ON LINEAR ORDERED CODES

ALEXANDER BARG* AND WOOMYOUNG PARK†

ABSTRACT. We consider linear codes in the metric space with the Niederreiter-Rosenbloom-Tsfasman (NRT) metric, calling them linear ordered codes. In the first part of the paper we examine a linear-algebraic perspective of linear ordered codes, focusing on the distribution of "shapes" of codevectors. We define a multivariate Tutte polynomial of the linear code and prove a duality relation for the Tutte polynomial of the code and its dual code. We further relate the Tutte polynomial to the distribution of support shapes of linear ordered codes, and find this distribution for ordered MDS codes. Using these results as a motivation, we consider ordered matroids defined for the NRT poset and establish basic properties of their Tutte polynomials. We also discuss connections of linear ordered codes with simple models of information transmission channels.

1. INTRODUCTION

Among many aspects of the theory of linear codes, some of the main questions include studies related to their weight distributions, transmission and decoding over symmetric channels, and associated applications to such classic information-theoretic problems as the wire-tap channel. In this paper we study this range of questions for codes in a metric space with distance derived from a partial order of coordinates.

1-A. **The ordered Hamming space.** Metrics on partially ordered Hamming-like spaces have been studied in the literature for close to two decades following their introduction by Brualdi et al. [10]. Here we focus on one such metric which we proceed to define. Let E be a finite set of cardinality $N = nr$. Below we always assume that E is written in the form

$$E = \big\{\{1,\dots,r\},\{r+1,\dots,2r\},\dots,\{(n-1)r+1,\dots,nr\}\big\}. \tag{1}$$

Definition 1. *Define a partial order P on E such that each of the r-blocks in* (1) *forms a linearly ordered set (a chain) and elements in different chains are incomparable:*

$$i \prec j \quad \Longleftrightarrow \quad \big(\exists_{k\in\{1,2,\dots,n\}} : i,j \in \{(k-1)r+1,\dots,kr\}\big) \wedge (i<j). \tag{2}$$

An *order ideal* of the poset (E,P) is a subset $I \subset E$ such that if $i \in I$ and $j \prec i$ then $j \in I$. The set of all ideals of P will be denoted by $\mathcal{I}(P)$. For a subset $A \subset E$ let $\langle A\rangle = \cap_{I\supset A} I$ be the smallest-size ideal of P that contains A.

Let $\mathbb{F}_q^N$ be an N-dimensional vector space over a finite field $\mathbb{F}_q$. For a vector $x \in \mathbb{F}_q^N$ define its support $\mathrm{supp}(x) := \{i \in E : x_i \neq 0\}$. Define the weight of x as follows:

$$w_P(x) = |\langle \mathrm{supp}(x)\rangle|. \tag{3}$$

By d_P we denote the distance on $\mathbb{F}_q^N$ derived from w_P. Note that the case $r = 1$ corresponds a single antichain, and the associated weight w_P is the usual Hamming norm. The case $n = 1$ corresponds to a single chain, and the weight $w_P(x)$ is simply the location of the rightmost nonzero entry in x.

The norm w_P was defined by Niederreiter [27, 28] in relation to constructions of uniformly distributed points in the cube and approximate evaluation of integrals. The distance d_P was independently defined by Rosenbloom and Tsfasman [35] for a particular generalization of Reed-Solomon (RS) codes[1], so we refer to the order (2) as the NRT order, and call

Date: June 26, 2015.

The results of this paper were presented in part at the 2010 Allerton Conference on Communication, Control and Computing and 2010 IEEE International Symposium on Information Theory [33, 34].

* Dept. of Electrical and Computer Engineering and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA, and Institute for Problems of Information Transmission, Russian Academy of Sciences, Moscow, Russia. Email: abarg@umd.edu. This research is supported in part by NSF grants CCF1217894, CCF0916919.

† Samsung Electronics, Suwon, Gyeonggi-do, Korea. Research done while at Department of ECE and Institute for Systems Research, University of Maryland, College Park, MD. Research supported by NSF grant CCF0916919.

[1]The concepts from coding theory used in this paper are found for instance the textbooks of MacWilliams and Sloane [24] or Tsfasman et al. [39].

the pair (E, P) the NRT poset. We also call the metric space $(\mathbb{F}_q^N, d_P)$ the *ordered Hamming space* and speak of the ordered weight, ordered distance, etc.

The authors of [35] remarked that this metric models transmission over a set of parallel channels subject to fading. The same model was independently introduced to describe the noise process in a wireless fading system in [38], see also [17]. Independently of these works, the norm w_P was used in [26] to study linear complexity of sequences, and in [29] for the analysis of a list decoding algorithm of a class of algebraic codes. In [25] the authors constructed the association scheme arising from the partition of the space $\mathbb{F}_q^n$ induced by the NRT order. This scheme was further studied in [4, 3] and its extension to infinite spaces was recently investigated in [6]. MacWilliams identities for linear codes in the ordered Hamming space were derived in [13]. Maximum distance separable (MDS) codes in this space were studied in [36] and near-MDS codes were considered in [5]. Currently poset metrics, and in particular the ordered Hamming distance form the subject of a large body of combinatorial literature.

1-B. **Linear codes in the Hamming space.** To motivate our study, we briefly recall several well-known facts about linear codes in the Hamming space [24]. Let $\mathcal{C}$ be a linear code of length N, i.e., a linear subspace of $\mathbb{F}_q^N$. The dual code $\mathcal{C}^\perp$ is defined as the set $\{x \in \mathbb{F}_q^N : \forall_{y\in\mathcal{C}} \langle x, y\rangle = 0\}$ where $\langle\cdot,\cdot\rangle$ denotes the dot product. The Hamming weight of a vector $x \in \mathbb{F}_q^N$ is the number of nonzero coordinates in it. One of the main parameters of the code $\mathcal{C} \in \mathbb{F}_q^N$ is the distribution of Hamming weights of its vectors. A classical theorem of MacWilliams connects this distribution with the weight distribution of the dual code $\mathcal{C}^\perp$. This result has a number of far-reaching consequences in coding theory [24]. Hamming weights are fundamental for the study of linear codes because the weight of the vector is invariant under the action of the group of linear automorphisms of the Hamming space. Hamming weights are also related to the distribution of ranks of subspaces of the code $\mathcal{C}$, and both are incorporated in the definition of the Tutte polynomial (an invariant of the matroid represented by the code); see Greene's well-known paper [18]. They are also used to characterize the performance (error probability of decoding) when the code is used to transmit information over a memoryless symmetric channel.

The notion of the Hamming weight can be extended to *generalized Hamming weights*. Following [41], define the support of a linear subcode $\mathcal{B} \subset \mathcal{C}$ as $\mathrm{supp}(\mathcal{B}) := \{i \in \{1,\dots,N\} : \exists_{x\in\mathcal{B}}\, x_i \neq 0\}$. The sth generalized Hamming weight (sth *higher weight*) of the code $\mathcal{C}$ is defined as $d_s = \min_{\mathcal{B}\subset\mathcal{C}:\dim(\mathcal{B})=s} |\mathrm{supp}(\mathcal{B})|, s = 1,\dots,\dim(\mathcal{C})$. While the original motivation to study higher weights of linear codes came from cryptography [41] (see Sect. 4-B), a geometric approach to their study was developed in [40].

1-C. **Contributions of this paper.** In this paper we make several contributions to the study of linear ordered codes by which we mean linear subspaces of the ordered Hamming space. While [35] emphasized the notion of the weight $w_P(x)$, we argue that the more fundamental parameter of the vector $x \in \mathcal{C}$ is a vector of r integers which we call the *shape* of x. The notion of shapes [4, 3] is justified by considering invariants of the group of linear automorphisms of the space $\mathbb{F}^N$. This prompts us to define a multivariate Tutte polynomial of the code, which enters a natural duality condition that extends Greene's results to the ordered case. Multivariate Tutte polynomials were previously studied in [37], and we make a connection of our Tutte polynomial with the results of that paper. For the case of the NRT poset, these results also give an answer to the question of defining the Tutte polynomials for ordered matroids that has been raised in several earlier papers, e.g., [8]. Finally, they also yield a linear-algebraic proof of the MacWilliams theorem for linear ordered codes proved by other means in [25, 13].

The line of thought that yields the described results is also connected to an extension of the so-called binomial moments of the distance distribution of linear codes. In the case of the Hamming metric binomial moments were used to derive weight distributions of codes on elliptic curves [22], to prove bounds for error events for transmission with codes over discrete symmetric channels [1], and to characterize energy-minimizing error-correcting codes [11].

We further extend these considerations to higher ordered weights introduced in [5] in analogy to the classic case. In particular, we relate the distribution of support weights of an ordered code to the multivariate Tutte polynomial, extending the result of [2]. We also find the distribution of support weights for ordered maximum distance separable (MDS) codes.

Finally, we briefly comment on the connection of linear ordered codes with information transmission. We define a probabilistic channel model in which the error events are controlled by shapes of the transmitted vectors. We also establish a relation of higher poset weights of linear codes to the ordered *wiretap channel*, which extends the well-known Wyner's model of the combinatorial wiretap channel [31] to the ordered case.

Overall this group of results connects linear ordered codes with the main problems of information transmission over noisy channels. It could be argued that these studies should be performed in a more general situation, for instance, for some class of posets; however, [3] contains evidence that such an extension is a difficult question.

2. Linear Ordered Codes

2-A. **Definitions.** Below $\mathbb{F}_q^N$ is the ordered Hamming space.

Definition 2. *Let $x \in \mathbb{F}_q^N$ be a vector written as $x = (x^{(1)}, x^{(2)}, \dots, x^{(n)})$, where $x^{(i)} := (x_{i,1}, \dots, x_{i,r}), i = 1, \dots, n$ (cf.* (1)*). The* shape *of x with respect to P is an r-vector $e = (e_1, e_2, \dots, e_r)$, where*

$$e_j = |\{i : 1 \le i \le n, w_P(x^{(i)}) = j\}|, \quad j = 1, \dots, n.$$

Below we use the notation $|e| := \sum_{i=1}^n e_i$, $e_0 := n - |e|$.

For instance, if $r = 3, n = 5$, then $e := \mathrm{shape}(010, 101, 110, 100, 000) = (1, 2, 1), |e| = 4, e_0 = 1$. This definition extends in an obvious way to the shape of an ideal $I \in \mathcal{I}(P)$, and we use the same notation $\mathrm{shape}(I)$ to refer to the shape of I. Thus, $\mathrm{shape}(x) = \mathrm{shape}(\langle \mathrm{supp}(x) \rangle)$. A shape vector e defines a partition of a number $j, 0 \le j \le n$ into a sum of r parts. Let $\Delta_{r,n} := \{e \in \mathbb{N}_0^r : e_1 + \dots + e_r \le n\}$ be the set of all such partitions.

To motivate this definition recall that the group of linear automorphisms of the ordered Hamming space is given by the wreath product $GL_P(n) = T_r \wr S_n$, where T_r is the set of all $r \times r$ upper-triangular matrices over $\mathbb{F}_q$ in which every element on the main diagonal is nonzero, and S_n is the symmetric group of order n [32]. The action of $GL_P(n)$ on vectors of a fixed shape is clearly transitive, and shape is the coarsest invariant for this action. We refer to [3] for more details about invariants of linear codes on posets and their connections with translation association schemes.

The ordered weight of a vector $x \in \mathbb{F}_q^N, \mathrm{shape}(x) = e$ is found as $w_P(x) = \sum_{i=1}^n i e_i$. An $[N, k, d]$ linear code is a linear subspace $\mathcal{C} \subset \mathbb{F}_q^N$ such that the dimension of $\mathcal{C}$ over $\mathbb{F}_q$ is k and the minimum ordered weight of a nonzero vector in $\mathcal{C}$ is d.

The *dual poset* $P^\perp$ on the set E is derived from P by inverting the order: $x \prec y$ in $P^\perp$ if and only if $y \prec x$ in P. An ideal in $P^\perp$ is called a *filter* with respect to the original order P. We call a subset of E *left-adjusted* (resp., *right-adjusted*) if it is an ideal (a filter) in P. The *dual code* $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ is defined as the set $\{y \in \mathbb{F}_q^N : \forall_{x \in \mathcal{C}} \sum_{i,j} x_{ij} y_{ij} = 0\}$. If the distances of $\mathcal{C}$ are defined using the poset P as in (3), then the distances in $\mathcal{C}^\perp$ should be defined using the dual order $P^\perp$. In other words, $w_{P^\perp}(x), x \in \mathbb{F}_q^N$ is the cardinality of the smallest filter in P that contains the support of x[(†)].

Let G be a $k \times N$ matrix whose rows form a basis of $\mathcal{C}$ and let H be the matrix whose rows form a basis of the dual code $\mathcal{C}^\perp$. In coding theory G is called the *generator matrix* and H the *parity-check matrix* of $\mathcal{C}$. Note that these matrices describe linear codes and do not depend on the metric being used.

Define the *shape enumerator* of the code $\mathcal{C}$ by

$$A(z_0, z_1, \dots, z_r) = \sum_{e \in \Delta_{r,n}} \mathcal{A}_e {z_0}^{e_0} {z_1}^{e_1} \dots {z_r}^{e_r}, \tag{4}$$

where $\mathcal{A}_e = |\{x \in \mathcal{C} : \mathrm{shape}(x) = e\}|$. The shape distribution is a natural analog of the weight distribution of a linear code in the Hamming space.

For a subset $F \in E$ let $\mathcal{C}_F := \mathrm{proj}_F \mathcal{C}$ be the projection of $\mathcal{C}$ on the coordinates indexed by F and let $\mathcal{C}^F := \{x \in \mathcal{C} : x_i = 0 \text{ for all } i \in F^c\}$. The subcode $\mathcal{C}^F$ is called the *shortening* of $\mathcal{C}$ and the subcode $\mathcal{C}_F$ the *puncturing* of $\mathcal{C}$. Clearly, $\dim \mathcal{C}_F = \mathrm{rk}(G(F))$, where $G(F)$ is the submatrix of G formed of the columns indexed by F. Standard properties of these subcodes are given in the following obvious lemma.

Lemma 2.1.
1) $\mathcal{C}_F \cong \mathcal{C}/\mathcal{C}^{F^c}$*;* $\dim \mathcal{C}_F = k - \dim C^{F^c}$*,*
2) $\dim \mathcal{C}^F = |F| - \mathrm{rk}(H(F))$*.*

2-B. **Rank distributions.**

(†) The reasons for this way of measuring the distances in $\mathcal{C}^\perp$ are rather subtle. They are related to duality in translation association schemes constructed on the poset metric space. A detailed discussion of this topic is contained in [3]; see also [6].

2-B.1. *Multivariate Tutte polynomial: The classical case.* We again begin with a brief motivating discussion. In the case of usual matroids the multivariate Tutte polynomial was introduced by Sokal in [37]. Let $\mathcal{M}$ be a matroid on the set $E = \{1, 2, \dots, N\}$ [42]. Let ρ be the rank function $\rho : 2^E \to \mathbb{Z}^+ \cup \{0\}$ of $\mathcal{M}$, which for every subset $A \subset E$ gives the cardinality of the largest independent subset contained in it. Let $v = (v_1, \dots, v_N)$. The *multivariate Tutte polynomial* of $\mathcal{M}$ is a function of $N+1$ variables v, q^{-1} given by

$$Z_{\mathcal{M}}(q, v) = \sum_{A \subset E} q^{-\rho A} \prod_{a \in A} v_a. \tag{5}$$

The Tutte polynomials of codes in the Hamming space and the ordered space are obtained as appropriate specializations of $Z_{\mathcal{M}}(q, v)$.

Let $\mathcal{M}^\perp$ be the dual matroid of $\mathcal{M}$. The Tutte polynomial of $\mathcal{M}^\perp$, denoted by $Z_{\mathcal{M}^\perp}$, is defined analogously to (5) using the dual rank function $\rho^\perp$. By [37, p. 186],

$$Z_{\mathcal{M}^\perp}(q, v) = q^{\rho E} \Big(\prod_{a \in E} \frac{v_a}{q} \Big) Z_{\mathcal{M}}\Big(\frac{q}{v}\Big) \tag{6}$$

where

$$Z_{\mathcal{M}}\Big(\frac{q}{v}\Big) = \sum_{A \subset E} q^{\rho A} \prod_{a \in A} \Big(\frac{q}{v_a}\Big).$$

In the situation of interest to us, the matroid $\mathcal{M}$ is represented by a linear code $\mathcal{C} \subset \mathbb{F}_q^N$.

The rank functions of $\mathcal{M}$ are given by the ranks of submatrices of G and H, namely $\rho A = \mathrm{rk}(G(A)), \rho^\perp(A) = \mathrm{rk}(H(A))$, where $A \subset E$. Below when we have in mind a pair of dual matroids represented by the codes $\mathcal{C}, \mathcal{C}^\perp$, we write Z and $Z^\perp$ instead of $Z_{\mathcal{M}}$ and $Z_{\mathcal{M}^\perp}$, respectively.

In classical theory [42], the Tutte polynomial of the matroid $\mathcal{M}$ is a bivariate polynomial defined as

$$T_{\mathcal{M}}(x, y) = \sum_{A \subset E} (x-1)^{\rho E - \rho A} (y-1)^{|A| - \rho A}. \tag{7}$$

Definition (5) reduces to (7) upon the change of variables $q = (x-1)(y-1)$, $v_1 = \dots = v_N = (y-1)$:

$$T_{\mathcal{M}}(x, y) = (x-1)^{\rho E} Z_{\mathcal{M}}\big((x-1)(y-1), y-1, \dots, y-1\big). \tag{8}$$

For the bivariate polynomials the duality relation (6) takes the form

$$T_{\mathcal{M}}(x, y) = T_{\mathcal{M}^\perp}(y, x). \tag{9}$$

This relation together with the celebrated Greene's theorem [18] implies the MacWilliams theorem for linear codes [24, p.146].

2-B.2. *The ordered case.* In [37], Sokal remarks that in several instances the "multivariate extension of a single variable result is not only vastly more powerful but also much easier to prove." Our study lends further support to this observation: as we shall see, the multivariate Tutte polynomial is well-suited to the study of codes in the ordered Hamming space.

Below in this section we assume that the set E is as in (1). Let $\mathcal{C} \subset \mathbb{F}_q^N$ be an ordered linear code with the rank function $\rho(I) = \mathrm{rk}(G(I)), I \subset E$ and let $z = (z_1, z_2, \dots, z_r)$ be a vector variable. Define the multivariate Tutte polynomial of $\mathcal{C}$ by

$$Z(q, z) = \sum_{e \in \Delta_{r,n}} \sum_{\substack{I \in \mathcal{I}(P) \\ \mathrm{shape}(I) = e}} q^{-\rho I} \prod_{i=1}^{r} z_i^{e_i}. \tag{10}$$

The relation of $Z(q, z)$ to the Tutte polynomial (5) is as follows. For a given ideal $I \in \mathcal{I}(P)$ we put $v_a = 1$ if a is not a maximal element of I and put $v_a = z_i$ if a is a maximal element in I and has index i in its chain. In other words, the polynomial $Z(q, z)$ is defined from (5) upon replacing the sum on all subsets A of E with the sum over the ideals $I \in \mathcal{I}(P)$ and collapsing some of the variables in v.

In this section we study relations between the Tutte polynomial of an ordered code $\mathcal{C}$ and the shape enumerator (4) of this code. For a shape vector $e = (e_1, \dots, e_r)$ denote by $\bar{e}$ the shape obtained by setting

$$\bar{e}_i = e_{r-i}, \quad i = 1, \dots, r-1. \tag{11}$$

Observe that $\bar{e}_r = e_0$.

Our first result is a duality relation for the Tutte polynomials of a pair of dual ordered codes.

Proposition 2.2. (MacWilliams theorem) *Let $\mathcal{C}$ be an ordered code, let $\mathcal{C}^\perp$ be its dual code, and let $Z(q,z)$ and $Z^\perp(q,z)$ be their Tutte polynomials. Then*

$$Z^\perp(q,z_1,z_2,\dots,z_r) = q^{\rho E - N} z_r^n Z\Big(q, \frac{qz_{r-1}}{z_r}, \frac{q^2 z_{r-2}}{z_r}, \dots, \frac{q^{r-1}z_1}{z_r}, \frac{q^r}{z_r}\Big). \tag{12}$$

Proof : Let $\bar{I} \in P^\perp, I^c = E\backslash \bar{I}$. Using Lemma 2.1 with $F = \bar{I}$, we obtain the relation

$$\rho^\perp \bar{I} = \rho I^c + |\bar{I}| - \rho E. \tag{13}$$

Now consider the definition of Z (10) and use (13) for each individual term in the sum on I. Consider an arbitrary pair of subsets $(\bar{I}, I^c)$ where $\bar{I} \in P^\perp$ and $I^c = E\backslash\bar{I} \in P$. Let $\mathrm{shape}(\bar{I}) = \bar{e} = (\bar{e}_1,\dots,\bar{e}_r)$. Then $\mathrm{shape}(I^c) = e = (e_1,e_2,\dots,e_r)$, where the vectors $\bar{e}$ and e are related as in (11). We have

$$\begin{aligned} q^{-\rho^\perp \bar{I}} \prod_{i=1}^r z_i^{\bar{e}_i} &= q^{-\rho I^c - |\bar{I}| + \rho E}\Big(\prod_{i=1}^{r-1} z_i^{e_{r-i}}\Big) z_r^{n-|e|} \\ &= q^{\rho E - N - \rho I^c + |I^c|} z_r^{n-e_r} \prod_{i=1}^{r-1}\Big(\frac{z_{r-i}}{z_r}\Big)^{e_i} \\ &= q^{\rho E - N} z_r^n q^{-\rho I^c}\Big(\frac{q^r}{z_r}\Big)^{e_r} \prod_{i=1}^{r-1}\Big(\frac{q^i z_{r-i}}{z_r}\Big)^{e_i}. \end{aligned} \tag{14}$$

Now let us sum the equality (14) on all the ideals $\bar{I}$. To each $\bar{I}$ there corresponds a unique $I^c \in \mathcal{I}(P)$, so we can sum on I^c on the right-hand side. This proves our claim. ∎

As already noted, the Tutte polynomial for the code in the Hamming metric is usually defined in the form (8) which relies on a different set of variables compared to (10). To introduce an expression analogous to (8) for the ordered code, let $y = (y_1,\dots,y_r)$ and let

$$T(x,y) = \sum_{e\in\Delta_{r,n}} \sum_{\substack{I\in\mathcal{I}(P)\\ \mathrm{shape}(A)=e}} \Big\{(x-1)^{\rho E - \rho I}(y_r-1)^{|I|-\rho I}\prod_{i=1}^{r-1}(y_i-1)^{e_i}\Big\}. \tag{15}$$

To move between Z and T we perform the following change of variables:

$$\begin{cases} q = (x-1)(y_r-1), \\ z_i = (y_i-1)(y_r-1)^i,\ 1\le i\le r-1, \\ z_r = (y_r-1)^r. \end{cases} \tag{16}$$

Then one can check that

$$T(x,y) = (x-1)^{\rho(E)} Z(q,z).$$

In the next theorem we derive an extension of the duality relation (9) to the ordered case.

Theorem 2.3.

$$T^\perp(x,y_1,\dots,y_r) = T(y_r,y_{r-1},\dots,y_1,x). \tag{17}$$

Proof : As in the previous proposition, we establish the claim by considering individual terms on the left- and right-hand sides. Multiply both sides of (14) by $(x-1)^{\rho^\perp E}$ and perform the change of variables (16). Using (13), we obtain

$$\begin{aligned}(x-1)^{\rho^\perp E-\rho^\perp \bar I}&(y_r-1)^{|\bar I|-\rho^\perp \bar I}\prod_{i=1}^{r-1}(y_i-1)^{\bar e_i}\\ &=(x-1)^{\rho^\perp E+\rho E-nr+|I^c|-\rho I^c}\Big(\prod_{i=1}^{r-1}(y_{r-i}-1)^{e^i}\Big)(y_r-1)^{(\rho E-rn-\rho I^c+|I^c|)+r(n-e_r)-\sum_{i=1}^{r-1} ie_i}\\ &=(x-1)^{|I|^c-\rho I^c}(y_r-1)^{|I^c|-\rho I^c}\prod_{i=1}^{r-1}(y_{r-i}-1)^{e^i}.\end{aligned}$$

Now sum both sides on $\bar I\in\mathcal{I}(P^\perp)$ and observe that on the right the sum goes over all $I^c\in\mathcal{I}(P)$. This proves the theorem. ∎

Below we argue that this relation is valid for any pair of mutually dual matroids defined on the NRT poset without appealing to their linear representations.

Remark: The polynomial Z can be written in a different form that is analogous to the Whitney function of usual matroids. For an ordered linear code with generator matrix G let us introduce the *shape-rank distribution* as the set of coefficients

$$R_e^v\triangleq|\{A\in\mathcal{I}(P):\mathrm{shape}(A)=e,\mathrm{rk}(G(A))=v\}|,\quad v=0,1,\dots,k. \tag{18}$$

Then

$$Z(y^{-1},z)=\sum_{e\in\Delta_{r,n}}\sum_{v=0}^{k}R_e^v{z_1}^{e_1}{z_2}^{e_2}\dots{z_r}^{e_r}y^v. \tag{19}$$

2-B.3. *The Tutte polynomial and shape enumerator.* Let f and e be shape vectors. We write $f\le e$ as a shorthand for the following set of conditions:

$$f_{r-l+1}+\dots+f_r\le e_{r-l+1}+\dots+e_r,\quad l=1,\dots,r. \tag{20}$$

In the following lemma we relate the two generating functions in the title of this section.

Lemma 2.4. *Let $T\in\mathcal{I}(P)$ be an ideal of shape f. The quantity*

$$N(f,e)=|\{S\in\mathcal{I}(P):\mathrm{shape}(S)=e,T\subset S\}| \tag{21}$$

does not depend on T, and the shape enumerator (4) *satisfies the expression*

$$A(z_0,z_1,\dots,z_r)=\sum_{e,f:f\le e}\mathcal{A}_fN(f,e)\Big(\prod_{i=0}^{r-1}(z_i-z_{i+1})^{e_i}\Big){z_r}^{e_r}. \tag{22}$$

Proof : Let $T,S\in\mathcal{I}(P),T\subset S,\mathrm{shape}(T)=f,\mathrm{shape}(S)=e$. Let $S_i,i=0,\dots,r$ be the subset of chains in S such that $w_P(S_i)=i$, and let $T_i,i=0,\dots,r$ be the same for T. The condition $T\subset S$ is equivalent to the set of r conditions

$$\bigcup_{j=r-l+1}^{r}T_i\subset\bigcup_{j=r-l+1}^{r}S_i,\quad l=1\dots r,$$

which in turn is equivalent to the condition $f\le e$. Thus, the count of the ideals S for which $T\subset S$ depends only on the shape f.

Consider a binary matrix Q with rows indexed by ideals of shape f and columns by ideals of shape e such that $Q_{ST}=\mathbb{1}(T\subset S)$. The matrix has dimensions $\binom{n}{f}\times\binom{n}{e}$, where for instance, $\binom{n}{f}=\binom{n}{f_1,f_2,\dots,f_r}$ is the number of ways to choose r subsets of size $f_1,\dots,f_r$ out of an n-set. We have

$$|\{T:Q_{ST}=1\}|=\binom{e_r}{f_r}\binom{e_r+e_{r-1}-f_r}{f_{r-1}}\dots\binom{e_r+\dots+e_0-(f_r+\dots+f_1)}{f_0}$$

and this quantity does not depend on S. Therefore, $N(f,e) = |\{T : Q_{ST} = 1\}|$ for any fixed S of shape e. Since $|\{T : Q_{ST} = 1\}|\binom{n}{f} = \{S : Q_{ST} = 1\}\binom{n}{e}$, we obtain

$$\begin{aligned} N(f,e) &= \binom{e_r}{f_r}\binom{e_r+e_{r-1}-f_r}{f_{r-1}}\cdots\binom{e_r+\cdots+e_0-(f_r+\cdots+f_1)}{f_0}\binom{n}{e}\binom{n}{f}^{-1} \\ &= \binom{e_r+e_{r-1}-f_r}{e_{r-1}}\binom{e_r+e_{r-1}+e_{r-2}-(f_r+f_{r-1})}{e_{r-2}}\cdots\binom{e_r+\cdots+e_0-(f_r+\cdots+f_1)}{e_0} \\ &= \binom{E_{r-1}-F_r}{e_{r-1}}\binom{E_{r-2}-F_{r-1}}{e_{r-2}}\cdots\binom{E_0-F_1}{e_0}, \end{aligned} \tag{23}$$

where the second equality follows on writing out the binomials explicitly and performing cancellations, and in the last step we just introduced the notation $E_i = \sum_{j=i}^r e_j$, $F_i = \sum_{j=i}^r f_j, i = 1,\ldots,r$.

Now let us substitute expression (23) into the right-hand side of (22) and interchange the order of summation:

$$\begin{aligned} &\sum_{e\in\Delta_{r,n}}\sum_{f\le e}\mathcal{A}_f N(f,e)(z_0-z_1)^{e_0}(z_1-z_2)^{e_1}\ldots(z_{r-1}-z_r)^{e_{r-1}}{z_r}^{e_r} \\ &\quad= \sum_f \mathcal{A}_f \sum_{e_r=f_r}^{n}\sum_{e_{r-1}=f_r+f_{r-1}-e_r}^{n-e_r}\cdots\sum_{e_1=f_r+\cdots+f_1-(e_r+\cdots+e_2)}^{n-e_r-\cdots-e_2} \\ &\qquad\qquad \binom{E_0-F_1}{E_1-F_1}\cdots\binom{E_{r-1}-F_r}{E_r-F_r}(z_0-z_1)^{e_0}(z_{r-1}-z_r)^{e_{r-1}}{z_r}^{e_r} \\ &\quad\overset{(a)}{=} \sum_f \mathcal{A}_f \sum_{E_1=F_1}^{n}\binom{n-F_1}{E_1-F_1}(z_0-z_1)^{n-E_1} \\ &\qquad\times\sum_{E_2=F_2}^{E_1}\cdots\sum_{E_r=F_r}^{E_{r-1}}\binom{E_{r-1}-F_r}{E_r-F_r}(z_{r-1}-z_r)^{E_{r-1}-E_r}{z_r}^{E_r-f_r}{z_r}^{f_r} \\ &\quad\overset{(b)}{=} \sum_f \mathcal{A}_f \sum_{E_1=f_1+\cdots+f_r}^{n}\binom{n-F_1}{E_1-F_1}(z_0-z_1)^{n-E_1} \\ &\qquad\sum_{E_2=F_2}^{E_1}\cdots\sum_{E_{r-1}=F_{r-1}}^{E_{r-2}}\binom{E_{r-2}-F_{r-1}}{E_{r-1}-F_{r-1}} \\ &\qquad\qquad\times(z_{r-2}-z_{r-1})^{E_{r-2}-E_{r-1}}{z_{r-1}}^{E_{r-1}-F_{r-1}}{z_{r-1}}^{f_{r-1}}{z_r}^{f_r} \\ &\quad= \cdots = \sum_f \mathcal{A}_f {z_0}^{f_0}\ldots{z_{r-1}}^{f_{r-1}}{z_r}^{f_r} \\ &\quad= A(z_0,z_1,\ldots,z_r), \end{aligned}$$

where in (a) we pull out the sum on e_1, then on e_2, and so on up to e_{r-1}, and then change the variables $e_i \to E_i, i = 1,\ldots,r$; to obtain (b) we notice that the sum on E_r on the previous line equals $z_{r-1}^{E_{r-1}-F_r} = z_{r-1}^{E_{r-1}-F_{r-1}+f_{r-1}}$, and evaluate successively the sums on E_i for all i. ∎

Remark: For the usual Hamming space the quantities $N(f,e)$ reduce to *binomial moments* of the weight distribution of the code; see Sect. 1-C in the Introduction.

Using Lemma 2.4, it is possible to relate the shape enumerator of the code (4) to the multivariate Tutte polynomial.

Theorem 2.5. *(Greene's theorem for ordered codes)*

$$A(z_0,z_1,\ldots,z_r) = q^k {z_r}^n Z\Big(q, \frac{z_{r-1}-z_r}{z_r}, \frac{z_{r-2}-z_{r-1}}{z_r}, \ldots, \frac{z_0-z_1}{z_r}\Big). \tag{24}$$

Proof : Consider the set

$$\{(x,I) : I \in \mathcal{I}(P), \mathrm{shape}(I) = e, x \in \mathcal{C}^I, \mathrm{shape}(x) \le e\}$$

Using Lemma 2.1.2, Eq. (13), and (18), we obtain the following chain of equalities

$$\begin{aligned}\sum_{f\le e}\mathcal{A}_f N(f,e) &= \sum_{\mathrm{shape}(I)=e}|\mathcal{C}^I| = \sum_{\mathrm{shape}(I)=e} q^{|I|-\mathrm{rk}(H(I))}\\ &= \sum_{\mathrm{shape}(I^c)=\bar e} q^{k-\mathrm{rk}(G(I^c))} = q^k \sum_{\mathrm{shape}(I^c)=\bar e} q^{-\mathrm{rk}(G(I^c))}\\ &= q^k\sum_{u=0}^{k} q^{-u}R^u_{\bar e}.\end{aligned}$$

Using this equality in (22), we obtain

$$\begin{aligned}A(z_0,z_1,\dots,z_r) &= \sum_{e\in\Delta_{r,n}}\sum_{f\le e}\mathcal{A}_f N(f,e)(z_0-z_1)^{e_0}\dots(z_{r-1}-z_r)^{e_{r-1}}{z_r}^{e_r}\\ &= \sum_{e\in\Delta_{r,n}}\sum_{u=0}^{k} q^{k-u}R^u_{\bar e}(z_0-z_1)^{e_0}\dots(z_{r-1}-z_r)^{e_{r-1}}{z_r}^{e_r}\\ &= \sum_{\bar e\in\Delta_{r,n}}\sum_{u=0}^{k} q^{k-u}R^u_{\bar e}(z_0-z_1)^{\bar e_r}\dots(z_{r-1}-z_r)^{\bar e_1}{z_r}^{\bar e_0}\\ &= \sum_{\bar e\in\Delta_{r,n}}\sum_{u=0}^{k} q^{k-u}R^u_{\bar e}\Big(\frac{z_{r-1}-z_r}{z_r}\Big)^{\bar e_1}\dots\Big(\frac{z_0-z_1}{z_r}\Big)^{\bar e_r}{z_r}^{n}\\ &= q^k{z_r}^n\sum_{\bar e\in\Delta_{r,n}}\sum_{u=0}^{k} R^u_{\bar e}\Big(\frac{z_{r-1}-z_r}{z_r}\Big)^{\bar e_1}\dots\Big(\frac{z_0-z_1}{z_r}\Big)^{\bar e_r}\Big(\frac{1}{q}\Big)^{u}\\ &\overset{(19)}{=} q^k{z_r}^n Z\Big(q,\frac{z_{r-1}-z_r}{z_r},\dots,\frac{z_0-z_1}{z_r}\Big).\end{aligned}$$

∎

Relying on this theorem, we can write the MacWilliams equation (12) in a more familiar form that involves shape distributions. The statement of the following theorem is known [25, 13], while our proof is new.

Theorem 2.6. *Let $\mathcal{C},\mathcal{C}^\perp\subset\mathbb{F}_q^N$ be a pair dual linear codes in the ordered Hamming space. Then*

$$A^\perp(u_0,u_1,\dots,u_r)=\frac{1}{|\mathcal{C}|}A(z_0,z_1,\dots,z_r)$$

where

$$\begin{aligned}z_0 &= u_0+(q-1)\sum_{i=1}^{r}q^{i-1}u_i,\\ z_{r-j+1} &= u_0+(q-1)\sum_{i=1}^{j-1}q^{i-1}u_k-q^{j-1}u_j,\quad 1\le j\le r.\end{aligned}$$

Proof : We have

$$\begin{aligned}&A^\perp(u_0,u_1,\dots,u_r)\\ &\quad= q^{nr-k}u_r^n\,Z^\perp\Big(q;\frac{u_{r-1}-u_r}{u_r},\dots,\frac{u_{r-j}-u_{r-j+1}}{u_r},\dots,\frac{u_0-u_1}{u_r}\Big)\\ &\quad= (u_0-u_1)^n Z\Big(q;\frac{u_1-u_2}{u_0-u_1}q,\dots,\frac{u_j-u_{j+1}}{u_0-u_1}q^j,\dots,\frac{u_{r-1}-u_r}{u_0-u_1}q^{r-1},\frac{u_r}{u_0-u_1}q^r\Big)\\ &\quad= \frac{1}{|\mathcal{C}|}A(z_0,z_1,\dots,z_r),\end{aligned}$$

where the first and the third steps rely on (24), the second equality uses (12), and the variables $z_i, i = 0, \dots, r$ have been introduced to write the generating function $A(\cdot)$ in a concise form. These variables are related to the u-variables in a way that is evident from (24): namely, we have

$$\begin{aligned} z_r &= u_0 - u_1 \\ z_{r-j} &= z_{r-j+1} + (u_j - u_{j+1})q^j, \quad j = 1, 2, \dots, r-1; \\ z_0 &= z_1 + u_r q^r. \end{aligned}$$

Solving for the z-variables proves the theorem. ∎

2-C. **Support shape distributions.** In the classical case of the Hamming space, the considerations of the previous section can be extended to support weight distributions (distributions of higher Hamming weights) [2]. In this section we do the same for the higher shape distributions of ordered codes. We refer to [5] for general results on higher weights of codes in poset metric spaces including the ordered Hamming space.

Let $\mathcal{C} \subset \mathbb{F}_q^N$ be a linear ordered code, and let

$$A^{(j)}(I) = |\{D : D \subset \mathcal{C}, \dim(D) = j, \langle \mathrm{supp}(D) \rangle = I\}|$$

where $\mathrm{supp}(D) = \cup_{x \in D} \mathrm{supp}(x)$ and $I \in \mathcal{I}(P)$ is an ideal.

Define

$$A_e^{(j)} = \sum_{I : \mathrm{shape}(I) = e} A^{(j)}(I).$$

The set $\{A_e^j, e \in \Delta_{r,n}\}$ is called the *jth support shape distribution* of $\mathcal{C}$. Let us introduce the following quantities:

$$[m]_u = \prod_{i=0}^{u-1} (q^m - q^i), \quad [m]_0 := 1,$$

$$D^{(m)}(I) = \sum_{u=0}^{m} [m]_u A^{(u)}(I), \ m \geq 0 \tag{25}$$

$$D_e^{(m)} = \sum_{I : \mathrm{shape}(I) = e} D^{(m)}(I)$$

$$D^{(m)}(z_0, z_1, \dots, z_r) = \sum_{e \in \Delta_{r,n}} D_e^{(m)} z_0^{e_0} \dots z_r^{e_r}, \ m \geq 0. \tag{26}$$

Theorem 2.7.

$$D^{(m)}(z_0, z_1, \dots, z_r) = q^{mk} {z_r}^n Z\left(q^m, \frac{z_{r-1} - z_r}{z_r}, \frac{z_{r-2} - z_{r-1}}{z_r}, \dots, \frac{z_0 - z_1}{z_r}\right).$$

Proof : Repeating the arguments in the proof of Lemma 2.4, we obtain the following equality:

$$D^{(m)}(z_0, z_1, \dots, z_r) = \sum_{e \in \Delta_{r,n}} \sum_{f \leq e} D_f^{(m)} N(f, e)(z_0 - z_1)^{e_0} (z_1 - z_2)^{e_1} \dots (z_{r-1} - z_r)^{e_{r-1}} {z_r}^{e_r}. \tag{27}$$

From (25) we have

$$\sum_{f \leq e} D_f^{(m)} N(f, e) = \sum_{f \leq e} \sum_{u=0}^{m} [m]_u A_f^{(u)} N(f, e) \tag{28}$$

Define the numbers

$$T_e^{(m)} = |\{X \in \mathcal{I}(P) : \mathrm{shape}(X) = e, \dim \mathcal{C}^X = m\}|.$$

We claim that

$$\sum_{f \leq e} A_f^{(j)} N(f, e) = \sum_{m=j}^{k} \begin{bmatrix} m \\ j \end{bmatrix} T_e^{(m)}, \tag{29}$$

where $\left[{t \atop u}\right] \triangleq [t]_u/[u]_u$ is the Gaussian binomial. This equality follows by counting in two different ways the size of the following set:

$$\{(D, X) : \dim(D) = j, X \subset E, \mathrm{shape}(X) = e, \langle \mathrm{supp}\, D\rangle \subset X\}$$

where D is a linear subcode of C. Further, from Lemma 2.1, the definition of $T_e^{(m)}$ and (18), we observe that $T_e^m = R_{\bar{e}}^{k-m}$. Hence we continue from (28) as follows:

$$\begin{aligned}\sum_{u=0}^{m}[m]_u \sum_{f\le e} N(f,e)A_f^{(u)} &= \sum_{u=0}^{m}[m]_u \sum_{t=u}^{k}\begin{bmatrix} t \\ u\end{bmatrix} R_{\bar{e}}^{k-t}\\ &= \sum_{u=0}^{m}\sum_{t=0}^{k}[m]_u \begin{bmatrix} t \\ u\end{bmatrix} R_{\bar{e}}^{k-t} = \sum_{u=0}^{m}\sum_{j=0}^{k}[m]_u \begin{bmatrix} k-j \\ u\end{bmatrix} R_{\bar{e}}^{j}\\ &= \sum_{j=0}^{k}\sum_{u=0}^{m}[m]_u \begin{bmatrix} k-j \\ u\end{bmatrix} R_{\bar{e}}^{j} = \sum_{j=0}^{k} q^{m(k-j)} R_{\bar{e}}^{j}.\end{aligned}$$

Therefore,

$$\begin{aligned}D^{(m)}(z_0, z_1, \dots, z_r) &= \sum_{e\in\Delta_{r,n}}\sum_{j=0}^{k} q^{m(k-j)} R_{\bar{e}}^{j}(z_0-z_1)^{e_0}\dots(z_{r-1}-z_r)^{e_{r-1}} {z_r}^{e_r}\\ &= \sum_{\bar{e}}\sum_{j=0}^{k} q^{m(k-j)} R_{\bar{e}}^{j}\Big(\frac{z_0-z_1}{z_r}\Big)^{\bar{e}_r}\dots\Big(\frac{z_{r-1}-z_r}{z_r}\Big)^{\bar{e}_1}{z_r}^{n}\\ &= q^{mk}{z_r}^{n} Z\Big(q^m, \frac{z_{r-1}-z_r}{z_r}, \dots, \frac{z_0-z_1}{z_r}\Big).\end{aligned}$$

∎

This theorem enables us to establish MacWilliams-type relations for the support weight enumerators of $\mathcal{C}$ and its dual code $\mathcal{C}^\perp$, extending the results of [2] to the ordered case.

Theorem 2.8. (MacWilliams theorem for higher poset weights) *Let $\mathcal{C}$ and $\mathcal{C}^\perp$ be a pair of mutually dual linear codes. Then*

$$(D^{(m)})^\perp(u_0, u_1, \dots, u_r) = \frac{1}{|\mathcal{C}|^m} D^{(m)}(z_0, z_1, \dots, z_r)$$

where

$$\begin{aligned}z_0 &= u_0 + (q^m-1)\sum_{i=1}^{r} q^{(i-1)m}u_i,\\ z_{r-j+1} &= u_0 + (q^m-1)\sum_{i=1}^{j-1} q^{(i-1)m}u_k - q^{(j-1)m}u_j, \qquad 1\le j\le r.\end{aligned}$$

The proof of this result is analogous to the computations that led to Theorem 2.6 and will be omitted.

2-C.1. *Ordered MDS codes.* The distributions of support shapes (A_e^j) contain a large amount of information about the structure of the linear code. At the same time, computing them is generally a difficult problem. In this section we compute support shape distributions for ordered MDS codes [14, 20] which we proceed to define.

A linear ordered code $\mathcal{C}[N = nr, k, d]$ is called *Maximum Distance Separable* (MDS) if its distance d, length N, and dimension k satisfy the equality $d = N - k + 1$. We note that $N - k + 1$ is the largest possible value of the code distance for given N and k. The equality condition restricts the structure of the code, making it possible to compute the shape distributions. In the case of the Hamming metric a similar calculation was performed in Helleseth et al. [19]. Let us start with the following straightforward lemma.

Lemma 2.9. [23] *Let $F_l = \{U : U$ a subspace of $\mathbb{F}_q^k$ of dimension $l\}$. Let $\mathcal{B}$ be a j-dimensional subcode of a linear code $\mathcal{C}$ of dimension k. For $j = 0, \ldots, k$, $\mathcal{B} \mapsto U_{\mathcal{B}}$ is a bijection between the set of j-dimensional subspaces of $\mathcal{C}$ and the set F_{k-j} where $U_B \in F_{k-j}$.*

Proposition 2.10. *Let $\mathcal{C} \subset \mathbb{F}_q^N$ be an $[N = nr, k]$ linear ordered code. Let i_0 be the largest integer such that any i_0 left-adjusted column vectors from the generator matrix of the code $\mathcal{C}$ are linearly independent. If $k - i_0 < j < k$, then*

$$A_e^{(j)} = \binom{n}{e} \sum_{h=0}^{k-j-N+i} (-1)^h \binom{i}{h} \begin{bmatrix} k-N+i-h \\ j \end{bmatrix}, \tag{30}$$

where e is a shape vector with $\sum_{s=1}^{n} se_s = i$.

Proof : The proof follows closely [19] and is included to make sure that the ordered case does not cause any complications. Let S be a set of column vectors of a generator matrix of $\mathcal{C}$, let $S_1 \subset S$ be an right-adjusted subset with $|S_1| = i$, and let $i \leq j < i_0$. Define the quantities $K_j(S_1)$ and $M_j(S_1)$ as follows:

$$\begin{aligned} K_j(S_1) =& |\{U : U \subset \mathbb{F}_{q^k}, U \text{ is a vector space}, \dim U = j, U \cap S = S_1\}|. \\ M_j(S_1) =& |\{U : U \subset \mathbb{F}_{q^k}, U \text{ is a vector space}, \dim U = j, U \supset S_1\}|. \end{aligned}$$

We have

$$\sum_{S_1 \subset S_2 \subset S} K_j(S_2) = M_j(S_1). \tag{31}$$

Note that neither S nor S_2 are assumed to be right-adjusted.

The quantity $M_j(S_1)$ is the number of j-dimensional subspaces of $\mathbb{F}_{q^k}$ containing the i-dimensional subspace spanned by the set S_1. Therefore,

$$M_j(S_1) = \begin{bmatrix} k-i \\ j-i \end{bmatrix} \tag{32}$$

We claim that for $j < i_0$ the quantity $K_j(S_1)$ depends only on i. First, when $i = j$, we have $K_j(S_1) = 1$. Arguing by induction, assume that $K_j(S_1)$ does not depend on S_1 for all $i = |S_1| > j - t$. If $i = j - t$, Eq. (31) becomes

$$K_j(S_1) + \sum_{S_1 \subsetneq S_2 \subset S} K_j(S_2) = \begin{bmatrix} k-i \\ j-i \end{bmatrix}.$$

Since $|S_2| > |S_1| > i$, by the induction hypotheses all the terms in the sum on S_2 depend only on the cardinality $|S_2|$, showing that $K_j(S_1)$ depends only on the cardinality of S_1, but not on the choice of the set S_1 itself. Writing K_{ij} for $K_j(S_1)$, we can rewrite (32) as follows:

$$\sum_{h=0}^{j-i} \binom{N-i}{h} K_{i+h,j} = \begin{bmatrix} k-i \\ j-i \end{bmatrix}.$$

Using Möbius inversion, we obtain

$$K_{i,j} = \sum_{h=0}^{j-i} (-1)^h \binom{nr-i}{h} \begin{bmatrix} k-i-h \\ k-j \end{bmatrix}.$$

By the definitions of K_{ij} and $A_e^{(j)}$ and Lemma 2.9, we have that

$$\begin{aligned} A_e^{(j)} &= \binom{n}{e} A^{(j)}(I) = \binom{n}{e} K_{nr-i,k-j} \\ &= \binom{n}{e} \sum_{h=0}^{k-j-nr+i} (-1)^h \binom{i}{h} \begin{bmatrix} k-nr+i-h \\ j \end{bmatrix}, \end{aligned}$$

which completes the proof. ∎

For the case of ordered linear MDS codes this proposition gives the entire shape distribution. Indeed, if $\mathcal{C}$ is an $[N,k,d]$ MDS code, then $i_0 = k$, and the values of $A_e^{(j)}, j = 1,\dots,k-1$ are found in (30). Further $A_e^{(0)} = 1$ if $e_0 = n, e_1 = \cdots = e_r = 0$, and $A_e^{(0)} = 0$ otherwise. Finally if $j = k$, then (30) implies that $A_e^{(j)} = 0$ unless $i = N$, i.e., the shape is such that $e_0 = e_1 = \cdots = e_{n-1} = 0$ and $e_n = n$, in which case $A_e^{(k)} = 1$.

3. Poset Matroids and Linear Ordered Codes

3-A. **Poset matroids.** Linear codes in the Hamming space have been studied from the point of view of matroid theory in several recent papers [9, 21]. In this section we discuss a connection between ordered linear codes and matroid theory. Matroid theory can be extended to posets in several ways including supermatroids [15] and geometries on partially ordered sets [16]. These and other possible generalizations are discussed in the recent paper [43]. Here we focus on a particular case of these generalizations under which all the classical definitions are modified to rely on order ideals rather than subsets.

The following definition is a particular case of the concept introduced by Barnabei et al. [7, 8]. While the results of these papers apply to all posets, in this section we consider only the case of P being the NRT poset. For $A \subset E$ consider the set $\mathrm{Min}(A) = \{x \in A : x \text{ is minimal in } A\}$. The *poset matroid* $\mathcal{M}$ on E is a family $\mathfrak{B}$ of ideals in E, called bases, satisfying the following axioms:

(B1) $\mathfrak{B} \neq \emptyset$.
(B2) For every $B_1, B_2 \in \mathfrak{B}; B_1 \not\subset B_2$.
(B3) For every $B_1, B_2 \in \mathfrak{B}$ and for every pair of ideals I_1, I_2 of E such that $I_1 \subset B_1, B_2 \subseteq I_2, I_1 \subseteq I_2$, there exists $B \in \mathfrak{B}$ such that $I_1 \subseteq B \subseteq I_2$.

Paper [8] further proves that all the bases of $\mathcal{M}$ have the same cardinality.

Similarly to usual matroids, it is possible to define a poset matroid via its independent sets. The family $\mathfrak{I}$ of all independent sets of a poset matroid $\mathcal{M}$ on the partially ordered set P satisfies the following properties:

(I1) $\mathfrak{I}$ is a nonempty collection of ideals.
(I2) Let $I_1, I_2 \in \mathcal{I}(P)$ be such that $I_2 \in \mathfrak{I}$ and $I_1 \subseteq I_2$, then $I_1 \in \mathfrak{I}$.
(I3) For every $I_1, I_2 \in \mathfrak{I}$ with $|I_1| < |I_2|$, there exists $y \in \mathrm{Min}(I_2 \backslash I_1)$ such that $I_1 \cup y \in \mathfrak{I}$.

The *dual poset matroid* $\mathcal{M}^\perp$ is defined in a way similar to the classical case: namely, its set of bases is the set of filters that are complements of the bases of $\mathcal{M}$, i.e. $\mathfrak{B}(\mathcal{M}^\perp) = \{F : F^c \in \mathfrak{B}(\mathcal{M})\}$ [8]. For $\mathcal{M}^\perp$ the definition of independent sets has to be modified by replacing the minimal elements of $I_2 \backslash I_1$ with the set of maximal elements.

Given a poset matroid $\mathcal{M}$, define the *rank function* as follows:

$$\rho : 2^E \to \mathbb{N} \cup \{0\}, \quad \rho(A) = \max\{|I| : I \subset A, I \in \mathfrak{I}\}, A \in \mathcal{I}(P). \tag{33}$$

The rank function of $\mathcal{M}^\perp$ is defined analogously. The basic relation (13) between the rank functions of $\mathcal{M}$ and $\mathcal{M}^\perp$, that was proved earlier by linear-algebraic arguments, can be easily proved from the first principles without appealing to the vector space representations.

Proposition 3.1. *Let $\bar{A} \in \mathcal{I}(P^\perp), A^c = E \backslash \bar{A}$. We have*

$$\rho^\perp \bar{A} = \rho A^c + |\bar{A}| - \rho E. \tag{34}$$

Proof : The proof follows by verifying that the standard arguments (e.g., [30, pp.72-73]) hold in the case of ordered matroids. ∎

Definition: Let $\mathcal{M}$ be a poset matroid. Define the multivariate Tutte polynomial $Z_{\mathcal{M}}(q,z)$ of $\mathcal{M}$ by relation (10), where ρ is the rank function (33). The Tutte polynomial $Z^\perp$ for the dual matroid $\mathcal{M}^\perp$ is defined analogously. These polynomials can be written in an equivalent form given in (15) using relations (16).

Observe that the duality relations (12) and (17) are proved based on relation (34). In other words, the following proposition holds true.

Proposition 3.2. *Let $\mathcal{M}$ and $\mathcal{M}^\perp$ be a pair of mutually dual poset matroids and let $T_{\mathcal{M}}(x, y_1, \dots, y_r)$ be the Tutte polynomial of $\mathcal{M}$ defined in* (15)*. Then the Tutte polynomial of $\mathcal{M}^\perp$ satisfies relation* (17)*.*

Similarly to the classical case, evaluations of $T(x,y)$ count objects (bases, independent sets, spanning sets, etc.) in $\mathcal{M}$. Indeed, the following statement follows from (15) by direct evaluation.

Proposition 3.3. *Let $\mathcal{M}$ be a poset matroid on P. We have*

$$\begin{aligned} T(2,2,\dots,2,2) &= (r+1)^n \\ T(1,2,\dots,2,1) &= |\mathfrak{B}| \\ T(2,2,\dots,2,1) &= |\mathfrak{I}| \\ T(1,2,\dots,2,2) &= |\{\text{spanning sets of } \mathcal{M}\}| \end{aligned}$$

($A \in \mathcal{I}(P)$ is spanning in $\mathcal{M}$ if $\rho A = \rho E$).

Of course, the results of this section are very simple. At the same time, they show that defining the Tutte polynomial for poset matroids is possible for the case of the NRT poset, and indicate that $T(x,y)$ depends on $r+1$ variables. Defining similar invariants for more general poset matroids remains an open problem [8]. It might be possible to pursue this connection using the more general definition of the rank function in [8]; however we will not do it here because poset matroids are not the main subject of this paper.

Ordered Linear Codes: In the classical case every linear subspace over $\mathbb{F}_q$ (a code) represents a matroid on the set of code's coordinates. This connection generally does not hold for poset matroids and ordered codes because not all the independent subsets of columns of code's generator matrix correspond to independent sets of the matroid. One exception is given by the class of ordered MDS codes. As remarked earlier, an ordered $[N,k,d]$ linear code $\mathcal{C}$ is MDS if $d = N-k+1$. Equivalently, $\mathcal{C}$ is MDS if any $N-k$ left-adjusted columns of the parity-check matrix of $\mathcal{C}$ are linearly independent. If $\mathcal{C}$ is MDS in P, then the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ is MDS with respect to $P^\perp$ [14].

A poset matroid $\mathcal{M}$ is called *k-uniform* if every ideal of size k is a base. We claim that a pair of linear mutually dual ordered MDS codes $\mathcal{C}, \mathcal{C}^\perp$ represents a pair of mutually dual uniform poset matroids $\mathcal{M}, \mathcal{M}^\perp$. Indeed, let G be a $k \times N$ generator matrix of $\mathcal{C}$. Since $\mathcal{C}^\perp$ is MDS with respect to the dual order $P^\perp$, every k right-adjusted columns of G are linearly independent, and every subset of $k+1$ right-adjusted columns has rank k. This means that every filter $I \in \mathcal{I}(P^\perp)$ of size k forms an independent subset with respect to the rank function $\rho(G(\cdot))$, and that k is the maximum size of an independent subset. Therefore, the set of all filters (ideals $I \in \mathcal{I}(P^\perp), |I| = k$) forms the set of bases of a uniform matroid $\mathcal{M}^\perp$. Similarly, all the ideals $I \in \mathcal{I}(P)$ of size $N-k$ define the set of bases of an $(N-k)$-uniform matroid $\mathcal{M}$.

4. Linear ordered codes and information transmission

Poset metrics are motivated in part by transmission over parallel channels in which the noise levels are coordinated in the sense that if in a given time slot, a link is exposed to high noise, then all the lower-numbered links also experience high levels of noise [35, 17]. In this section we introduce a simple channel model that allows one to formalize the connection between ordered codes and some standard information-theoretic results.

4-A. Ordered symmetric channel.

A discrete memoryless communication channel is a stochastic map $W : \mathcal{X} \to \mathcal{Y}$, where the finite sets $\mathcal{X}$ and $\mathcal{Y}$ model the input and the output alphabets of the channel. A symbol $x \in \mathcal{X}$ transmitted over the channel is received at the output with probability $W(y|x), y \in \mathcal{Y}$. One of the most important channel models in the theory of linear codes is the q-ary symmetric channel. Assume that $\mathcal{X} = \mathcal{Y} = \mathbb{F}_q$, and $W(y|x) = (1-\varepsilon)\mathbb{1}_{\{y=x\}} + \frac{\varepsilon}{q-1}\mathbb{1}_{\{y\neq x\}}$.

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a linear code used for transmission over the channel W. A codeword $x = (x_1,\dots,x_N) \in \mathcal{X}^N$ is transmitted from the input to the output by applying the mapping W coordinatewise, so that the vector received at the output is $y = (y_1,\dots,y_N)$, where each value y_i is sampled from the distribution $W(\cdot|x_i)$. The Hamming distance plays an important role in the analysis of transmission over the q-ary symmetric channel since, given y, the most probable transmitted codeword is also the one closest to y by the Hamming distance.

Switching to the case of ordered codes, let us assume that one use of the channel corresponds to transmission of a vector $\boldsymbol{x} \in \mathbb{F}_q^r$ over r parallel links. Let $\varepsilon = (\varepsilon_0, \varepsilon_1, \dots, \varepsilon_r)$, where $0 \le \varepsilon_i \le 1$ for all i and $\sum_i \varepsilon_i = 1$. Let $W_r : \mathbb{F}_q^r \to \mathbb{F}_q^r$ be a

memoryless vector channel defined by

$$W_r(y|x) = \begin{cases} \varepsilon_0 & \text{if } y = x \\ \frac{\varepsilon_i}{q^{i-1}(q-1)} & \text{if } d_P(x,y) = i, 1 \le i \le r. \end{cases}$$

Every row of the matrix of transition probabilities $W_r(y|x)$ contains ε_0 and $q^{i-1}(q-1)$ entries of the form $\frac{\varepsilon_i}{q^{i-1}(q-1)}$ for all $i = 1, \dots, r$, and the same is true for every column. Therefore, the channel W_r is symmetric in the sense of [12, p.97]. The channel can be also thought of as a set of dependent parallel symmetric channels because the conditional probability of error in symbol $x_j, 1 \le j \le r-1$ depends on the values of errors in higher-numbered symbols within the same block of r symbols.

Below we assume that

$$\varepsilon_0 > \frac{\varepsilon_1}{q-1} > \cdots > \frac{\varepsilon_r}{q^{r-1}(q-1)}. \tag{35}$$

This assumption accounts for the fact that a correct transmission has higher probability than an error.

The shape distribution of a linear code $\mathcal{C} \subset \mathbb{F}_q^N, N = nr$ characterizes the performance of the code on the channel considered. By linearity we can assume that the input vector is $x = 0$. Suppose that the vector received after n uses of the channel is $y \in \mathbb{F}_q^N, \mathrm{shape}(y) = e$ and compute the transition probability from 0 to y :

$$\begin{aligned} W_r(y|0) &= \varepsilon_0^{e_0} \left(\frac{\varepsilon_1}{q-1}\right)^{e_1} \cdots \left(\frac{\varepsilon_r}{q^{r-1}(q-1)}\right)^{e_r} = \varepsilon^e \left(\frac{q-1}{q}\right)^{-|e|} q^{-\sum_i i e_i} \\ &= \frac{\varepsilon_0^{e_0}}{q^{w_P(y)}} \prod_{i=1}^r \left(\frac{q\varepsilon_i}{q-1}\right)^{e_i}. \end{aligned}$$

We conclude that the shape of the error vector determines the transition probability. The ordering of shape vectors defined in (20) also suffices to claim an inequality for probabilities of channel outputs. Namely, if $y, z \in \mathbb{F}_q^N$ are two vectors with $\mathrm{shape}(y) = e$ and $\mathrm{shape}(z) = f$, and $f \le e$ then $W_r(y|0) \le W_r(z|0)$ with equality if (but not only if) $f = e$. This is confirmed by an elementary calculation, omitted here.

The Shannon capacity $\mathscr{C}(W_r)$ of the channel $W_r(\varepsilon_1, \dots, \varepsilon_r)$ is also easy to find (see [12] for the definition of capacity and the associated quantities such as entropy and mutual information).

Proposition 4.1. *The capacity of $W_r(\varepsilon)$ equals*

$$\mathscr{C}(W_r(\varepsilon)) = r(1 - h_{q,r}(\varepsilon)), \tag{36}$$

where

$$h_{q,r}(\varepsilon) \triangleq \frac{1}{r}\Big(H_q(\varepsilon) + \sum_{i=1}^r \varepsilon_i \log_q(q^{i-1}(q-1))\Big)$$

and $H_q(\varepsilon) = -\sum_{i=0}^r \varepsilon_i \log_q \varepsilon_i$.

Proof : This is shown by a straightforward calculation. We have:

$$\mathscr{C}(W_r(\varepsilon)) = \max_{P_X} I(X;Y) = \max_{P_X}(H(Y) - H(Y|X)),$$

where P_X is a distribution on $\mathbb{F}_q^r$, $H(Y)$ and $H(Y|X)$ denote the entropy and conditional entropy of the channel output Y, and $I(X;Y)$ is the mutual information between X and Y. Since the channel is symmetric, the maximum is attained on uniform P_X, so X is uniformly distributed on $\mathbb{F}_q^r$, and therefore, Y is also uniform. Thus, $H(Y)$ above equals r. Furthermore,

$$\begin{aligned} H(Y|X) &= \sum_{x,y} P_{XY}(x,y) \log_q \frac{1}{P_{Y|X}(y|x)} = -\varepsilon_0 \log_q \varepsilon_0 - \sum_{i=1}^r \varepsilon_i \log_q \frac{\varepsilon_i}{q^{i-1}(q-1)} \\ &= H_q(\varepsilon) + \sum_{i=1}^r \varepsilon_i \log_q(q^{i-1}(q-1)). \end{aligned}$$

This gives (36). ∎

Observe that the quantity $h_{q,r}(\varepsilon)$ expresses the exponent of the number of vectors of shape $e = (\varepsilon_1 n, \ldots, \varepsilon_r n)$ in the space $\mathbb{F}_q^N$ (the volume of the "shape-sphere") [35]. Thus the capacity is attained by codes such that the spheres around the codewords of shape εn are almost disjoint (i.e., intersect by a vanishing proportion of their volume). In particular, this can be shown to be true with high probability for a code spanned by k randomly chosen vectors in the space $\mathbb{F}_q^N$ for any $k < \mathscr{C}(W_r)n$. We refer to [33] for a more detailed discussion of information transmission over the channel W_r.

4-B. **The wiretap channel and higher weights of linear ordered codes.** Here we return to the concept of higher weights considered in Sect. 2-C. While it has been mostly studied in geometric context, its original motivation comes from a combinatorial model of information transmission in a system with an eavesdropper [41]. We will show that this model can be modified to apply to ordered codes, leading to an analogous connection between higher (ordered) weights of linear ordered codes.

Suppose that the transmission of information between two parties X and Y is conducted using an $[N = nr, N - k]$ linear ordered code $\mathcal{C}$. The transmission can be overheard by a third party Z that can access only a subset of coordinates. We assume that the transmission uses a combinatorial version of the ordered symmetric channel described in the previous section so that every r-tuple of symbols of $\mathbb{F}_q$ is transmitted over r parallel links (see (1)). Suppose that Z requires progressively greater resources to access higher-numbered links in a given time slot, so that the subsets of coordinates accessible by Z are limited to ideals of the order P. The message space of X is a k-dimensional linear space over $\mathbb{F}_q$. Note that the quotient space $\mathbb{F}_q/\mathcal{C}$ contains exactly q^k cosets. To transmit a message $m \in \mathbb{F}_q^k$, X maps it on a coset and then transmits an N-symbol vector x chosen from this coset randomly and uniformly. This transmission scheme is analogous to the scheme used in classical case of the wiretap channel [31, 41] (similar schemes are also used in a number of other information theoretic primitives [12]).

Suppose that Z has access to a subset x_I of coordinates of x, where $I \in \mathcal{I}(P), |I| = s$ is an order ideal. This gives Z some information about the message m. To formalize this, let X be a uniform random message, and let Z be the observation. Denote by $\Delta(I) := H(X|Z)$ the conditional entropy of the message given Z. This quantity represents the residual uncertainty of Z about m and is called equivocation. Let $\Delta_s := \min_{I \in \mathcal{I}(P):|I|=s} \Delta(I)$ be the minimum equivocation over the choice of the ideal of size s.

Proposition 4.2.

$$\Delta_s = \min_{I^c \in \mathcal{I}(P^\perp), |I^c| = n-s} \operatorname{rk} H(I).$$

Proof : Let $h_i, i = 1, \ldots, n$ be the columns of H, and let $I \in \mathcal{I}(P), |I| = s, I^c := E \backslash I$. The entire message m would be known if Z knew the coset, or, which is the same, the vector $z := Hx^T$ (called the syndrome of x). As it is, the known part of the syndrome is $\sum_{i \in I} h_i x_i$, and therefore

$$z - \sum_{i \in I} h_i x_i = \sum_{i \in I^c} h_i x_i.$$

The vector on the left is contained in the subspace spanned by the columns $h_i, i \in I^c$, and so the equivocation about its value equals $\operatorname{rk}(H(I^c))$. ∎

Suppose we are given s and the associated equivocation Δ_s. Define the ith higher ordered weight of the code $\mathcal{C}$ as follows [5]:

$$d_i(\mathcal{C}) := \min\{\langle \operatorname{supp}(\mathcal{D}) \rangle : \mathcal{D} \text{ is an } i\text{-dimensional subcode of } \mathcal{C}\}.$$

It is easy to see [5, Lemma 2] that $\mathcal{D}$ is this definition can be taken to be supported on the entire ideal $\langle \operatorname{supp}(\mathcal{D}) \rangle$. Therefore we immediately conclude that

$$d_{n-s-\Delta_s}(\mathcal{C}^\perp) \leq n - s < d_{n-s-\Delta_s+1}(\mathcal{C}^\perp).$$

This implies that the change of the equivocation Δ_s is determined by the higher weights of the dual code $\mathcal{C}^\perp$. This establishes a link between higher weights and the ordered wiretap channel described above much in the same way as this is done in the classical case.

It is also possible to define a probabilistic version of the ordered wiretap channel where the links between X and Y and X and Z are described by ordered symmetric channels, and design a scheme based on ordered linear codes that attains its secrecy capacity. We refer to [33] for more details on these results.

REFERENCES

[1] A. Ashikhmin and A. Barg, *Binomial moments of the distance distribution: Bounds and applications*, IEEE Trans. Inform. Theory **45** (1999), no. 2, 438–452.

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

[3] A. Barg, L. Felix, M. Firer, and M. Spreafico, *Linear codes on posets with extension property*, Discrete Math. **317** (2014), 1–13.

[4] A. Barg and P. Purkayastha, *Bounds on ordered codes and orthogonal arrays*, Mosc. Math. J. **9** (2009), no. 2, 211–243.

[5] _____, *Near MDS poset codes and distributions*, Error-Correcting Codes, Cryptography and Finite Geometries (A. Bruen and D. Wehlau, eds.), Providence, RI: AMS, 2010, pp. 135–147.

[6] A. Barg and M. Skriganov, *Association schemes on general measure spaces and zero-dimensional Abelian groups*, Adv. Math. **281** (2015), 142–247.

[7] M. Barnabei, G. Nicoletti, and L. Pezzoli, *The symmetric exchange property for poset matroids*, Adv. Math. **102** (1993), no. 2, 230–239.

[8] _____, *Matroids on partially ordered sets*, Adv. in Appl. Math. **21** (1998), no. 1, 78–112.

[9] T. Britz, *Code enumerators and Tutte polynomials*, IEEE Trans. Inform. Theory **56** (2010), no. 9, 4350–4358.

[10] R. A. Brualdi, J.S. Graves, and K. M. Lawrence, *Codes with a poset metric*, Discrete Math. **147** (1995), no. 1-3, 57–72.

[11] H. Cohn and Y. Zhao, *Energy-minimizing error-correcting codes*, IEEE Trans. Inform. Theory **60** (2014), no. 12, 7442–7450.

[12] I. Cziszar and J. Körner, *Information theory*, 2nd ed., Cambridge Univ. Press, 2011.

[13] S. T. Dougherty and M. M. Skriganov, *MacWilliams duality and the Rosenbloom-Tsfasman metric*, Mosc. Math. J. **2** (2002), no. 1, 81–97, 199.

[14] _____, *Maximum distance separable codes in the ρ metric over arbitrary alphabets*, J. Algebraic Combin. **16** (2002), 71–81.

[15] F.D.J. Dunstan, A.W. Ingleton, and D. J. A.. Welsh, *Supermatroids*, Proc. Conf. Combin. Math. (Oxford, 1972), Inst. Math. Appl., 1972, pp. 72–122.

[16] U. Faigle, *Geometries on partially ordered sets*, J. Combin. Theory Ser. B **28** (1980), 26–51.

[17] A. Ganesan and P. O. Vontobel, *On the existence of universally decodable matrices*, IEEE Trans. Inform. Theory **53** (2007), no. 7, 2572–2575.

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

[19] T. Helleseth, T Kløve, and J. Mykkeltveit, *The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/n)$*, Discrete Math. **18** (1977), 179–211.

[20] J. Y. Hyun and H. K. Kim, *Maximum distance separable poset codes*, Des. Codes Cryptogr. **28** (2008), no. 3, 247–261.

[21] N. Kashyap, *A decomposition theory for binary linear codes*, IEEE Trans. Inform. Theory **54** (2008), no. 7, 3035–3058.

[22] G. L. Katsman and M. A. Tsfasman, *Spectra of algebraic-geometric codes*, Probl. Inf. Transm. **23** (1987), no. 4, 19–34.

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

[24] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1991.

[25] W. J. Martin and D. R. Stinson, *Association schemes for ordered orthogonal arrays and (t, m, s)-nets*, Canad. J. Math. **51** (1999), no. 2, 326–346.

[26] J. L. Massey and S. Serconek, *Linear complexity of periodic sequences: a general theory*, Advances in cryptology—CRYPTO '96 (Santa Barbara, CA), Lecture Notes in Comput. Sci., vol. 1109, Springer, Berlin, 1996, pp. 358–371.

[27] H. Niederreiter, *Low-discrepancy point sets*, Monatsh. Math. **102** (1986), no. 2, 155–167.

[28] _____, *A combinatorial problem for vector spaces over finite fields*, Discrete Math. **96** (1991), no. 3, 221–228.

[29] R. R. Nielsen, *A class of Sudan-decodable codes*, IEEE Trans. Inform. Theory **46** (2000), no. 4, 1564–1572.

[30] J. G. Oxley, *Matroid theory*, Oxford University Press, Oxford e.a., 1992.

[31] L. Ozarow and A. Wyner, *Wire-tap channel II*, AT&T Bell Labs Techn. J. **63** (1984), no. 10, 2135–2157.

[32] L. Panek, M. Firer, H. K. Kim, and J. Y. Hyun, *Groups of linear isometries on poset structures*, Discrete Math. **308** (2008), no. 18, 4116–4123.

[33] W. Park and A. Barg, *Linear ordered codes, shape enumerators, and parallel channels: Extended abstract*, Proc. 48th Annual Allerton Conf. Commun. Control Comput., Monticello, IL, 2010, pp. 361–367.

[34] _____, *The ordered Hamming metric and ordered symmetric channels*, Proc. 2011 IEEE Internat. Sympos. Inform. Theory, St.Petersburg, Russia, 2011, pp. 2194–2198.

[35] M. Yu. Rosenbloom and M. A. Tsfasman, *Codes for the m-metric*, Probl. Inf. Transm. **33** (1997), no. 1, 45–52.

[36] M. M. Skriganov, *Coding theory and uniform distributions*, Algebra i Analiz **13** (2001), no. 2, 191–239, English translation in *St. Petersburg Math. J.* vol. 13 (2002), no. 2, 301–337.

[37] A. D. Sokal, *The multivariate Tutte polynomial (alias Potts model) for graphs and matroids*, Surveys in combinatorics 2005 (B. Webb, ed.), London Math. Soc. Lecture Note Ser., vol. 327, Cambridge Univ. Press, Cambridge, 2005, pp. 173–226.

[38] S. Tavildar and P. Viswanath, *Approximately universal codes over slow-fading channels*, IEEE Trans. Inform. Theory **52** (2006), no. 7, 3233–3258.

[39] M. Tsfasman, S. Vlăduţ, and D. Nogin, *Algebraic geometric codes: Basic notions*, Mathematical Surveys and Monographs, vol. 139, American Mathematical Society, Providence, RI, 2007.

[40] M. A. Tsfasman and S. G. Vlăduţ, *Geometric approach to higher weights*, IEEE Trans. Inform. Theory **41** (1995), 1564–1588.

[41] V. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Inform. Theory **37** (1991), no. 5, 1412–1418.

[42] D. J. A. Welsh, *Matroid theory*, Academic Press, London, 1976.

[43] M. Wild, *Weakly submodular rank functions, supermatroids, and the flat lattice of a distributive supermatroid*, Discrete Math. **308** (2008), 999–1017.