perp & = & \|1_L\|, \\ \rho^\perp(1_{L^\perp}) & = & \|1_L\| - \rho(1_L) \end{array} \tag{39}$$

and we can relate 'length differences' and 'rank differences' by noting that for any $x, y \in L$,

$$\begin{array}{rcl} \|y\| - \|x\| & = & \left\|x^\perp\right\|^\perp - \left\|y^\perp\right\|^\perp \\ = \quad \rho(y) - \rho(x) & + & \rho^\perp(x^\perp) - \rho^\perp(y^\perp)\ . \end{array} \tag{40}$$

We generalize the first lines of (3) and (9) as follows.

5.14. **Lemma.** *For a latroid $\rho = (\rho, \|\cdot\|, L)$ and $l, m \in L$ with $l \le m$,*

(i) *$\rho^\perp = (\rho^\perp, \|\cdot\|^\perp, L^\perp)$ is indeed a latroid,*
(ii) *$(\rho, \|\cdot\|, L)^{\perp\perp} = (\rho, \|\cdot\|, L)$,*
(iii) *$(\rho{:}[l, m])^\perp = \rho^\perp{:}[m^\perp, l^\perp]$,*
(iv) *$(\|\cdot\|_{[l,m]})^\perp = (\|\cdot\|^\perp)_{[m^\perp, l^\perp]}$.*

Proof. The proofs of the corresponding standard matroid results are routinely generalized. □

6. Duality

We have discussed latroid duality. Now we consider code duality. There are category dualities between categories of modules, including *Morita dualities* (see [1] and below). In [22], code duality is related to Morita duality by Jay Wood, who attributes the idea to an anonymous referee of that paper.

It turns out that in generalizing results of Greene [8] and other classical results in Section 2 about codes and matroids over fields to codes and latroids over rings and modules, Morita duality is exactly what we need. Actually some results work for more general module category dualities, but we will stick with Morita duality here.

We give a brief survey, but also refer the reader to [1] for more details and for definitions of *italicized* terms that are left undefined here. Recall the categories of

modules ${}_R\mathfrak{F}$ and $\mathfrak{F}_S$ from Section 4. Let ${}_RU_S$ be an (R,S)-*bimodule*. We define a pair of *contravariant functors* determined by ${}_RU_S$, denoted ${}^* : \mathfrak{F}_S \rightleftharpoons {}_R\mathfrak{F}$, where, for a module or a homomorphism X in ${}_R\mathfrak{F}$ or $\mathfrak{F}_S$,

$$X^* = \mathrm{Hom}(X, {}_RU_S). \tag{41}$$

For example, if X is a right S-module, the set of all S-module homomorphisms from X_S to ${}_RU_S$ forms a left R-module, denoted X^*.

If ${}_RU_S$ is *injective* as both a right S-module and a left R-module, then * is an *exact* functor, in the sense that, in the diagram below, the upper sequence is exact if and only if the lower sequence is exact:

$$\begin{array}{ccccc} C & \xrightarrow{f} & M & \xrightarrow{g} & N \\ C^* & \xleftarrow{f^*} & M^* & \xleftarrow{g^*} & N^*. \end{array} \tag{42}$$

Now ${}^* : \mathfrak{F}_S \rightleftharpoons {}_R\mathfrak{F}$ is a *Morita duality* if ** is *naturally equivalent* to the identity on both $\mathfrak{F}_S$ and ${}_R\mathfrak{F}$. Every Morita duality * is determined by some bimodule ${}_RU_S$, in the above sense, and two Morita dualities are naturally equivalent if and only if the corresponding bimodules are isomorphic as bimodules. A bimodule ${}_RU_S$ determines a Morita duality if and only if ${}_RU_S$ is a *balanced* bimodule such that ${}_RU$ and U_S are *injective cogenerators*. Definitions of these terms, and other details, are found in [1].

The most familiar Morita duality is when $U = R = S = K$, for a field K, which will correspond to the case summarized in Section 2, as some further discussion may clarify. Rather than delving into the theory of Morita duality, we will spell out the appropriate properties of Morita dualities, and how they relate to the topics of this paper.

Consider a code $C \leq M$ in $\mathfrak{F}_S$. Much information is contained in the following picture, in which the *dual code* $C^\perp$ is defined:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C & \longrightarrow & M & \longrightarrow & M/C & \longrightarrow & 0 \\ 0 & \longleftarrow & C^* \cong M^*/(C^\perp) & \longleftarrow & M^* & \longleftarrow & (M/C)^* \cong C^\perp & \longleftarrow & 0. \end{array} \tag{43}$$

The upper, lower row is a short exact sequence in $\mathfrak{F}_S$, ${}_R\mathfrak{F}$, respectively, with * swapping terms (up to isomorphism) directly above and below each other.

It is essential that we distinguish between C^*, which we call the *Morita dual* or *category dual* or **-dual* (*star dual*) of C, with $C^\perp$, which we call the *code dual* or *orthogonal complement* or ${}^\perp$*-dual* (*perp dual*) of C.

Note that C^* depends only on C, whereas, $C^\perp$ depends on both C and the ambient module M. Define $(M/C)^\perp = M^*/(C^\perp)$ so that ${}^\perp$-duality sends codes to codes and cocodes to cocodes. In a sense, the *-duality swaps between the two exact sequences reading left to right, whereas the ${}^\perp$-duality swaps between the two exact sequences reading along the arrows. So the cocode $M/C = C^{*\perp} = C^{\perp *}$.

More discussion about code and Morita duality, and their interaction with code minors in the context of categories of modules, appears in Section 7.

Here is a more explicit description of $C^\perp$, which also depends on M. For $w \in M$ and $\lambda \in M^* = \mathrm{Hom}(M, {}_RU_S)$ define the *inner product* $\langle w, \lambda \rangle = \lambda(w) \in {}_RU_S$. Then

$$C^\perp = \{\lambda \in M^* : \langle w, \lambda \rangle = 0 \text{ for all } w \in C\} \tag{44}$$

which resembles (1) as we would want. Then from [1],

$$C^{\perp\perp} = C. \tag{45}$$

Moreover, via the mapping $x \mapsto x^\perp$, the lattices $\mathcal{L}(M)$ and $\mathcal{L}(M^*)$ are anti-isomorphic [1], that is, one is isomorphic to the lattice-dual of the other.

6.1. **Definition.** For a code $C \leq M$ with lattice L, the *code-dual* or $^\perp$*-dual* of (C, L) is $(C, L)^\perp = (C^\perp, L^\perp)$, where $C^\perp$ is as above and $L^\perp$ is the 0-1 sublattice of $\mathcal{L}(M^*)$ with elements $L^\perp = \left\{x^\perp \in \mathcal{L}(M^*) : x \in L\right\}$.

For dualizing a latroid, $L^\perp$ is just an abstract lattice, with elements called $x^\perp$. But for dualizing a code, $L^\perp$ is a concrete lattice, and each element $x^\perp \in L^\perp$ is a module as given in (44) with module x in place of C.

Recall the definition of length $\|M\|$ for $M \in \mathfrak{F}_S$, from Section 4. By facts about Morita duality [1], if $S_1, S_2, \ldots, S_k$ are the simple right S-modules, then $S_1^*, S_2^*, \ldots, S_k^*$ are the simple left R-modules. Moreover, for every $i \in [k]$, the simple module S_i appears exactly r_i times as a composition factor of M if and only if the simple module S_i^* appears exactly r_i times as a composition factor of M^*. The conclusion is that Morita duality preserves length, that is, for every $M \in \mathfrak{F}_S$ or $M \in {}_R\mathfrak{F}$,

$$\|M\| = \|M^*\| . \tag{46}$$

For the $^\perp$-dual, we find for any submodule C of M

$$\left\|C^\perp\right\| = \|(M/C)^*\| = \|M/C\| = \|M\| - \|C\| . \tag{47}$$

A key observation is that Morita duality swaps module epimorphisms and monomorphisms which were used to define contraction and deletion. Thus we expect an appropriate interaction between code minors and code duality, as in (9).

Note that the length function, $\|\cdot\|$, for the latroid of any code obtained by taking minors and/or duals, whenever applied to any element of $\mathfrak{F}_S$ or ${}_R\mathfrak{F}$, will be the length function $\|\cdot\|$ defined immediately before Proposition 4.1.

With such observations, we can generalize more results from Section 2 such as (3), (9), and (10). Recall the definition of the latroid ρ_C represented by the code C, immediately following Lemma 5.9.

6.2. **Lemma.** *For a code $C \leq M$ with lattice L, and $l, m \in L$ with $l \leq m$,*

(i) $(C, L)^{\perp\perp} = (C, L)$,
(ii) $\rho_{(C^\perp)} = (\rho_C)^\perp$,
(iii) $\rho_{C:[l,m]} = (\rho_C){:}[l, m]$,
(iv) $(C{:}[l, m])^\perp = C^\perp{:}[m^\perp, l^\perp]$.

Proof. Part (i) follows from the definitions. Lemma 5.11 already gave (iii), which is restated here for convenience.

To prove (ii) consider any $x \in L$, $x^\perp \in L^\perp$. Now $(x + C)^\perp = x^\perp \cap C^\perp$ by Theorem 24.5 of [1]. Also $\left\|x^\perp\right\|^\perp = \left\|x^\perp\right\|$, where the left-hand side uses the length function for the latroid $(\rho_C)^\perp$ while the right-hand side uses the length function in

${}_R\mathfrak{F}$. Then

$$\begin{aligned}
\rho_{(C^\perp)}(x^\perp) &= \left\|x^\perp\right\| - \left\|x^\perp \cap C^\perp\right\| \quad \text{by (26)} \\
&= \left\|x^\perp\right\| - \left\|(x+C)^\perp\right\| \\
&= (\|M\| - \|x\|) - (\|M\| - \|x+C\|) \quad \text{by (47)} \\
&= \|x+C\| - \|x\| \\
&= \|C\| - \|x \cap C\| \quad \text{by (26)} \\
&= (\|M\| - \|x\|) - \big((\|M\| - \|M \cap C\|) - (\|x\| - \|x \cap C\|)\big) \\
&= \left\|x^\perp\right\|^\perp - (\rho_C(1_L) - \rho_C(x)) \text{ by (37), (26) and } M = 1_L \\
&= (\rho_C)^\perp(x^\perp) \text{ by (37).}
\end{aligned} \tag{48}$$

Finally, (iv) follows from basic facts about Morita duality. □

7. A big picture

Figure 1 is a dual pair of commuting diagrams, in which all straight lines are short exact sequences.

The upper diagram is a classic diagram (see the front cover of [2]). The lower diagram is the Morita dual of the upper diagram. We adopt the convention that the correspondence between the entries in one diagram and their Morita duals in the other diagram are given by a translation with no reflection or rotation. Restricting Figure 1 to the middle row of both the upper and lower diagrams gives (43).

Note that in going between diagrams, all arrows are reversed and short exact sequences go to short exact sequences. Thus, duality swaps monomorphisms and epimorphisms, and as a consequence, duality swaps the roles of deletion and contraction.

In the upper diagram, C and x appear to be interchangeable, but we will assign them different roles. Suppose we are considering minors of a code $C \leq M$ with lattice L, a 0-1 sublattice of $\mathcal{L}(M)$. Suppose $x \in L$.

Recall that we could think of the code as consisting of the whole short exact sequence $0 \to C \to M \to M/C \to 0$, the middle horizontal row in the upper diagram. We can view any code minor in a similar way.

If we restrict or delete to x, then we get

$$C{:}[0_L, x] = C{:}[0, x] = C|x = C \cap x \leq x. \tag{49}$$

This code is illustrated by shifting to the upper horizontal row in the upper diagram.

Similarly, if we contract x, then we get

$$C{:}[x, 1_L] = C{:}[x, M] = C/x = C/(x \cap C) \leq M/x. \tag{50}$$

Here C/x denotes C contract x while $C/(x \cap C)$ denotes the factor module C modulo $x \cap C$, that is, the image of C under the natural epimorphism $M \to M/x$.

This code is illustrated by shifting to the lower horizontal row in the upper diagram.

Any sequence of deletions and contractions is equivalent to a deletion followed by a contraction (or visa-versa). So to find the minor $C{:}[l, m]$, we do one of each of the above types of moves with x in the role of m (respectively, l) for deletion (respectively, contraction).

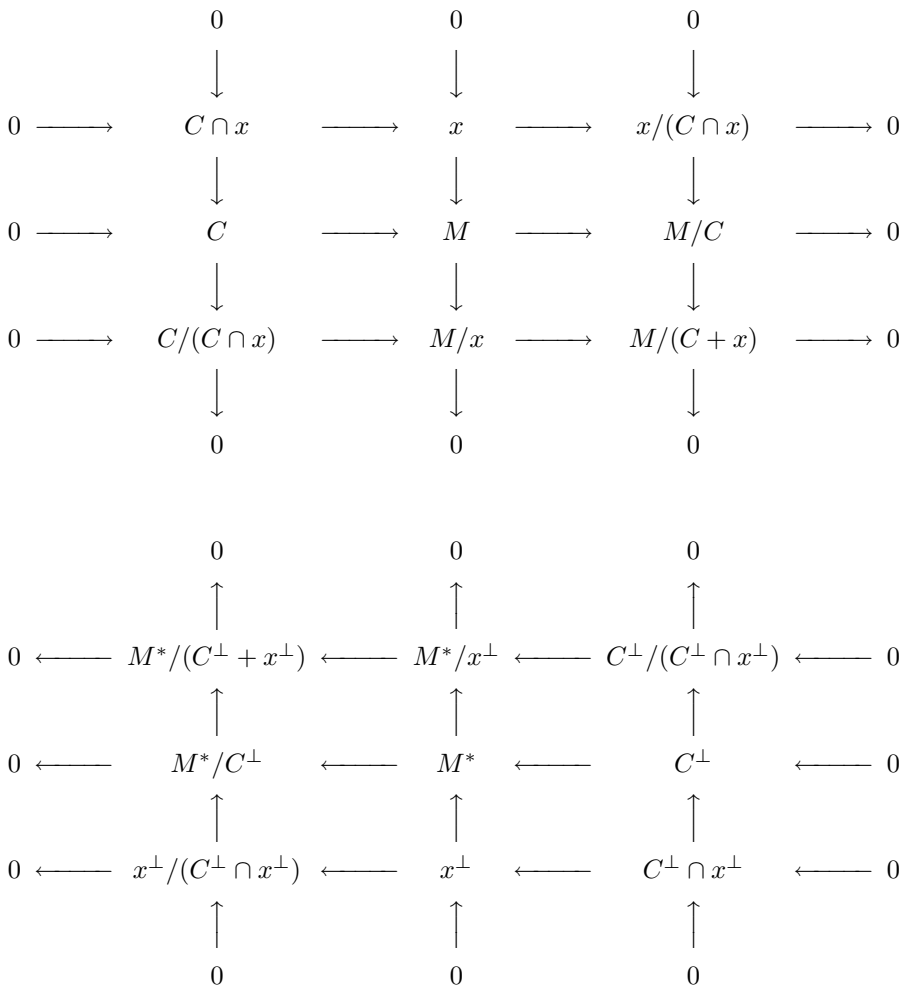

FIGURE 1. A dual pair of commutative diagrams; see Section 7.

We must also describe and illustrate minors for the lattice L with C. Suppose we are taking the minor specified by the subinterval $[l, m]$ of $\mathcal{L}(M)$. Each $y \in L$ with $y \notin [l, m]$ is discarded. But for each $y \in [l, m]$, we put y in place of C in the diagrams and above discussion, and do for y exactly what we did for C.

The interaction between minors and duality may be understood by applying the above descriptions simultaneously to the upper and lower diagrams.

8. Generating functions

Let $\rho = (\rho, \|\cdot\|, L)$ be an $\mathbb{A}$-latroid. We define a generating function for ρ. It will be a polynomial or an infinite series with integer coefficients in commuting variables

$$\mathbf{u}^m,\ \mathbf{v}^{m^\perp} \text{ for all } m \in L, \tag{51}$$

$$\mathbf{x}^a,\ \mathbf{y}^a \text{ for all } a \in \mathbb{A}, \tag{52}$$

We treat these as independent variables except for the condition that

$$\mathbf{x}^a\mathbf{x}^b = \mathbf{x}^{a+b},\ \mathbf{y}^a\mathbf{y}^b = \mathbf{y}^{a+b} \text{ for all } a, b \in \mathbb{A}. \tag{53}$$

Negative integer powers of variables are allowed, although multiplication by an appropriate factor can convert all equations here to polynomial equations.

In some cases we will impose further dependencies between the variables, for example by interpreting the symbols as described at the end of Section 1. These generating functions will typically be written as a sum of monomials, and we need only ensure that each monomial appears only finitely often in the summation for it to be well-defined.

8.1. **Definition.** The weighted Tutte-Whitney rank generating function, TW-function, of an $\mathbb{A}$-latroid $\rho = (\rho, \|\cdot\|, L)$ is defined to be

$$R(\rho, \|\cdot\|, L; \mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}) = \sum_{m\in L} \mathbf{u}^m\mathbf{v}^{m^\perp}\mathbf{x}^{\rho(1_L)-\rho(m)}\mathbf{y}^{\|m\|-\rho(m)}. \tag{54}$$

Note the resemblance to (12) and (13). Here 'weighted' refers to the term $\mathbf{u}^m\mathbf{v}^{m^\perp}$. It may seem to be redundant having $\mathbf{u}^m\mathbf{v}^{m^\perp}$ instead of just $\mathbf{u}^m$, but there are aesthetic reasons of symmetry for doing this. The TW-function is homogeneous of degree one in the variables $\mathbf{u}^m\mathbf{v}^{m^\perp}$, $m \in L$. Note that the TW-function completely describes $(\rho, \|\cdot\|, L)$.

Naturally this gives rise to a generating function for codes.

8.2. **Definition.** For a code $C \leq M$ with lattice L and length function $\|\cdot\|$, the complete weight enumerator for $C = (C, \|\cdot\|, L)$ via submodules is defined to be

$$\begin{aligned} R(C, \|\cdot\|, L; \mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}) = &\quad R(\rho_C, \|\cdot\|, L; \mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}) \\ = &\quad \sum_{m\in L} \mathbf{u}^m\mathbf{v}^{m^\perp}\mathbf{x}^{\rho_C(1_L)-\rho_C(m)}\mathbf{y}^{\|m\|-\rho_C(m)}, \end{aligned} \tag{55}$$

that is, it is simply the TW-function of ρ_C.

We may also consider another type of generating function for codes.

8.3. **Definition.** For a code $C \leq M$, let $\mathbf{w}^c$, $\mathbf{z}^c$ be independent commuting variables for all $c \in M$. Then the complete weight enumerator for C via elements is

$$W(C; \mathbf{w}, \mathbf{z}) = \sum_{c\in C} \mathbf{w}^c\mathbf{z}^c. \tag{56}$$

Again using $\mathbf{w}^c\mathbf{z}^c$ instead of just, say, $\mathbf{z}^c$ seems redundant, but there are reasons of convenience for doing this. Now (15) can be generalized to all latroids, relating the TW-function of a latroid to that of its dual. In (15) we can say that matroid duality swaps x with y. In (57) below, we can say that latroid duality swaps $\mathbf{u}$ with $\mathbf{v}$, and swaps $\mathbf{x}$ with $\mathbf{y}$.

8.4. **Theorem.** *For any latroid $(\rho, \|\cdot\|, L)$ it holds that*

$$R(\rho^\perp, \|\cdot\|^\perp, L^\perp; \mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}) = R(\rho, \|\cdot\|, L; \mathbf{v}, \mathbf{u}, \mathbf{y}, \mathbf{x}). \tag{57}$$

Proof. The left-hand side equals

$$\sum_{m^\perp\in L^\perp} \mathbf{u}^{m^\perp}\mathbf{v}^m\mathbf{x}^{\rho^\perp(1_{L^\perp})-\rho^\perp(m^\perp)}\mathbf{y}^{\|m^\perp\|^\perp-\rho^\perp(m^\perp)}. \tag{58}$$

Now summing over all $m^\perp \in L^\perp$ is equivalent to summing over all $m \in L$. Using (38), this equals

$$\sum_{m\in L} \mathbf{u}^{m^\perp}\mathbf{v}^m\mathbf{x}^{\|m\|-\rho(m)}\mathbf{y}^{\rho(1_L)-\rho(m)} \tag{59}$$

which equals the right-hand side. □

8.5. **Corollary.** *Equation* (15) *holds.*

Proof. The two parts of (15) are equivalent by (13). Set $(\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}) = (1,1,x,y)$ in (57), and, recalling Example 5.7, specialize to $L = 2^E = L^\perp$, $\mathbb{A} = \mathbb{Z}$, $\|\cdot\| = |\cdot| = \|\cdot\|^\perp$, $m = A \subseteq E$, $m^\perp = \overline{A} = E - A$. □

Any identity relating some generating function of a code to that of a dual code is generally called a *MacWilliams identity* [12, 13]. We get such an identity as an immediate corollary of the above theorem.

8.6. **Corollary.** *Let $C \leq M \in \mathfrak{F}_S$ be a code with lattice L. Let $C^\perp \in {}_R\mathfrak{F}$ be the $^\perp$-dual code with lattice $L^\perp$ defined via a Morita duality $^* : \mathfrak{F}_S \rightleftharpoons {}_R\mathfrak{F}$. Then*

$$R(C^\perp, \|\cdot\|^\perp, L^\perp; \mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}) = R(C, \|\cdot\|, L; \mathbf{v},\mathbf{u},\mathbf{y},\mathbf{x}). \tag{60}$$

Proof. Combine Definition 8.2 with Theorem 8.4. □

These identities also work in the 'grounded' case when we have lattice $L = \mathbf{L}^E = \prod_{e\in E} L_e$. The only real difference is how we interpret terms such as $\mathbf{u}^m$, $m \in L$. For all $e \in E$, $m_e \in L_e$ let $u_e^{m_e}$ be independent commuting variables and for the $|E|$-tuple $m \in \mathbf{L}^E$, $m = (m_e : e \in E)$, define $\mathbf{u}^m = \prod_{e\in E} u_e^{m_e}$. Define $\mathbf{v}^{m^\perp}$ similarly.

We can choose a similar convention when the ordered Abelian group $\mathbb{A}$ is a direct product, for example $\mathbb{A} = \mathbb{Z}^k$ as we use for codes. Let x_i, y_i, where $i \in [k]$ be independent commuting variables. For $a = (a_i : i \in [k])$ define $\mathbf{x}^a = \prod_{i\in[k]} x_i^{a_i}$ and $\mathbf{y}^a = \prod_{i\in[k]} y_i^{a_i}$.

9. More identities

Corollary 8.6 gives, in full generality, a MacWilliams identity for complete weight enumerators via submodules for code duality defined in terms of any Morita duality and for any chosen lattice L. Essentially this is because Morita duality dualizes everything needed for such an identity.

However, if we change 'via submodules' to 'via elements' we may run into difficulties. We will speak loosely of vS (via submodule) and vE (via element) identities and enumerators.

Consider the following depiction of generating functions and identities:

$$\begin{array}{ccc} R(C^\perp) & \longleftrightarrow & R(C) \\ \updownarrow & & \updownarrow \\ W(C^\perp) & \dashleftarrow\dashrightarrow & W(C) \end{array} \tag{61}$$

Here $R(C^\perp)$ and $R(C)$ are vS enumerators as in Definition 8.2, whereas $W(C^\perp)$ and $W(C)$ are vE enumerators as in Definition 8.3. The arrows represent identities relating these enumerators or specializations thereof. Now $R(C^\perp)$ and $R(C)$ are

related as much as could be wanted in (60) which generalizes (15), exemplifying the upper horizontal arrow in (61). In [8], which covers the case where the Morita duality is determined by ${}_KK_K$ where K is a finite field, the vertical arrows in (61) are exemplified by (16) (or (17)), the upper horizontal arrow in (61) is exemplified by (15), and then from these, the vE MacWilliams identity, (18), is deduced, exemplifying the lower horizontal arrow in (61).

Essentially the connection from $W(C^\perp)$ to $W(C)$ in the 'classical, finite field' case was deduced in [8] by traversing the other three sides of the square in (61). However it may not always be possible to generalize (17) as much as we would like, which provides an obstacle to deducing vE identities as a consequence of vS identities. Of course, one may ignore vS identities completely and search directly for vE identities. Alternatively, one may ignore vE identities and be completely satisfied with (60). Nevertheless, we will proceed with the 'three sides' approach to produce decent generalizations of (17) and hence of (18).

For a Morita duality $^* : \mathfrak{F}_S \rightleftharpoons {}_R\mathfrak{F}$, an element of a module $c \in M \in \mathfrak{F}_S$ is *not* one of the things that Morita duality dualizes. We are prompted to make the following definition.

9.1. **Definition.** For finite rings R, S, the Morita duality $^* : \mathfrak{F}_S \rightleftharpoons {}_R\mathfrak{F}$ is *equicardinal* if and only if $|M^*| = |M|$ for every $M \in \mathfrak{F}_S$ (or $M \in {}_R\mathfrak{F}$).

Note that if R and S are finite, then so is every module in $\mathfrak{F}_S$ and ${}_R\mathfrak{F}$; see Section 4.

Not every Morita duality is equicardinal; see Theorems 10.2, 10.3(i), (ii) for example. We will show one type of vE MacWilliams identity that holds for equicardinal Morita dualities.

Suppose the ring S is finite and $S_1, \dots, S_k$ are the distinct simple right S-modules, as in Section 4. Let $\mathbf{s} = (s_i : i \in [k])$, where $s_i = |S_i|$ for $i \in [k]$.

For a module $M \in \mathfrak{F}_S$ if $\|M\| = \mathbf{a} = (a_1, \dots, a_k)$, then

$$|M| = \mathbf{s}^{\|M\|} = \prod_{i=1}^{k} s_i^{a_i}, \tag{62}$$

as can be shown by considering the composition series of M and using induction. If $^* : \mathfrak{F}_S \rightleftharpoons {}_R\mathfrak{F}$ is a Morita duality and $S_1^*, \dots, S_k^*$ are the corresponding simple modules in ${}_R\mathfrak{F}$, then we may similarly define $\mathbf{s}^* = (s_i^* : i \in [k])$, where $s_i^* = |S_i^*|$, and for $N \in {}_R$ we have

$$|N| = (\mathbf{s}^*)^{\|N\|}. \tag{63}$$

9.2. **Lemma.** *With $^* : \mathfrak{F}_S \rightleftharpoons {}_R\mathfrak{F}$ and $\mathbf{s}, s^*$ as above, the following are equivalent:*

(i) ** is an equicardinal Morita duality.*
(ii) $\mathbf{s} = \mathbf{s}^*$.

Proof. Clearly (i) implies (ii). But considering (62) and (63) with (46), we see that (ii) is sufficient for (i). □

For $c \in \mathbf{M}^E = \prod_{e\in E} M_e$ written as $c = (c_e : e \in E)$, where $c_e \in M_e$ for every $e \in E$, the *support* of c is defined and denoted by $\operatorname{supp}(c) = \{e \in E : c_e \neq 0\}$, and its complement is $\overline{\operatorname{supp}(c)} = E - \operatorname{supp}(c)$. If we had written $c \in \mathbf{M}^E = \bigoplus_{e\in E} M_e$, then we would uniquely write $c = \sum_{e\in E} c_e$, where $c_e \in M_e$ for every $e \in E$, and again $\operatorname{supp}(c) = \{e \in E : c_e \neq 0\}$.

We will work with the following specialization of Definition 8.3, the complete weight enumerator via elements.

9.3. **Definition.** Suppose R and S are finite rings. Let $C \leq \mathbf{M}^E$ in $\mathfrak{F}_S$ or ${}_R\mathfrak{F}$ be a code with ground set E. For each $e \in E$, let w_e, z_e be commuting variables, and for $A \subseteq E$, define $\mathbf{w}^A = \prod_{e\in A} w_e$ and $\mathbf{z}^A = \prod_{e\in A} z_e$. The Hamming weight enumerator is denoted and defined by

$$\begin{aligned} W(C;\mathbf{w},\mathbf{z}) &= \textstyle\sum_{c\in C} \mathbf{w}^{\overline{\mathrm{supp}(c)}}\mathbf{z}^{\mathrm{supp}(c)} \\ &= \textstyle\sum_{A\subseteq E} n_C(A)\mathbf{w}^{\overline{A}}\mathbf{z}^A, \end{aligned} \tag{64}$$

where $n_C(A) = |\{c \in C : \mathrm{supp}(c) = A\}|$.

Note that we have specialized (56) by setting $\mathbf{w}^c = \mathbf{w}^{\overline{\mathrm{supp}(c)}}$ and $\mathbf{z}^c = \mathbf{z}^{\mathrm{supp}(c)}$. This generating function tells us precisely how many codewords have support equalling A for each $A \subseteq E$. The finite ring condition guarantees that each $n_C(A)$ is finite.

We will always say that such a code is with the lattice $\mathbf{L}^E = \prod_{e\in E} L_e$, where for each $e \in E$, L_e is the two element lattice $\{0, M_e\}$. Thus we may identify $\mathbf{L}^E$ with the Boolean lattice 2^E via an isomorphism $\alpha : 2^E \to \mathbf{L}^E$, where for $A \subseteq E$, $\alpha(A) = \bigoplus_{e\in A} M_e = \prod_{e\in A} M_e = \mathbf{M}^A \leq \mathbf{M}^E$. Hence, in what follows we will often write A instead of $\alpha(A) = \mathbf{M}^A$ and e instead of $\{e\}$, M_e or $\mathbf{M}^{\{e\}}$.

The Boolean lattice 2^E is self-dual, and $A^\perp$ is simply $\overline{A}$.

The length $\|\cdot\|$ is defined on all elements of $\mathcal{L}(\mathbf{M}^E)$ as in the discussion preceding Proposition 4.1, and we define $\|\cdot\|$ on elements of $2^E \cong \mathbf{L}^E \leq \mathcal{L}(\mathbf{M}^E)$ in the natural way. That is, $\|e\| = \|M_e\|$ and $\|A\| = \left\|\mathbf{M}^A\right\| = \sum_{e\in A} \|e\|$.

Define and denote the following vectors of all 1's:

$$\begin{aligned} \mathbf{1} &= (1 : i \in [k]), \\ \breve{\mathbf{1}} &= (1 : e \in E). \end{aligned} \tag{65}$$

Theorem 9.4 holds for all finite rings, does not involve duality and exemplifies the vertical arrows in (61).

We show how Theorem 9.4 generalizes (17) in Corollary 9.7.

9.4. **Theorem.** *Let S be a finite ring and let $\mathbf{s}$ be the vector described following Definition 9.1. For a code $C \leq \mathbf{M}^E$ in $\mathfrak{F}_S$, with lattice $\mathbf{L}^E \cong 2^E$, as specified above*

$$W(C;\mathbf{w},\mathbf{z}) = R(\rho_C, \|\cdot\|, 2^E; \mathbf{z}, \mathbf{w}-\mathbf{z}, \mathbf{1}, \mathbf{s}). \tag{66}$$

The same holds in ${}_R\mathfrak{F}$, for R finite, with an appropriate $\mathbf{s}$.

Proof. By (26) we have $\rho_C(A) = \left\|\mathbf{M}^A\right\| - \left\|\mathbf{M}^A \cap C\right\|$ so

$$\begin{aligned} \left\|\mathbf{M}^A \cap C\right\| &= \|A\| - \rho_C(A) \text{ and} \\ |\mathbf{M}^A \cap C| &= \mathbf{s}^{\left\|\mathbf{M}^A\cap C\right\|} = \mathbf{s}^{\|A\|-\rho_C(A)}. \end{aligned} \tag{67}$$

Let $N_C(A) = \{c \in C : \mathrm{supp}(c) = A\}$, so $n_C(A) = |N_C(A)|$ and $(N_C(A) : A \subseteq E)$ is a partition of C. Therefore since $\mathbf{M}^A \cap C = \{c \in C : \mathrm{supp}(c) \subseteq A\}$, we have

$$|\mathbf{M}^A \cap C| = \sum_{B\subseteq A} n_C(B). \tag{68}$$

By the inclusion-exclusion principle, which is Möbius inversion for the Boolean lattice, [19] Section 15.2, we obtain

$$n_C(A) = \sum_{B\subseteq A} (-1)^{|A|-|B|}|\mathbf{M}^B \cap C| = \sum_{B\subseteq A} (-1)^{|A|-|B|}\mathbf{s}^{\|B\|-\rho_C(B)} \tag{69}$$

and by (64)

$$\begin{aligned} W(C;\mathbf{w},\mathbf{z}) &= \sum_{A\subseteq E}\sum_{B\subseteq A} (-1)^{|A|-|B|}\mathbf{s}^{\|B\|-\rho_C(B)}\mathbf{w}^{\overline{A}}\mathbf{z}^A \\ &= \sum_{B\subseteq E} \mathbf{s}^{\|B\|-\rho_C(B)} \sum_{\substack{A\\ B\subseteq A\subseteq E}} (-1)^{|A|-|B|}\mathbf{w}^{\overline{A}}\mathbf{z}^A \\ &= \sum_{B\subseteq E} \mathbf{s}^{\|B\|-\rho_C(B)}\mathbf{z}^B(\mathbf{w}-\mathbf{z})^{\overline{B}} \\ &= R(\rho_C, \|\cdot\|, 2^E; \mathbf{z}, \mathbf{w}-\mathbf{z}, \mathbf{1}, \mathbf{s}) \text{ by (54).} \end{aligned} \tag{70}$$

One can verify that $\mathbf{z}^B(\mathbf{w}-\mathbf{z})^{\overline{B}} = \sum_{\substack{A\\ B\subseteq A\subseteq E}} (-1)^{|A|-|B|}\mathbf{w}^{\overline{A}}\mathbf{z}^A$ for every $B \subseteq E$ by expanding the product $\mathbf{z}^B(\mathbf{w}-\mathbf{z})^{\overline{B}}$ and collecting the monomials. □

One may regard (69) as a generalization of (a dual of) the Critical Theorem [6]. Along those lines we also observe that

$$n_C(E) = R(\rho_C, \|\cdot\|, 2^E; \breve{\mathbf{1}}, -\breve{\mathbf{1}}, \mathbf{1}, \mathbf{s}). \tag{71}$$

Some identities for TW-functions are found by 'scaling' the variables. For a grounded $\mathbb{Z}^k$-latroid with lattice 2^E and variables $\mathbf{u} = (u_e : e \in E)$, $\mathbf{v} = (v_e : e \in E)$, $\mathbf{x} = (x_i : i \in [k])$, $\mathbf{y} = (y_i : i \in [k])$, one obvious scaling is, with any vector of commuting variables $\mathbf{r} = (r_e : e \in E)$,

$$R(\rho, \|\cdot\|, 2^E; \mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}) = (\mathbf{r}^E)^{-1}R(\rho, \|\cdot\|, 2^E; \mathbf{r}u, \mathbf{r}v, \mathbf{x}, \mathbf{y}), \tag{72}$$

since for every $A \subseteq E$, $(\mathbf{r}^E)^{-1}\mathbf{r}^A\mathbf{r}^{\overline{A}} = 1$. Here and below, we use conventions such as

$$\mathbf{ru} = (r_e u_e : e \in E) \text{ and } \mathbf{r}^{-1} = (r_e^{-1} : e \in E). \tag{73}$$

We may similarly note that for a code C on the ground set E,

$$W(C;\mathbf{w},\mathbf{z}) = (\mathbf{r}^E)^{-1}W(C;\mathbf{r}w,\mathbf{r}z). \tag{74}$$

Now suppose we have some vector of commuting variables $\mathbf{t} = (t_i : i \in [k])$. Define the vector

$$\breve{\mathbf{t}} = (\breve{t}_e : e \in E) \text{ where } \breve{t}_e = \mathbf{t}^{\|e\|}. \tag{75}$$

This notation is consistent with (65). The length axioms of Definition 5.4 easily imply that

$$\|A\| = \sum_{e\in A} \|e\| \tag{76}$$

so that

$$\mathbf{t}^{\|A\|} = \prod_{e\in A} \mathbf{t}^{\|e\|} = \prod_{e\in A} \breve{t}_e = \breve{\mathbf{t}}^A. \tag{77}$$

Note that $\breve{\mathbf{t}}$ depends on both $\mathbf{t}$ and $\|\cdot\| : 2^E \to \mathbb{Z}^k$, but nothing else. Here is another not quite so obvious scaling of the variables.

9.5. **Lemma.**

$$R(\rho, \|\cdot\|, 2^E; \mathbf{u}, \mathbf{v}, \mathbf{tx}, \mathbf{t}^{-1}\mathbf{y}) = \mathbf{t}^{\rho(E)-\|E\|} R(\rho, \|\cdot\|, 2^E; \mathbf{u}, \breve{\mathbf{t}}\mathbf{v}, \mathbf{x}, \mathbf{y}). \tag{78}$$

Proof. The left-hand side equals

$$\sum_{A \subseteq E} \mathbf{u}^A \mathbf{v}^{\overline{A}} \mathbf{x}^{\rho(E)-\rho(A)} \mathbf{y}^{\|A\|-\rho(A)} \mathbf{t}^{\rho(E)-\rho(A)-(\|A\|-\rho(A))}. \tag{79}$$

The $\rho(A)$'s in the exponent of $\mathbf{t}$ cancel, and this is the crucial point that makes this work. By (77), $\mathbf{t}^{\|A\|} = \breve{\mathbf{t}}^A$. The constant term $\mathbf{t}^{\rho(E)}$ can be brought outside the summation. Finally $\mathbf{v}^{\overline{A}} \left(\breve{\mathbf{t}}^A\right)^{-1} = \left(\breve{\mathbf{t}}\mathbf{v}\right)^{\overline{A}} \left(\breve{\mathbf{t}}^E\right)^{-1} = \left(\breve{\mathbf{t}}\mathbf{v}\right)^{\overline{A}} \left(\mathbf{t}^{\|E\|}\right)^{-1}$. This gives the right-hand side. □

We are ready to prove a vE MacWilliams identity for the Hamming weight enumerator as defined in Definition 9.3. This works only for a code duality arising from an *equicardinal* Morita duality, since we use Theorem 9.4 applied to both a code C and its code-dual $C^\perp$ and we must have the *same* $\mathbf{s}$ in both cases. This theorem exemplifies the lower horizontal arrow in (61) and it generalizes (18), as shown in Corollary 9.7.

9.6. **Theorem.** *Let* ${}^* : \mathfrak{F}_S \rightleftharpoons {}_R\mathfrak{F}$ *be an equicardinal Morita duality, so* R *and* S *are finite rings. Let* $\mathbf{s}$ *be the vector described following Definition 9.1. Let* $C \leq \mathbf{M}^E$ *be a code with ground set* E *and lattice* $\mathbf{L}^E \cong 2^E$ *as above. Define* $\breve{\mathbf{s}} = (\breve{s}_e : e \in E)$ *where* $\breve{s}_e = \mathbf{s}^{\|e\|}$*, noting that* $\breve{\mathbf{s}}$ *depends only on* $\mathbf{M}^E$*. Then*

$$W(C^\perp; \mathbf{w}, \mathbf{z}) = \mathbf{s}^{\rho_C(E)-\|E\|} W(C; \mathbf{w} - \mathbf{z} + \breve{\mathbf{s}}\mathbf{z}, \mathbf{w} - \mathbf{z}). \tag{80}$$

Proof. By Theorem 9.4 the left-hand side equals $R(\rho_{C^\perp}; \mathbf{z}, \mathbf{w}-\mathbf{z}, \mathbf{1}, \mathbf{s})$. By Theorem 8.4 and Lemma 6.2(ii) this equals $R(\rho_C; \mathbf{w} - \mathbf{z}, \mathbf{z}, \mathbf{s}, \mathbf{1})$.

Applying Lemma 9.5, with $\mathbf{t} = \mathbf{s}$, $(\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}) = (\mathbf{w} - \mathbf{z}, \mathbf{z}, \mathbf{1}, \mathbf{s})$ and $\rho = \rho_C$, gives $\mathbf{s}^{\rho_C(E)-\|E\|} R(\rho_C; \mathbf{w} - \mathbf{z}, \breve{\mathbf{s}}\mathbf{z}, \mathbf{1}, \mathbf{s})$.

Applying Theorem 9.4 again gives the right-hand side, as required. □

9.7. **Corollary.** *Equations* (16)*,* (17) *and* (18) *hold.*

Proof. Note that (16) is equivalent to (17) using (13).

Let C be a code over a finite field K on the ground set E. In this special case we have the Morita duality given by the bimodule ${}_RU_S$, where $U = R = S = K$, for a finite field of size $|K| = q$. The length $\|\cdot\|$ takes values in $\mathbb{A} = \mathbb{Z}$, so that $k = 1$, since a 1-dimensional vector space is the only simple K-module up to isomorphism. Recall the discussion preceding Theorem 9.4, where we identify the Boolean lattice 2^E with a sublattice of $\mathcal{L}(K^E)$, and $\|\cdot\|$ on 2^E is inherited from $\|\cdot\|$ on $\mathcal{L}(K^E)$. So for a vector space $V \in \mathcal{L}(K^E)$ we have $\|V\| = \dim(V)$, whereas for a set $A \in 2^E$ we have $\|A\| = |A|$.

Note that, by (26) with $l = K^E$,

$$\rho_C(E) = |E| - \dim(C). \tag{81}$$

Recall $\breve{\mathbf{1}} = (1 : e \in E)$. Set $\mathbf{s} = q = |K|$, so that $\breve{\mathbf{s}} = q\breve{\mathbf{1}}$. Set $(\mathbf{w}, \mathbf{z}) = (\breve{\mathbf{1}}, z\breve{\mathbf{1}})$, so that $\mathbf{w}^{\overline{A}}\mathbf{z}^A = z^{|A|}$.

This identifies the left-hand sides of (17) and (66), while the right-hand side of (66) may be written as $R(\rho_C; z\breve{\mathbf{1}}, (1-z)\breve{\mathbf{1}}, 1, q)$. Now rescale this using (78) with $\mathbf{t} = z/(1-z)$, so that $\breve{\mathbf{t}} = (z/(1-z))\breve{\mathbf{1}}$, to yield

$$(z/(1-z))^{\rho_C(E)-|E|} R(\rho_C; z\breve{\mathbf{1}}, z\breve{\mathbf{1}}, (1-z)/z, qz/(1-z)). \tag{82}$$

Then rescale this using (72) with $\mathbf{r} = z^{-1}\breve{\mathbf{1}}$ to yield

$$z^{\rho_C(E)}(1-z)^{|E|-\rho_C(E)}R(\rho_C; \breve{\mathbf{1}}, \breve{\mathbf{1}}, (1-z)/z, qz/(1-z)), \tag{83}$$

which equals the right-hand side of (17).

Using the above values of $\mathbf{w}$, $\mathbf{z}$, $\breve{\mathbf{s}}$ in (80), and then applying (74) with $\mathbf{r} = (1+(q-1)z)^{-1}\breve{\mathbf{1}}$, yields (18). □

We briefly discuss the sense in which the equicardinality assumption is necessary, although we refrain from giving a rigorous formulation of this necessity.

Note that, in terms of information contained in generating functions, the Hamming weight enumerator $W(C)$ of Definition 9.3 is a specialization of the TW-function $R(C)$ of Definition 8.2, obtained by setting $\mathbf{xy} = \mathbf{s}$, by which we mean $x_i y_i = s_i$ for every $i \in [k]$. Note that in the scaling equations (72), (78), and the duality equation (60), all the changes of variables preserve the condition that $\mathbf{xy} = \mathbf{s}$.

If $\mathbf{s} = \mathbf{s}^*$, then $W(C^\perp)$ is also obtained by specializing to $\mathbf{xy} = \mathbf{s}$, which is why we can obtain (80). However, if $\mathbf{s} \neq \mathbf{s}^*$, then $W(C^\perp)$ would be obtained by specializing to $\mathbf{xy} = \mathbf{s}^* \neq \mathbf{s}$ and there is no reason to expect that one specialization would determine the other, in general.

On the positive side, the MacWilliams identity (60) holds in full generality for all Morita dualities, and the TW-functions on each side each contain, in the finite ring case, the Hamming weight enumerator $W(C)$ of Definition 9.3 as a special case, if not as dual specializations. On the other hand, it must be conceded that some vE enumerators are not specializations of TW-functions, so we do not get immediate corollaries about these.

10. Related results

In this section we briefly survey some other results [10, 22] to place our work in context. We will comment on two types of Morita duality which we call *character duality* and *classical duality*.

Here is a list of relevant classes of rings each properly containing the next which are defined in [22].

(i) Finite rings
(ii) Finite Quasi-Frobenius rings
(iii) Finite Frobenius rings
(iv) Finite weakly symmetric rings
(v) Finite symmetric rings
(vi) Finite fields

For commutative rings, (ii), (iii) and (iv) coincide. The standard theory of linear codes is done over finite fields. The extension to finite rings is more recent. In such generalizations it would seem natural to define duality analogously to (1), with appropriate care for the non-commutative case. This leads to the *classical duality*, defined later, a duality which is not defined for all finite rings.

We first consider *character duality* [15], which is arguably more natural, and which is defined for all finite rings. These two dualities are equivalent for fields, so the distinction is not apparent in that case.

For a finite abelian group M, written additively, the character group $\widehat{M} = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$, where for $\pi_1, \pi_2 \in \widehat{M}$, $\pi_1, \pi_2 : M \to \mathbb{Q}/\mathbb{Z}$, $x \in M$, we have

$(\pi_1 + \pi_2)(x) = \pi_1(x) + \pi_2(x)$. Actually, Wood and many others write $\widehat{M}$ as a multiplicative group via the map $p \in \mathbb{Q}/\mathbb{Z} \mapsto e^{2\pi ip}$ to the complex roots of unity, but one can easily convert between these presentations.

If M is a left (resp. right) R-module, then $\widehat{M}$ is a right (resp. left) R-module via $(\pi r)(x) = \pi(rx)$ (resp. $(r\pi)(x) = \pi(xr)$) for $\pi \in \widehat{M}$, $r \in R$, $x \in M$. We call the duality $^* : \mathfrak{F}_R \rightleftharpoons {}_R\mathfrak{F}$, where $M^* = \widehat{M}$, the *character duality*. From [22] and a simple observation here, we have the following.

10.1. **Theorem.** *For any finite ring R, the functor $^* : \mathfrak{F}_R \rightleftharpoons {}_R\mathfrak{F}$, where $M^* = \widehat{M}$, is a Morita duality and it is determined by the bimodule ${}_R\widehat{R}_R$. Moreover $*$ is an equicardinal Morita duality.*

Proof. The first sentence is proved in [22]. Since, for any finite Abelian group, $\widehat{M} \cong M$ as an Abelian group, so that $|\widehat{M}| = |M|$, the character duality is an equicardinal Morita duality. □

So the results of Section 9 hold for all finite rings provided we use character duality. But in fact, for character duality, a completely general MacWilliams identity follows from standard character theory.

We give a brief presentation. First note that $\widehat{M} = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$ can be identified with $M^* = \mathrm{Hom}(M, {}_R\widehat{R}_R)$ in a natural way; see [22]. It is convenient for us to use the former of these. For $c \in C$ and $\gamma \in \widehat{M}$ we define $\langle c, \gamma\rangle = \gamma(c) \in \mathbb{Q}/\mathbb{Z}$, and we note that $e^{2\pi i\langle x,\gamma\rangle}$ is well defined. For a right (left) R-submodule $C \leq M$ define a left (right) R-module

$$C^\perp = \{\gamma \in \widehat{M} : \langle c, \gamma\rangle = 0 \text{ for all } c \in C\}. \tag{84}$$

Setting $\mathbf{w} = \mathbf{1}$ or $\mathbf{z} = \mathbf{1}$ in Definition 8.3, the complete weight enumerators of C and $C^\perp$ are

$$W(C; \mathbf{z}) = \sum_{c\in C} \mathbf{z}^c \text{ and } W(C^\perp; \mathbf{w}) = \sum_{\gamma\in C^\perp} \mathbf{w}^\gamma \tag{85}$$

where the $\mathbf{z}^c$'s and $\mathbf{z}^\gamma$'s are regarded as independent variables unless conditions are imposed to relate them. Then, using only Abelian group structure and using identities in [15], a general MacWilliams identity for the character dual is

$$W(C; \mathbf{z}) = \frac{1}{|C^\perp|} W(C^\perp; \mathbf{w}) \text{ where } \mathbf{w}^\gamma = \sum_{x\in M} e^{2\pi i\langle x,\gamma\rangle}\mathbf{z}^x. \tag{86}$$

Many identities can be deduced from this with some extra work. Formulas can also be derived when $M = \mathbf{M}^E$, using a product formula in [22].

Now we discuss the classical duality. If C is a right R-submodule of R^E, define

$$C^\perp = \left\{y \in R^E : y \cdot x = 0 \text{ for all } x \in C\right\}, \tag{87}$$

which is a left R-submodule of R^E.

If C is a left R-submodule of R^E, define

$$C^\perp = \left\{y \in R^E : x \cdot y = 0 \text{ for all } x \in C\right\}, \tag{88}$$

which is a right R-submodule of R^E.

We assume we know from the context whether C is considered to be a left or right R-module. It is not true in general that $C^{\perp\perp} = C$. The case $|E| = 1$ corresponds to left and right ideals of R. This definition of $\perp$-dual is essentially that given by

(44) arising from the Morita duality determined by the bimodule ${}_RR_R$, *for those rings* R such that ${}_RR_R$ does indeed determine a Morita duality. This prompts the following which can be deduced using [22].

10.2. **Theorem.** *Let R be a finite ring. The following are equivalent.*

(i) *R is Quasi-Frobenius.*
(ii) *${}_RR_R$ determines a Morita duality.*
(iii) *$C^{\perp\perp} = C$, as defined in* (87),(88) *for every left-submodule of R^E, E finite.*
(iv) *$I^{\perp\perp} = I$, as defined in* (87),(88) *for every left ideal of R.*
(iii′) *$C^{\perp\perp} = C$, as defined in* (87),(88) *for every right-submodule of R^E, E finite.*
(iv′) *$I^{\perp\perp} = I$, as defined in* (87),(88) *for every right ideal of R.*

We call the Morita duality determined by the bimodule ${}_RR_R$ the *classical duality*. It is defined precisely for QF-rings. However some results in [10, 22] require further restriction to Frobenius rings. Combining results of [10, 22] and inserting an easy equivalence ((ii) below) we get the following. Here the $\perp$-dual is as in (44) for the contravariant functor ${}^* : \mathfrak{F}_R \rightleftharpoons {}_R\mathfrak{F}$ defined by ${}_RR_R$.

10.3. **Theorem.** *Let R be a finite ring. The following are equivalent.*

(i) *R is Frobenius.*
(ii) *${}_RR_R$ determines an equicardinal Morita duality.*
(iii) *As left R-modules, ${}_R\widehat{R} \cong {}_RR$.*
(iv) *For every $C \leq M \in {}_R\mathfrak{F}$, $|M| = |C||C^{\perp}|$.*
(v) *For every left ideal I of R, $|R| = |I||I^{\perp}|$.*
(iii′) *As right R-modules, $\widehat{R}_R \cong R_R$.*
(iv′) *For every $C \leq M \in \mathfrak{F}_R$, $|M| = |C||C^{\perp}|$.*
(v′) *For every right ideal I of R, $|R| = |I||I^{\perp}|$.*

So although the classical duality is defined for QF-rings, it is equicardinal if and only if R is Frobenius and many results in [10, 22] and this paper seem to need this restriction.

Actually, for classical duality, in the equicardinal case, Wood [22] gives a MacWilliams identity that resembles (86) and again is more general (more variables) than Theorem 9.6 for *this* duality. The resemblance is because ${}_RR \cong {}_R\widehat{R}$, but they are not the same since it need not be true that ${}_RR_R \cong {}_R\widehat{R}_R$ as bimodules. For completeness we note the following [22].

10.4. **Theorem.** *Let R be a finite ring. The following are equivalent*

(i) *R is a symmetric ring.*
(ii) *${}_RR_R$ and ${}_R\widehat{R}_R$ determine the same Morita duality.*
(iii) *${}_RR_R \cong {}_R\widehat{R}_R$ as bimodules.*

So for finite fields the two dualities mentioned are the same.

The results of Section 9 work for all equicardinal Morita dualities, but apart from two types of examples in this section, we do not say which such dualities exist. For the two types of equicardinal Morita duality in this section, it seems that stronger MacWilliams identities (more variables) than those in Section 9 hold. This suggests some questions.

1. What equicardinal Morita dualities are there?
2. What are the most general MacWilliams identities for each of these?

3. Can anything be salvaged from the non-equicardinal case?

Once again, however, we emphasize that these problems only arise for vE enumerators, and that (60) is completely general for vS enumerators.

We also mention that we hope for this paper to lay the foundation for the expansion of the subject of matroid representation theory. There is far more to this topic than enumerators and identities.

Acknowledgements

The author thanks Jilyana Cazaran and Keisuke Shiromoto for useful discussions while Keisuke Shiromoto visited Louisiana State University in early 2000.

The author especially thanks Jilyana Cazaran for many discussions about algebra, and for familiarizing the author with the literature.

References

[1] Frank W. Anderson and Kent R. Fuller, *Rings and categories of modules*, Graduate Texts in Mathematics, vol. 13, Springer-Verlag, New York, 1974, MR **54:**5281

[2] T. S. Blyth, *Module theory. An approach to linear algebra*, second ed., The Clarendon Press Oxford University Press, New York, 1990, MR **91i:**16001

[3] Thomas H. Brylawski, *A decomposition for combinatorial geometries*, Trans. Amer. Math. Soc. **171** (1972), 235–282, MR **46:**8869

[4] Jilyana Cazaran, Keisuke Shiromoto, Thomas Britz, and Carrie Rutherford, 1999–2002, Independent Private Communication.

[5] Henry H. Crapo, *The Tutte polynomial*, Aequationes Math. **3** (1969), 211–229, MR **41:**6705

[6] Henry H. Crapo and Gian-Carlo Rota, *On the foundations of combinatorial theory: Combinatorial geometries*, The M.I.T. Press, Cambridge, Mass.-London, 1970, MR **45:**74

[7] T. A. Dowling, *Codes, packings and the critical problem*, Atti del Convegno di Geometria Combinatoria e sue Applicazioni (Univ. Perugia, Perugia, 1970), Ist. Mat., Univ. Perugia, Perugia, 1971, pp. 209–224. MR **49:**2438

[8] Curtis Greene, *Weight enumeration and the geometry of linear codes*, Studies in Appl. Math. **55** (1976), no. 2, 119–128, MR **56:**5335

[9] A. Roger Hammons, Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and Patrick Solé, *The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319, MR **95k:**94030

[10] Thomas Honold, *Characterization of finite Frobenius rings*, Arch. Math. (Basel) **76** (2001), no. 6, 406–415, MR **2002b:**16033

[11] A. S. Kuz′min, V. L. Kurakin, V. T. Markov, A. V. Mikhalev, and A. A. Nechaev, *Codes and recurrences over finite rings and modules (Russian)*, Vestnik Moskov. Univ. Ser. I Mat. Mekh. (1999), no. 5, 18–31, 80. translation in Moscow Univ. Math. Bull. **54** (1999), no. 5, 15–28 (2000), MR **2001g:**94018

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

[13] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes I, II*, North-Holland Mathematical Library, vol. 16, North-Holland Publishing Co., Amsterdam, 1977, MR **57:**5408a

[14] A. A. Nechaev, *Kerdock's code in cyclic form (Russian)*, Diskret. Mat. **1** (1989), no. 4, 123–139, translation in Discrete Math. Appl. **1** (1991), no. 4, 365–384, MR **91a:**94038

[15] L. Pontryagin, *Topological Groups*, Princeton University Press, Princeton, 1939, MR **1:**44e

[16] Charles Semple and Geoff Whittle, *Partial fields and matroid representation*, Adv. in Appl. Math. **17** (1996), no. 2, 184–208, MR **97g:**05046

[17] Anne Penfold Street and W. D. Wallis, *Combinatorial theory: an introduction*, Charles Babbage Research Centre, Winnipeg, Man., 1977, MR **56:**2831

[18] W. T. Tutte, *A ring in graph theory*, Proc. Cambridge Philos. Soc. **43** (1947), 26–40, MR **8:**284k

[19] D. J. A. Welsh, *Matroid theory*, London Math. Soc. Monographs, vol. 8, Academic Press [Harcourt Brace Jovanovich Publishers], London, 1976, MR **55:**148

[20] Geoff Whittle, *A characterisation of the matroids representable over $GF(3)$ and the rationals*, J. Combin. Theory Ser. B **65** (1995), no. 2, 222–261, MR **96m:**05046

[21] ———, *On matroids representable over $GF(3)$ and other fields*, Trans. Amer. Math. Soc. **349** (1997), no. 2, 579–603, MR **97g:**05047

[22] Jay A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575, MR **2001d:**94033

Department of Mathematics, Louisiana State University, Baton Rouge, Louisiana 70803-4918

E-mail address: vertigan@math.lsu.edu