Codes and Projective Multisets

Stefan Dodunekov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
8 G. Bontchev Str.
1113 Sofia, Bulgaria
e-mail: stedo@moi2.math.acad.bg

Juriaan Simonis
Delft University of Technology
Faculty of Information Technology and Systems
Department of Technical Mathematics and Informatics
P.O. Box 5031
2600 GA Delft, the Netherlands
e-mail: J.Simonis@twi.tudelft.nl

Submitted: December 25, 1997; Accepted: July 27, 1998.

Abstract

The paper gives a matrix-free presentation of the correspondence between full-length linear codes and projective multisets. It generalizes the Brouwer-Van Eupen construction that transforms projective codes into two-weight codes. Short proofs of known theorems are obtained. A new notion of self-duality in coding theory is explored.

94B05, 94B27, 51E22.

1 Introduction

We start by describing the main idea in an informal way. Let G be a generator matrix of a q-ary linear $[n, k, d]$-code $\mathcal{C}$, and let $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_n \in \mathbb{F}_q^k$ be the columns of G. Suppose that none of the $\mathbf{g}_i$'s is the zero vector. (We say that the code $\mathcal{C}$ is of *full length.*) Then each $\mathbf{g}_i$ determines a point $[\mathbf{g}_i]$ in the projective space $\Pi := \mathbb{P}(\mathbb{F}_q^k)$. If the $\mathbf{g}_i$ happen to be pair-wise independent, then $X := \{[\mathbf{g}_1], [\mathbf{g}_2], \dots, [\mathbf{g}_n]\}$ is a set of n points in Π. When dependence occurs, we interpret X as a *multiset* and count each point with the appropriate multiplicity. Different generator matrices yield projectively equivalent codes. In fact, we have a bijective correspondence between the equivalence classes of full-length q-ary linear codes and the projective equivalence classes of multisets in finite Desarguesian projective spaces. It is easy to recover minimum distance d of $\mathcal{C}$ from X. A nonzero codeword $\mathbf{c} := (c_1, c_2, \dots, c_n) \in \mathcal{C}$ corresponds to the hyperplane H_c in Π with equation $c_1\xi_1 + c_2\xi_2 + \cdots + c_n\xi_n = 0$ and the weight of $\mathbf{c}$ equals the size of $X \cap (\Pi \setminus H_{\mathbf{c}})$. So $d = n - \min |X \cap H|$, where H runs through the hyperplanes of Π.

The first one to use this relationship between linear codes and projective multisets was Slepian [27], who used the term *modular representation.* See also [25]. Delsarte, Hill and others studied the relation between projective two-weight codes and projective (n, k, h_1, h_2) sets. These are subsets of size n of $\mathbb{P}(\mathbb{F}_q^k)$ with the property that every hyperplane is met in h_1 points or h_2 points. Two-weight codes are surveyed in Calderbank and Cantor's paper [6].

Subsets of a finite projective space that have a small intersection with all subspaces of a given dimension have been extensively studied by finite geometers. In [17], Hirschfeld and Storme survey the known results with respect to so-called $(n; r, s; N, q)$-*sets.* These are spanning subsets $K \subset \mathbb{P}(\mathbb{F}_q^{N+1})$ of size n and such that all s-dimensional projective subspaces of $\mathbb{P}(\mathbb{F}_q^{N+1})$ intersect K in at most s points. So $(n; k-2, n-d; k-1, q)$-sets correspond to q-ary linear $[n, k, d]$-codes for which the columns of any generator matrix are pair-wise independent. Other good references are the survey papers by Hill [16] and Landgev [22].

Yet another terminology has been introduced by Hamada and Tamari in [13]. They defined a *minihyper* (*maxhyper*) $\{f, m; t, q\}$ to be a multiset w in $\mathbb{P}(\mathbb{F}_q^{t+1})$ of size f and such that all hyperplanes intersect w in at most (at least) m points. Hence there is a bijective correspondence between the $\{n, n-d; k-1, q\}$ maxhypers that span $\mathbb{P}(\mathbb{F}_q^k)$ and the (equivalence classes) of q-ary linear $[n, k, d]$-codes. A recent survey of results on minihypers and their relation to codes meeting the Griesmer bound can be found in [14].

Goppa's work [12] initiated a constant flow of contributions to coding theory by algebraic geometers. Of course, the natural setting here is the correspondence between linear codes and projective multisets. A good example is the book [32]. where the term "projective system" is used. As a matter of fact, in Problem 1.1.9 of [32] the reader is invited to "Rewrite existing books on coding theory in terms of projective systems". The present paper can be regarded as a first step towards this goal.

Quite recently, Brouwer and Van Eupen published a gem of a paper, [5], in which they used a correspondence between projective codes and two-weight codes to construct optimal codes and to prove the uniqueness of certain codes. Their construction, a generalization of an old result on projective two-weight codes (cf. [15], Th. 8.7, or [6], Th. 5.2), transforms subsets of a finite projective space Π into multisets of the dual space Π^*. Although mainly dual transforms of "degree" one are considered, the final section of their paper gives a more general construction in which the degree of the dual transform is arbitrary. Our paper describes the dual transform in its full generality.

Outline of the paper

Section 2 contains a concise introduction to algebraic coding theory and fixes notation. In particular, we introduce the *reduced distribution matrix* of a code, a convenient notion in our treatment of the dual transform. In Section 3, we list some basic properties of projective multisets. The notion of *lifting* is introduced. We need this notion in Proposition 2 to repair a minor flaw in [5]. The section also contains a matrix-free presentation of the correspondence between full-length linear codes and projective multisets. Section 4 is devoted to the dual transform of multisets. We give simple expresssions of the basic parameters of the dual transform in terms of the reduced distribution matrix of the dual of the original code. Section 5 treats dual transforms of degree one. To demonstrate the effectiveness of this concept, we give short proofs of a theorem of Ward, a theorem of Bonisoli and the uniqueness of the generalized MacDonald codes. Finally, Section 6 explores a new kind of duality in coding theory. A code $\mathcal{C}$ is said to be σ-self-dual if its dual transform $\mathcal{C}^\sigma$ is equivalent to $\mathcal{C}$. We give a list of examples and derive strong conditions in the case of transforms of degree one.

2 Codes

2.1 Basic definitions

Let $\mathbb{F}_q$ be the finite field of q elements and let S be a finite set of size n.

Definition 1 *The* standard vector space $\mathbb{F}_q^S$ *over $\mathbb{F}_q$ is the $\mathbb{F}_q$-vector space of the mappings*

$$\mathbf{x} : S \to \mathbb{F}_q .$$

(If $S := \{1, 2, \ldots , n\}$, we usually write $\mathbb{F}_q^n$ for $\mathbb{F}_q^S$.)
The value of $\mathbf{x} \in \mathbb{F}_q^S$ in $s \in S$ is denoted by x_s.

The *natural basis* $\{\mathbf{e}_s \mid s \in S\}$ of $\mathbb{F}_q^S$ is defined by

$$(\mathbf{e}_s)_t := \begin{cases} 1 & \text{if} \quad s = t, \\ 0 & \text{if} \quad s \neq t. \end{cases}$$

So the dimension of $\mathbb{F}_q^S$ is equal to n.

Definition 2 *Let S, S' be two sets of size n, and let $\{\mathbf{e}_s \mid s \in S\}$, $\{\mathbf{e}'_{s'} \mid s' \in S'\}$ be the natural bases of $\mathbb{F}_q^S$, $\mathbb{F}_q^{S'}$ respectively. A linear isomorphism $\mu : \mathbb{F}_q^S \to \mathbb{F}_q^{S'}$ is said to be* monoidal *if nonzero elements $a_s \in \mathbb{F}_q$ and a bijection $\sigma : S \to S'$ exist such that $\mu(\mathbf{e}_s) = a_s \mathbf{e}'_{\sigma(s)}$ for all $s \in S$.*

Definition 3 *A q-ary* (linear) code $\mathcal{C}$ *of* length n *and* dimension k *is a k-dimensional linear subspace of the n-dimensional standard vector space $\mathbb{F}_q^S$. Two codes $\mathcal{C} \subseteq \mathbb{F}_q^S$, $\mathcal{C}' \subseteq \mathbb{F}_q^{S'}$ are said to be* equivalent *if a monoidal isomorphism $\mu : \mathbb{F}_q^S \to \mathbb{F}_q^{S'}$ exists such that $\mu(\mathcal{C}) = \mathcal{C}'$.*

2.2 Weight and distance

The *Hamming weight* $|\mathbf{x}|$ of a vector $\mathbf{x} \in \mathbb{F}_q^S$ is the size of its support:

$$|\mathbf{x}| := |\{s \mid s \in S \wedge x_s \neq 0\}|.$$

The Hamming weight is a norm on the vector space $\mathbb{F}_q^S$. The induced metric, with distance function

$$d(\mathbf{x}, \mathbf{y}) := |\mathbf{x} - \mathbf{y}|, \;\; \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^S,$$

is called the *Hamming metric*. Note that the monoidal isomorphisms are precisely the linear isomorphisms that leave the Hamming weight invariant. Hence equivalent codes are isometric.

Definition 4 *The* weight distribution *of a code $\mathcal{C} \subseteq \mathbb{F}_q^S$ is the sequence*

$$A_0(\mathcal{C}), A_1(\mathcal{C}), \ldots, A_n(\mathcal{C})$$

defined by

$$A_i(\mathcal{C}) := |\{\mathbf{c} \mid \mathbf{c} \in \mathcal{C} \wedge |\mathbf{c}| = i\}|, \;\; i = 0, 1, \ldots, n.$$

The weight set *of $\mathcal{C}$ is the set*

$$W_{\mathcal{C}} := \{i \mid i \in \{1, 2, \ldots, n\} \wedge A_i(\mathcal{C}) \neq 0\}$$

and the minimum weight *of $\mathcal{C}$ is the integer*

$$d_{\mathcal{C}} := \min W_{\mathcal{C}}.$$

Let

$$D_i(\mathcal{C}, \mathbf{x}) := |\{\mathbf{c} \mid \mathbf{c} \in \mathcal{C} \wedge d(\mathbf{x}, \mathbf{c}) = i\}|$$

be the number of codewords at distance i from $\mathbf{x} \in \mathbb{F}_q^S$.

Definition 5 (Cf. [8]) *The* distribution matrix *of $\mathcal{C}$ is the $q^n \times (n+1)$ matrix $\mathbf{D}$ parametrized by $\mathbb{F}_q^S \times \{0, 1, \ldots, n\}$ having $D_i(\mathcal{C}, \mathbf{x})$ as its $(\mathbf{x}, i)$ entry.*

The linearity of $\mathcal{C}$ immediately implies that $D_i(\mathcal{C}, \mathbf{x}) = D_i(\mathcal{C}, \mathbf{x} + \mathbf{c})$ for all $c \in \mathcal{C}$. In other words, the rows of $\mathbf{D}$ are constant on the cosets of $\mathcal{C}$. Moreover, $D_i(\mathcal{C}, a\mathbf{x}) = D_i(\mathcal{C}, \mathbf{x})$ for all $a \in \mathbb{F}_q \setminus \{0\}$. Hence the following definition makes sense.

Definition 6 *The* reduced distribution matrix *of $\mathcal{C}$ is the $\frac{q^{n-k}-1}{q-1} \times (n+1)$ matrix $\bar{\mathbf{D}}$ parametrized by $\mathbb{P}(\mathbb{F}_q^S/\mathcal{C}) \times \{0, 1, \ldots, n\}$ and having $D_i(\mathcal{C}, \mathbf{x}) - D_i(\mathcal{C}, \mathbf{o})$ as its $([\bar{\mathbf{x}}], i)$ entry. (Here $\bar{\mathbf{x}}$ denotes the vector in $\mathbb{F}_q^S/\mathcal{C}$ corresponding to the coset $\mathbf{x} + \mathcal{C}$ and $[\bar{\mathbf{x}}]$ denotes the projective point determined by $\bar{\mathbf{x}}$ in the projective space $\mathbb{P}(\mathbb{F}_q^S/\mathcal{C})$ over $\mathbb{F}_q^S/\mathcal{C}$.) The $(i+1)$-st column of $\bar{\mathbf{D}}$ will be denoted by $\bar{\mathbf{D}}_i$.*

2.3 Dual codes

The standard inner product on $\mathbb{F}_q^S$ is defined by

$$\langle \mathbf{x}, \mathbf{y} \rangle := \sum_{s \in S} x_s y_s, \ \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^S.$$

Definition 7 *The* dual *of a code $\mathcal{C} \subseteq \mathbb{F}_q^S$ is the code*

$$\mathcal{C}^\perp := \{\mathbf{x} \mid \mathbf{x} \in \mathbb{F}_q^S \wedge \langle \mathbf{x}, \mathbf{c} \rangle = 0 \textit{ for all } \mathbf{c} \in \mathcal{C}\}.$$

The external distance *$t_\mathcal{C}$ of $\mathcal{C}$ is the size of the weight set of $\mathcal{C}^\perp$ and the* dual distance *of $\mathcal{C}$ is the minimum distance of $\mathcal{C}^\perp$. A code $\mathcal{C}$ is said to be* of full length *if $d_{\mathcal{C}^\perp} \geq 2$ and* projective *if $d_{\mathcal{C}^\perp} \geq 3$.*

The external distance of a code $\mathcal{C}$ gives information about its distribution matrix. In fact, Delsarte proved the

Theorem 1 ([8]) *The rank of the distribution matrix $\mathbf{D}$ of $\mathcal{C}$ is equal to $t_\mathcal{C} + 1$. In fact, the first $t_\mathcal{C} + 1$ columns of $\mathbf{D}$ are independent and the i-th column of $\mathbf{D}$ can be expressed in these columns by a linear relation that only depends on k, n, q, i and the weight set $W_{\mathcal{C}^\perp}$ of $\mathcal{C}^\perp$.*

In 1963, MacWilliams found a remarkable relation between the weight spectra of $\mathcal{C}$ and $\mathcal{C}^\perp$.

Theorem 2 ([23]) *For $i = 0, 1, \dots, n$, we have the identities*

$$\sum_{j=0}^{n} \binom{n-j}{i} A_j(\mathcal{C}) = q^{k-i} \sum_{j=0}^{n} \binom{n-j}{n-i} A_j(\mathcal{C}^\perp).$$

If we solve this system of equations for the $A_j(\mathcal{C})$, we find

$$A_i(\mathcal{C}) = q^{k-n} \sum_{j=0}^{n} K_i(j) A_j(\mathcal{C}^\perp), \tag{1}$$

with

$$K_i(j) := \sum_{m=0}^{i} (-1)^m (q-1)^{i-m} \binom{j}{m} \binom{n-j}{i-m}.$$

The $K_i(j)$ are polynomials of degree i in j, the so-called *Krawtchouk polynomials*, cf. [21]. A comprehensive description can be found in [24], pp. 129 ff., 150 ff.. We shall need the fact that the $K_i(j)$ satisfy the *orthogonality relations*

$$\sum_{j=0}^{n} K_l(j) K_j(i) = q^n \delta_{l,i}, \ l, i = 0, 1, \dots, n. \tag{2}$$

3 Projective multisets

3.1 Basic definitions

Let $\Pi := \mathbb{P}(\mathcal{V})$ be the projective space over a finite-dimensional $\mathbb{F}_q$-vector space $\mathcal{V}$, and let $\mathbb{N}$ denote the set of the nonnegative integers.

Definition 8 *A* projective multiset *in Π is a mapping $\gamma : \Pi \to \mathbb{N}$ of Π into $\mathbb{N}$. The* multiplicity *of a point $p \in \Pi$ in γ is the integer $\gamma(p)$. The* multiplicity set *of γ is the set*

$$M_\gamma := \operatorname{Im} \gamma.$$

If $M_\gamma \subseteq \{0, 1\}$, we identify γ with its support and call it a *set.*

Definition 9 *The* spanning space *of γ is the projective span*

$$\Sigma_\gamma := \langle \operatorname{supp}(\gamma) \rangle$$

of the support

$$\operatorname{supp}(\gamma) := \{p \mid p \in \Pi \wedge \gamma(p) \neq 0\}.$$

of γ in Π. The dimension *of γ is the integer*

$$k_\gamma := \dim \Sigma_\gamma + 1.$$

Definition 10 *Two projective multisets γ, γ' are said to be* equivalent *if a projective isomorphism $\varphi : \Sigma_\gamma \to \Sigma_{\gamma'}$ exists such that $\gamma = \gamma' \circ \varphi$.*

For example, any projective multiset $\gamma : \Pi \to \mathbb{N}$ is equivalent to the restriction $\gamma|_{\Sigma_\gamma}$ of γ to its spanning space.

We can extend the mapping γ to the *power set* of Π as follows.

Definition 11 *If $W \subseteq \Pi$ is any subset, then*

$$\gamma(W) := \sum_{p \in W} \gamma(p).$$

In particular, the integer

$$n_\gamma := \gamma(\Pi)$$

is called the length *of the multiset γ.*

3.2 Projective multisets and full-length codes

In Definition 7, we defined a full-length code to be a code with dual distance ≥ 2. This can be rephrased as follows: a code $\mathcal{C} \subseteq \mathbb{F}_q^S$ is of full length if and only if the natural basis $\{\mathbf{e}_s \mid s \in S\}$ does not intersect the dual code $\mathcal{C}^\perp$.

Definition 12 *Let $\mathcal{C} \subseteq \mathbb{F}_q^S$ be a full-length code, and let $\overline{\mathbf{e}_s}$ denote the image of the standard basis vector $\mathbf{e}_s$ under the quotient mapping $\mathbb{F}_q^S \to \mathbb{F}_q^S/\mathcal{C}^\perp$. Then the multiset*

$$\gamma_{\mathcal{C}} : \mathbb{P}(\mathbb{F}_q^S/\mathcal{C}^\perp) \to \mathbb{N}, \;\; p \mapsto |\{s \mid p = [\overline{\mathbf{e}_s}]\}|$$

is called the projective multiset induced by $\mathcal{C}$.

Remark 1 *The multiset induced by $\mathcal{C}$ can be identified with the (second) column $\bar{\mathbf{D}}_1$ of the reduced distribution matrix $\bar{\mathbf{D}}$ of $\mathcal{C}^\perp$.*

The length and dimension of a full-length code $\mathcal{C}$ are equal to the length and dimension of the induced multiset $\gamma_{\mathcal{C}}$. A full-length code $\mathcal{C}$ is *projective* if and only if the induced multiset $\gamma_{\mathcal{C}}$ is a *set.*

Proposition 1 *Any projective multiset is equivalent to a projective multiset induced by a code. Two induced multisets $\gamma_{\mathcal{C}}$, $\gamma_{\mathcal{C}'}$ are equivalent if and only if the codes $\mathcal{C}$, $\mathcal{C}'$ are equivalent.*

Proof. Let $\gamma : \Pi := \mathbb{P}(\mathcal{V}) \to \mathbb{N}$ be a projective multiset of dimension k and length n. Choose a list $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ of vectors $\mathbf{v}_i \in \mathcal{V}$ such that

$$\{[\mathbf{v}_1], [\mathbf{v}_2], \ldots, [\mathbf{v}_n]\} = \operatorname{supp}(\gamma)$$

and such that each point $p \in \Pi$ occurs in the list $([\mathbf{v}_1], [\mathbf{v}_2], \ldots, [\mathbf{v}_n])$ with multiplicity $\gamma(p)$. Consider the linear mapping $\varphi : \mathbb{F}_q^n \to \mathcal{V}$ fixed by $\varphi(\mathbf{e}_i) = \mathbf{v}_i$, $i = 1, 2, \ldots, n$. If we put $\mathcal{C} := \ker(\varphi)^\perp$, then $\gamma = \gamma_{\mathcal{C}}$. Secondly, if two full-length codes $\mathcal{C}$, $\mathcal{C}'$ are equivalent under a monoidal isomorphism $\mu : \mathbb{F}_q^S \to \mathbb{F}_q^{S'}$, then $\mu(\mathcal{C}^\perp) = \mathcal{C}'^\perp$. So the induced projective isomorphism $\tilde{\mu} : \mathbb{P}(\mathbb{F}_q^S/\mathcal{C}^\perp) \to \mathbb{P}(\mathbb{F}_q^{S'}/\mathcal{C}'^\perp)$ is well-defined. It obviously defines an equivalence between the projective multisets $\gamma_{\mathcal{C}}$ and $\gamma_{\mathcal{C}'}$.

Conversely, let $\mathcal{C} \subseteq \mathbb{F}_q^S$, $\mathcal{C}' \subseteq \mathbb{F}_q^{S'}$ be two full-length codes such that $\gamma_{\mathcal{C}}$ and $\gamma_{\mathcal{C}'}$ are equivalent. Let $\varphi : \mathbb{F}_q^S/\mathcal{C}^\perp \to \mathbb{F}_q^{S'}/\mathcal{C}'^\perp$ be a linear isomorphism such that the induced projective isomorphism $\tilde{\varphi} : \mathbb{P}(\mathbb{F}_q^S/\mathcal{C}^\perp) \to \mathbb{P}(\mathbb{F}_q^{S'}/\mathcal{C}'^\perp)$ is an equivalence between $\gamma_{\mathcal{C}}$ and $\gamma_{\mathcal{C}'}$. Then a bijection $\sigma : S \to S'$ exists such that $\tilde{\varphi}([\overline{\mathbf{e}_s}]) = [\overline{\mathbf{e}'_{\sigma(s)}}]$, $s \in S$. So nonzero elements $a_s \in \mathbb{F}_q$ exist such that $\varphi(\overline{\mathbf{e}_s}) = a_s\overline{\mathbf{e}'_{\sigma(s)}}$, $s \in S$. Now the monoidal isomorphism $\mu : \mathbb{F}_q^S \to \mathbb{F}_q^{S'}$ fixed by $\mu(\mathbf{e}_s) := a_s\mathbf{e}'_{\sigma(s)}$, $s \in S$, determines an equivalence between $\mathcal{C}$ and $\mathcal{C}'$. ■

Notation If γ is a projective multiset, then $\mathcal{C}_\gamma$ denotes any code such that the multiset induced by $\mathcal{C}_\gamma$ is equivalent to γ. The preceding proposition shows that the code $\mathcal{C}_\gamma$ exists and that it is determined by γ up to equivalence.

3.3 Quotient multisets

An interesting way to obtain new projective multisets from old ones is by considering *quotient spaces.* Let $\mathcal{U}$ be an $(m+1)$-dimensional linear subspace of the vector space $\mathcal{V}$,and let $L := \mathbb{P}(\mathcal{U})$ be the corresponding m-dimensional projective subspace of the projective space $\Pi := \mathbb{P}(\mathcal{V})$. Then the points of the projective space

$$\Pi/L := \mathbb{P}(\mathcal{V}/\mathcal{U})$$

can be identified with the $(m+1)$-dimensional projective subspaces M of Π such that $M \supset L$. More generally, the i-dimensional subspaces of Π/L correspond to the $(i+m+1)$-dimensional subspaces of Π that contain L. In particular, the dual space $(\Pi/L)^*$ will be identified with the subspace of Π^* consisting of all hyperplanes in Π that contain L.

Definition 13 *The* quotient multiset *of γ by L is the mapping $\gamma^L : \Pi/L \to \mathbb{N}$ defined by*

$$(\gamma^L)(M) := \gamma(M \setminus L), \;\; M \in \Pi/L.$$

Note that the dimension of γ^L is equal to $k_\gamma - \dim(L \cap \Sigma_\gamma) - 1$.

Remark 2 *Let $\gamma := \gamma_{\mathcal{C}}$ be the projective multiset induced by the code $\mathcal{C} \subseteq \mathbb{F}_q^S$. An m-dimensional subspace $L \subseteq \mathbb{P}(\mathbb{F}_q^S/\mathcal{C}^\perp)$ is of the form $\mathbb{P}(\mathcal{U})$, where $\mathcal{U}$ is a subspace of the vector space $\mathbb{F}_q^S/\mathcal{C}^\perp$. If $\mathcal{W}$ is the inverse image of $\mathcal{U}$ under the quotient mapping $\mathbb{F}_q^S \to \mathbb{F}_q^S/\mathcal{C}^\perp$, then $\mathcal{D} := \mathcal{W}^\perp$ is a subcode of codimension $m+1$ in $\mathcal{C}$ and $\gamma^L = \gamma_{\mathcal{D}}$. So the quotient multisets of γ correspond to the subcodes of $\mathcal{C}$ of the same codimension.*

3.4 Weights

Now we turn to the dual space Π^* of the projective space Π. (The points of Π^* are the hyperplanes $H \subset \Pi$.)

Definition 14 *The* weight function *of γ is the mapping*

$$\mu : \Pi^* \to \mathbb{N}, \;\; H \longmapsto \gamma(\Pi \setminus H).$$

The weight set *of γ is the set*

$$W_\gamma := \operatorname{Im}\mu \setminus \{0\}.$$

The minimum weight *of γ is the integer*

$$d_\gamma := \min W_\gamma.$$

The frequency *of a weight $w \in W_\gamma$ is the integer*

$$f_w(\gamma) := q^{\dim \Sigma_\gamma - \dim \Pi} |\mu^{-1}(w)|.$$

Note that $\mu^{-1}(0) = (\Pi/\Sigma_\gamma)^*$. Hence μ takes the value 0 if and only if $\dim\gamma < \dim\Pi + 1$.

Remark 3 *The weight distribution of $\mathcal{C}_\gamma$ and the frequencies $f_w(\gamma)$ of γ are related as follows:*

$$A_i(\mathcal{C}_\gamma) = \begin{cases} 1 & \text{for } i = 0, \\ 0 & \text{for } i \notin W_\gamma \cup \{0\}, \\ (q-1)f_w(\gamma) & \text{for } i \in W_\gamma. \end{cases}$$

Hence the weight set of $\mathcal{C}_\gamma$ is equal to W_γ. In particular, the minimum weight of $\mathcal{C}_\gamma$ is the minimum weight of γ.

Example 1 *Let the projective multiset γ be (the characteristic function of) the complement of a $(u-1)$-dimensional subspace L of a $(k-1)$-dimensional projective space Π. Denote by $\begin{bmatrix} k \\ j \end{bmatrix}$ the q-ary* Gaussian binomial coefficient. *If $u = 0$, then $\mathcal{C}_\gamma$ is called a* simplex code, *with parameters*

$$[\begin{bmatrix} k \\ 1 \end{bmatrix},\ k,\ q^{k-1}].$$

It has only one weight: q^{k-1}. If $k > u > 0$,then $\mathcal{C}_\gamma$ is called a Macdonald code, *with parameters*

$$[\begin{bmatrix} k \\ 1 \end{bmatrix} - \begin{bmatrix} u \\ 1 \end{bmatrix},\ k,\ q^{k-1} - q^{u-1}].$$

This code is a two-weight code, with weights $q^{k-1} - q^{u-1}$ and q^{k-1}. Both the simplex codes and the MacDonald codes attain the Griesmer bound. Hence they are length-optimal.

3.5 Simple constructions

In this section, we describe two methods of constructing a new projective multiset γ' from a projective multiset γ. In both cases the parameters of γ' only depend on those of γ and on the construction parameters.

3.5.1 Linear transforms

Let γ be a projective multiset on the projective space Π, and let $a \in \mathbb{Q}^*, b \in \mathbb{Q}$ be such that

$$\gamma' : \Pi \to \mathbb{Q},\ \ \gamma'(p) := a\gamma(p) + b,$$

is a projective multiset, i.e. such that $\operatorname{Im}\gamma' \subset \mathbb{N}$. Putting $l := \dim\Pi + 1$, we find that

$$n_{\gamma'} = an + b\begin{bmatrix} l \\ 1 \end{bmatrix}$$

and

$$\mu_{\gamma'}(H) = a\mu_\gamma(H) + bq^{l-1}.$$

If $b \neq 0$, the dimensions k, k' of γ and γ' may differ. In fact, if $k' \neq k$ then either $k = l$ or $k' = l$.

If $k' \leq k$, then

$$W_{\gamma'} = \{aw + bq^{l-1} \mid w \in W_\gamma\} \setminus \{0\}$$

and

$$f_{w'}(\gamma') = q^{k'-k} f_w(\gamma), \;\; w' = aw + bq^{l-1}.$$

Three special cases are particularly important:

- $\gamma'(p) := a\gamma(p)$, with $a \in \mathbb{N}$. Then the code $\mathcal{C}_{\gamma'}$ is said to be the a-fold *replication* of $\mathcal{C}_\gamma$.
- $\gamma'(p) := m - \gamma(p)$, with $m := \max M_\gamma$. In this case $\mathcal{C}_{\gamma'}$ is called an *anticode* of $\mathcal{C}_\gamma$. The Macdonald codes, for instance, are the anticodes of the simplex codes.
- $\gamma'(p) := \gamma(p) + b$, $b \in \mathbb{N}$. Then $\mathcal{C}_{\gamma'}$ is said to be obtained from $\mathcal{C}_\gamma$ by *adding b simplex codes* of dimension l.

Example 2 *If we add $t-1$ simplex codes of dimension k to the $[\left[{k \atop 1}\right] - \left[{u \atop 1}\right], k, q^{k-1} - q^{u-1}]$ MacDonald code, we obtain a* generalized MacDonald code*, with parameters*

$$[t\begin{bmatrix}k\\1\end{bmatrix} - \begin{bmatrix}u\\1\end{bmatrix}, \;k, \;tq^{k-1} - q^{u-1}].$$

3.5.2 Lifting

Let N be an $(s-1)$-dimensional subspace of Π and let $\gamma : \Pi/N \to \mathbb{N}$ be a k-dimensional projective multiset of length n. Choose a nonnegative integer c and define a projective multiset γ' on Π as follows:

$$\gamma'(p) := \begin{cases} c & \text{if } \;p \in N, \\ \gamma(Np) & \text{if } \;p \notin N. \end{cases}$$

We say that γ' is obtained from γ by an (s,c)-*lifting* of γ to Π. If $s > 0$, the lifting is said to be *proper*. So a properly lifted projective multiset $\gamma' : \Pi \to \mathbb{N}$ is characterized by the property that a nonempty projective subspace $N \subset \Pi$ exists such that γ' is constant on N and on all sets $M \setminus N$, $M \in \Pi/N$.

The dimension of γ' is $k + s$ and its length is $q^s n + c\left[{s \atop 1}\right]$. The weight function of γ' is given by

$$\mu_{\gamma'}(H) = \begin{cases} (q-1)q^{s-1}n + q^{s-1}c & \text{if } \;H \not\supseteq N, \\ q^s\mu_\gamma(H) & \text{if } \;H \supseteq N. \end{cases}$$

Hence the minimum weight of γ' is equal to

$$d_{\gamma'} = \min\{q^s d_\gamma, (q-1)q^{s-1}n + q^{s-1}c\}.$$

Note that the quotient multiset $(\gamma')^N$ is equivalent to $q^s\gamma$.

Remark 4 *If $\gamma, \delta : \Pi/N \to \mathbb{N}$ are equivalent, the (s,c)-lifted multisets $\gamma', \delta' : \Pi \to \mathbb{N}$ are equivalent.*

4 Dual transforms of multisets

4.1 Definition and basis properties

Now consider any function

$$\sigma : W \to \mathbb{N}$$

on the weight set $W := W_\gamma$ of a projective multiset $\gamma : \Pi \to \mathbb{N}$. Let us extend this function to a polynomial function

$$\sigma(i) := \sum_{y\in W} \sigma(y) \frac{\prod\limits_{w\in W\setminus y}(i-w)}{\prod\limits_{w\in W\setminus y}(y-w)}$$

on $\mathbb{Q}$ by Lagrange interpolation. Note that the degree $g := g_\sigma$ of the polynomial σ does not exceed $|W| - 1 = t - 1$, where t is the external distance of the dual of $\mathcal{C}_\gamma$.

For each σ, we shall construct from γ a new multiset on the dual of the spanning space $\Sigma := \Sigma_\gamma$.

Definition 15 *The* dual transform *of the projective multiset γ with respect to σ is the multiset*

$$\gamma^\sigma : \Sigma^* \to \mathbb{N}, \;\; H \longmapsto \sigma(\mu(H)).$$

Obviously, the multiplicity set of $\Gamma := \gamma^\sigma$ is the σ-image of the weight set of $\gamma :$

$$M_\Gamma = \{\sigma(w) \mid w \in W_\gamma\}. \tag{3}$$

The length of Γ is equal to

$$n_\Gamma = \sum_{w\in W} \sigma(w) f_w(\gamma)$$

and its weight function is given by

$$\mu_\Gamma(p) = n_\Gamma - \sum_{H\ni p} \Gamma(H) = \sum_{w\in W} \sigma(w)\{f_w(\gamma) - f_w(\gamma^p)\}, \quad p \in \Sigma. \tag{4}$$

From (4), we see that the weight function μ_Γ is known if we can calculate the frequencies of all 1-codimensional quotient multisets γ^p of γ.

Now we turn to the dimension of Γ. The dual of the spanning space Σ_Γ of Γ is equal to $N := \mu_\Gamma^{-1}(0) \subseteq \Sigma_\gamma$. Hence N is a projective subspace of Σ_γ and $\Sigma_\Gamma = (\Sigma/N)^*$. This implies that the dimension k_Γ of Γ is equal to

$$k_\gamma - \dim N - 1.$$

In particular,

$$k_\Gamma < k_\gamma \iff \mu_\Gamma^{-1}(0) \neq \emptyset. \tag{5}$$

4.2 Dual transforms of codes

Let $\mathcal{C} \subseteq \mathbb{F}_q^S$ be a k-dimensional full-length code, and let σ be a function that takes integer values on the weight set of $\mathcal{C}$.

Definition 16 *The* dual transform *of $\mathcal{C} \subseteq \mathbb{F}_q^S$ with respect to σ is the code $\mathcal{C}^\sigma := \mathcal{C}_\Gamma$, where $\Gamma := \gamma^\sigma$, the dual transform of $\gamma := \gamma_{\mathcal{C}}$ with respect to σ.*

There is a bijective correspondence between the 1-codimensional subcodes $\mathcal{D} \subset \mathcal{C}$ and the points $p = [\mathcal{D}^\perp/\mathcal{C}^\perp] \in \mathbb{P}(\mathbb{F}_q^S/\mathcal{C}^\perp)$. Since $f_w(\gamma) = \frac{1}{q-1}A_w(\mathcal{C})$ and $f_w(\gamma^p) = \frac{1}{q-1}A_w(\mathcal{D})$, we can use the MacWilliams identities (1) to express μ_Γ in terms of σ and the reduced distribution matrix $\bar{\mathbf{D}}$ of $\mathcal{C}^\perp$. From equation (1), we get

$$\begin{aligned}
\mu_\Gamma(p) &= \sum_{w\in W} \sigma(w)\{f_w(\gamma) - f_w(\gamma^p)\} \\
&= \frac{1}{q-1}\sum_{w\in W} \sigma(w)\{A_w(\mathcal{C}) - A_w(\mathcal{D})\} \\
&= \frac{1}{q-1}\sum_{j=0}^{n} \sigma(j)\{A_j(\mathcal{C}) - A_j(\mathcal{D})\} \\
&= \frac{q^{k-n-1}}{q-1}\sum_{j=0}^{n} \sigma(j)\sum_{i=0}^{n} K_j(i)\{qA_i(\mathcal{C}^\perp) - A_i(\mathcal{D}^\perp)\} \\
&= -q^{k-n-1}\sum_{i=0}^{n}\sum_{j=0}^{n} \sigma(j)K_j(i)\bar{\mathbf{D}}_{p,i}.
\end{aligned}$$

To simplify this further, let us express the polynomial σ in the Krawtchouk polynomials. There are – uniquely determined – rational numbers $a_0, a_1, \dots, a_g$ such that

$$\sigma(j) = \sum_{l=0}^{g} a_l K_l(j).$$

The orthogonality relations (2) imply that

$$\sum_{j=0}^{n} \sigma(j)K_j(i) = \sum_{l=0}^{g} a_l \sum_{j=0}^{n} K_l(j)K_j(i) = q^n a_i.$$

Hence

$$\mu_\Gamma(p) = -q^{k-1} \sum_{i=0}^{g} a_i \bar{\mathbf{D}}_{p,i}. \tag{6}$$

We infer that the weight function μ_Γ of Γ is a linear combination of the first $g+1 \leq t$ columns of the reduced distribution matrix $\bar{\mathbf{D}}$ of $\mathcal{C}^\perp$.

We can express the *length* $n_{\mathcal{C}^\sigma} = n_\Gamma$ of $\mathcal{C}^\sigma$ in terms of the weight distribution of $\mathcal{C}^\perp$:

$$\begin{aligned}
n_{\mathcal{C}^\sigma} &= \sum_{w \in W_\gamma} \sigma(w) f_w(\gamma) = \\
&= \frac{1}{q-1} \sum_{j=0}^{n} \sigma(j) A_j(\mathcal{C}) - \frac{\sigma(0)}{q-1} = \\
&= \frac{q^{k-n}}{q-1} \sum_{i=0}^{n} \sum_{j=0}^{n} \sigma(j) K_j(i) A_i(\mathcal{C}^\perp) - \frac{\sigma(0)}{q-1} = \\
&= \frac{q^k}{q-1} \sum_{i=0}^{g} \sum_{j=0}^{n} a_i A_i(\mathcal{C}^\perp) - \frac{1}{q-1} \sum_{i=0}^{g} a_i (q-1)^i \binom{n}{i} = \\
&= \sum_{i=0}^{g} a_i \{ \frac{q^k}{q-1} A_i(\mathcal{C}^\perp) - (q-1)^{i-1} \binom{n}{i} \}.
\end{aligned} \tag{7}$$

An even simpler formula, in terms of the reduced distribution matrix $\bar{\mathbf{D}}$ of $\mathcal{C}^\perp$, is

$$n_{\mathcal{C}^\sigma} = -\sum_{i=0}^{g} a_i \sum_{p \in \Pi_\gamma} \bar{\mathbf{D}}_{p,i}. \tag{8}$$

Example 3 *Let $\mathcal{C}$ be the unique binary $[48, 8, 22]$-code. (Cf. [9] for a construction and [18] for a computerized uniqueness proof.) The weight set of $\mathcal{C}$ is $\{22,24,30,32\}$. If we choose for σ the function with $\sigma(22) = \sigma(30) = 1$ and $\sigma(24) = \sigma(32) = 0$, then the dual transform $\mathcal{C}^\sigma$ turns out to be a $[192, 8, 96]$-code which in fact is optimal. Another, record breaking, example is the $[245, 9, 120]$ code described in [19]. D. Jaffe found this example (and several others that happen to improve the table [4]) by means of an extensive computer search. The basic problem here is to develop a theory that predicts which input codes $\mathcal{C}$ and which transform functions σ produce record-breaking output codes $\mathcal{C}^\sigma$.*

4.3 The dual distance

If the dual distance of $\mathcal{C}$ is at least $2e+1$, i.e. if

$$A_1(\mathcal{C}^\perp) = A_2(\mathcal{C}^\perp) = \cdots = A_{2e+1}(\mathcal{C}^\perp) = 0,$$

the columns $\bar{\mathbf{D}}_1$, $\bar{\mathbf{D}}_2, \dots, \bar{\mathbf{D}}_e$ of the reduced distribution matrix $\bar{\mathbf{D}}$ of $\mathcal{C}^\perp$ are $\{0,1\}$-functions on Π whose supports are the projective images of the Hamming spheres of radius i, $i = 1, \dots, e$, in $\mathbb{F}_q^S$. So

$$|\operatorname{supp}(\bar{\mathbf{D}}_i)| = (q-1)^{i-1}\binom{n}{i}, \quad i = 1, \dots, e.$$

Let us suppose that the degree g of the polynomial σ does not exceed e. Then we can calculate the parameters of the dual transform $\mathcal{C}^\sigma$ of $\mathcal{C}$ explicitly. Let Γ be the dual transform of $\gamma := \gamma_{\mathcal{C}}$ with respect to σ. Using (7) or (8), we find that the length of Γ (and $\mathcal{C}^\sigma$) is equal to

$$n_{\mathcal{C}^\sigma} = a_0 \begin{bmatrix} k \\ 1 \end{bmatrix} - \sum_{i=1}^{g} a_i (q-1)^{i-1} \binom{n}{i}.$$

The weight function μ_Γ is given by

$$\mu_\Gamma(p) = \begin{cases} q^{k-1}(a_0 - a_i) & \text{if } \; p \in \operatorname{supp}(\bar{\mathbf{D}}_i), \\ \\ q^{k-1} a_0 & \text{if } \; p \notin \bigcup_{i=1}^{g} \operatorname{supp}(\bar{\mathbf{D}}_i). \end{cases}$$

The sets $\operatorname{supp}(\bar{\mathbf{D}}_i)$, $i = 1, 2, \dots, g$, fill the space $\mathbb{P}(\mathbb{F}_q^S/\mathcal{C}^\perp)$ if and only if $n = k = g$. Let us exclude that trivial case. Then the weight set of $\mathcal{C}^\sigma$ is equal to

$$\{q^{k-1}(a_0 - a_i) \mid i = 1 \dots e\} \cup \{q^{k-1} a_0\}$$

As to the dimension of $\mathcal{C}^\sigma$, we observe that $k_\Gamma = k$ unless $a_0 = 0$ or $a_0 = a_i$ for some i between 1 and g.

Finally we calculate the frequencies of Γ. Suppose that $k_{\mathcal{C}^\sigma} = k$. Then

$$f_w(\Gamma) = \begin{cases} \left[\begin{smallmatrix} k \\ 1 \end{smallmatrix}\right] - \displaystyle\sum_{\{j \mid j>0, a_j \neq 0\}} (q-1)^{j-1}\tbinom{n}{j} & \text{if } \; w = q^{k-1} a_0, \\ \\ \displaystyle\sum_{\{j \mid j>0, a_j = a_i\}} (q-1)^{j-1}\tbinom{n}{j} & \text{if } \; w = q^{k-1}(a_0 - a_i) \neq q^{k-1} a_0. \end{cases}$$

5 Dual transforms of degree one

Let $\mathcal{C} \subseteq \mathbb{F}_q^S$ be a k-dimensional full-length code of length n, and let $\gamma := \gamma_{\mathcal{C}}$ be the corresponding projective multiset on $\Pi := \mathbb{P}(\mathbb{F}_q^S/\mathcal{C}^\perp)$. In this section, we study dual transforms $\mathcal{C}^\sigma$ under the assumption that the transform function σ is *has degree one:* $\sigma(j) := aj + b$. Two choices for σ are particularly useful: If $\Delta := \gcd W$, $d := \min W$ and $D := \max W$, then the functions σ_+ and σ_- defined by

$$\sigma_+(j) := \frac{j-d}{\Delta}, \; \sigma_-(i) := \frac{-j+D}{\Delta} \tag{9}$$

indeed take nonnegative integer values on $W_{\mathcal{C}}$.

5.1 Length, weights, dimension, frequencies

Expressing the polynomial σ in the Krawtchouk polynomials $K_0(j) := 1$ and $K_1(j) := (q-1)n - qj$, we get

$$\begin{aligned}\sigma(j) &= a_0 K_0(j) + a_1 K_1(j) = \\ &= (b + \frac{(q-1)an}{q})K_0(j) + (-\frac{a}{q})K_1(j).\end{aligned}$$

Let $\mathcal{D} := \mathcal{C}^\sigma$ be the dual transform of $\mathcal{C}$ with respect to σ. Since the code $\mathcal{C}$ is of full length, i.e. $A_1(\mathcal{C}^\perp) = 0$, Formula (7) for the length of $\mathcal{D}$ reduces to

$$\begin{aligned}n_{\mathcal{D}} &= a_0(\frac{q^k}{q-1} - \frac{1}{q-1}) + a_1 n = \\ &= nq^{k-1}a + \begin{bmatrix} k \\ 1 \end{bmatrix} b.\end{aligned} \tag{10}$$

Now we consider the weight function of $\Gamma := \gamma^\sigma$. Formula (6) gives us

$$\begin{aligned}\mu_\Gamma(p) &= -q^{k-1}\{(b + \frac{(q-1)an}{q})\bar{\mathbf{D}}_{p,0} + (-\frac{a}{q})\bar{\mathbf{D}}_{p,1}\} = \\ &= q^{k-2}\{qb + (q-1)an + a\gamma(p)\} = \\ &= \alpha\gamma(p) + \beta,\end{aligned} \tag{11}$$

with

$$\alpha := q^{k-2}a$$

and

$$\beta := q^{k-1}b + q^{k-2}(q-1)an = \frac{(q-1)n_{\mathcal{D}} + b}{q}.$$

Remark 5 *Note that the weight set $W_{\mathcal{D}}$ of $\mathcal{D}$ is equal to*

$$\{\alpha m + \beta \mid m \in M_\gamma\} \setminus \{0\}.$$

If, in particular, $\mathcal{C}$ is projective, *then $\mathcal{D}$ is a (≤ 2)-weight code. This case is the main subject matter of Brouwer and Van Eupen's paper [5].*

Next we discuss the possibility of a dimension drop. Put

$$N := \{p \in \Pi \mid \alpha\gamma(p) + \beta = 0\}.$$

This is a projective subspace of Π on which γ has the constant value $-\frac{\beta}{\alpha} = -q\frac{b}{a} - (q-1)n$. From (5) we see that the dimension $k_{\mathcal{D}}$ of $\mathcal{D}$ is equal to k unless

$$-q\frac{b}{a} - (q-1)n \in M_\gamma.$$

If $p \in \Pi \setminus N$, then $w := \mu_\Gamma(p) \in W_\mathcal{D}$. Moreover γ takes the constant value $\frac{w-\beta}{\alpha}$ on $Np \setminus N$. Hence if $k_\mathcal{D} < k$, then γ has to be a *properly lifted* projective multiset, cf. subsubsection 3.5.2.

Formula (11) immediately gives the *minimum distance* of $\mathcal{D}$. If $k_\mathcal{D} = k$, then

$$d_\mathcal{D} = \begin{cases} (an+b)q^{k-1} + a(\min M_\gamma - n)q^{k-2} & \text{if} \quad a > 0, \\ (an+b)q^{k-1} + a(\max M_\gamma - n)q^{k-2} & \text{if} \quad a < 0. \end{cases}$$

If $k_\mathcal{D} < k$, then $\min M_\gamma$ and $\max M_\gamma$ have to be replaced by $\min(M_\gamma \setminus \{\min M_\gamma\})$ and $\max(M_\gamma \setminus \{\max M_\gamma\})$ respectively.

Finally, we see from (11) that the frequency of a weight $w := \alpha m + \beta$ of Γ is equal to

$$f_w(\Gamma) = q^{k-k_\mathcal{D}} |\gamma^{-1}(m)|.$$

Example 4 *An alternative construction of the* $[162, 8, 80]$*-codes (cf. [2]). There exist binary* $[21, 8, 8]$*-codes* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *with the same weight set* $\{8, 12, 16\}$, *but with* $A_2(\mathcal{C}_1^\perp) = 0$ *and* $A_2(\mathcal{C}_2^\perp) = 1$ *(cf. [18]). Hence we can calculate the values of* $|\gamma^{-1}(m)|$*:*

	$\lvert\gamma^{-1}(0)\rvert$	$\lvert\gamma^{-1}(1)\rvert$	$\lvert\gamma^{-1}(2)\rvert$
$\mathcal{C}_1$	234	21	0
$\mathcal{C}_2$	235	19	1

Consequently, as one of the referees of [2] pointed out, the codes $\mathcal{C}_i^{\sigma+}$, $i = 1, 2$, *have parameters* $[162, 8, 80]$ *and weight distributions*

	A_{80}	A_{96}	A_{112}
$\mathcal{C}_1^{\sigma+}$	234	21	0
$\mathcal{C}_2^{\sigma+}$	235	19	1

.

5.2 The inverse of the dual transform

If γ, δ are equivalent k-dimensional projective multisets, then their dual transforms Γ, Δ with respect to any function σ obviously are equivalent as well. For dual transforms of degree *one* the converse is also true. This follows from the following proposition and Remark 4. We use the notation of the preceding subsection.

Proposition 2 *Let* Γ *be the dual transform of* γ *with respect to a function* σ *of degree one. Then a function* τ *of degree one exists such that* γ *is an* (s, c)*-lifting of the dual transform* γ' *of* Γ *with respect to* τ. *The parameters* s *and* c *depend only* Γ, k_γ *and* σ.

Proof. From (11), we see that the function $\tau : j \mapsto a'j + b'$ defined by

$$a' := \frac{1}{q^{k-2}a}, \quad b' := -q\frac{b}{a} - (q-1)n = -\frac{(q-1)n_\Gamma + b}{aq^{k-1}},$$

takes nonnegative integer values on W_Γ. The spanning space Σ_Γ of Γ is equal to $(\Sigma/N)^*$ and $\gamma' : \Sigma/N \to \mathbb{N}$ takes the value $\gamma(p)$ on Np, $p \notin N$. So γ is an (s, c)-lifting of γ', with $s := k - k_\Gamma$ and $c := b'$. ■

Remark 6 *This result is an extension of Section 4: "Going Back and Forth" in [5], where only projective* sets *are considered and the absence of a dimension drop is tacitly assumed.*

5.3 Short proofs of known results

As an amusing sideline, we give short proofs of a theorem of Ward, a theorem of Bonisoli and the uniqueness of the generalized MacDonald codes.

Proposition 3 *([33], Th. 1) Let $\mathcal{C}$ be a q-ary full-length code, and let Δ be the greatest common divisor of the codeword weights. If y is the maximal factor of Δ that is relatively prime to q, then $\mathcal{C}$ is a y-fold replicated code.*

Proof. We use the notation of Subsection 5.1 and consider the σ_+-dual transform $\mathcal{D}$ of $\mathcal{C}$. From the fact that

$$n_\Gamma = \frac{nq^{k-1}}{\Delta} - \frac{q^k-1}{q-1}\frac{d}{\Delta} \in \mathbb{N}$$

and $\Delta \mid d$, we see that $y \mid n$. Since

$$\mu_\Gamma(p) = -\frac{q^{k-1}d}{\Delta} + \frac{q^{k-2}(q-1)n}{\Delta} + \frac{q^{k-2}\gamma(p)}{\Delta} \in \mathbb{N} \text{ for all } p \in \Pi,$$

we infer that $y \mid \gamma(p)$ for all $p \in \Pi$. ■

Example 5 *In [7], Cherdieu et al. described a code Γ_0 with length q^{2n}, dimension $n^2 \log_r q$ and weight distribution*

$$w_\rho = q^{2n} - r^{-1}q^{2n} - r^{-1}(-1)^\rho q^{2n-\rho}(r-1), \rho = 0, 1, ..., n$$

where n and r are integers > 1 , $r \mid q$. Since all weights w_ρ, $\rho = 1, ..., n$ are divisible by $q+1$, the code Γ_0 is a $(q+1)$-fold replicated code extended by an appropriate number of zero columns.

Proposition 4 *([1]) Let $\mathcal{C}$ be a q-ary k-dimensional full-length code with exactly one non-zero weight d. Then $\mathcal{C}$ is a $\frac{d}{q^{k-1}}$ times replicated simplex code.*

Proof. By counting the non-zero entries in the list of all codewords, we see that

$$n = \frac{(q^k-1)d}{q^{k-1}(q-1)}.$$

Consider the σ_+-dual transform Γ of $\gamma_{\mathcal{C}}$. Note that $\Delta = d$. Hence

$$n_\Gamma = \frac{nq^{k-1}}{d} - \frac{q^k-1}{q-1}\frac{d}{d} = 0,$$

which implies that

$$\mu_\Gamma(p) = -\frac{q^{k-1}d}{d} + \frac{q^{k-2}(q-1)n}{d} + \frac{q^{k-2}\gamma(p)}{d} =$$
$$= -\frac{1}{q} + \frac{q^{k-2}\gamma(p)}{d} = 0 \text{ for all } p \in \Pi.$$

So γ is the constant function $\frac{d}{q^{k-1}}$. ■

Proposition 5 (Tamari [28]) *The generalized MacDonald codes are unique.*

Proof. Let $\mathcal{C}$ be a q-ary code with parameters

$$[t\begin{bmatrix}k\\1\end{bmatrix} - \begin{bmatrix}u\\1\end{bmatrix},\ k,\ tq^{k-1} - q^{u-1}],$$

and let $\gamma := \gamma_{\mathcal{C}}$ be the corresponding multiset in $\Pi := \mathbb{P}(\mathbb{F}_q^n/\mathcal{C}^\perp)$. Consider the dual transform Γ of γ with respect to $\sigma : j \mapsto j - tq^{k-1} + q^{u-1}$. Substitution of the parameters in (11) yields

$$\mu_\Gamma(p) = q^{k-2}(-t + 1 + \gamma(p)).$$

Since μ_Γ is nonnegative, the minimum multiplicity of γ must be at least $t-1$. In fact this minimum is equal to $t-1$, and $|\gamma^{-1}(t-1)| \geq \left[\begin{smallmatrix}u\\1\end{smallmatrix}\right]$, because $t|\Pi| - n_\gamma = \left[\begin{smallmatrix}u\\1\end{smallmatrix}\right]$. Consequently, the dimension $v-1$ of the projective subspace $\mu_\Gamma^{-1}(0) = \gamma^{-1}(t-1)$ of Π is not smaller than $u-1$. From Proposition 2, we see that γ is a $(v, t-1)$-lifting of a multiset γ'. By Subsection 3.5.2, the length of γ' is equal to

$$q^{-v}(n_\gamma - (t-1)\begin{bmatrix}v\\1\end{bmatrix}) = t\begin{bmatrix}k-v\\1\end{bmatrix} + \frac{q^{u-v}-1}{q-1}.$$

This is an integer if and only if $v \leq u$. Hence $u = v$. So $\gamma(p) \geq t$ outside a $(u-1)$-dimensional subspace $L := \gamma^{-1}(t-1) \subset \Pi$. But the existence of any point p with $\gamma(p) > t$ would imply that

$$n_\gamma > t\begin{bmatrix}k\\1\end{bmatrix} - \begin{bmatrix}u\\1\end{bmatrix}.$$

Hence

$$\gamma(p) = \begin{cases} t-1 & \text{if } p \in L, \\ t & \text{if } p \in \Pi \setminus L. \end{cases}$$

■

6 σ–self-dual codes

Let $\mathcal{C} \subseteq \mathbb{F}_q^S$ be a k-dimensional full-length code, and let σ be a function that takes integer values on the weight set of $\mathcal{C}$.

Definition 17 *The code $\mathcal{C}$ is said to be* self-dual *with respect to σ if it is equivalent to its dual transform $\mathcal{C}^\sigma$.*

Example 6 *Let $\mathcal{C}$ be the $[48, 8, 22]$-code $\mathcal{C}$ discussed in Example 3. If we take σ to be the function with $\sigma(30) := 1$ and $\sigma(w) := 0$ for $w \in W_{\mathcal{C}} \setminus \{30\}$, then $\mathcal{C}^\sigma$ turns out to have the same parameters as $\mathcal{C}$. Hence the uniqueness of $\mathcal{C}$ implies that it is self-dual with respect to σ.*

Example 7 *It is known [10] that there are exactly two nonequivalent binary* $[18, 6, 8]$-*codes* $\mathcal{C}_1$, $\mathcal{C}_2$. *Their weight distributions are*

	A_8	A_{12}	A_{16}	$A_2(\mathcal{C}_i^\perp)$
$\mathcal{C}_1$	46	16	1	1
$\mathcal{C}_2$	45	18	0	0

Both codes are easily seen to be self-dual with respect to σ_+.

Example 8 *The unique binary* $[51, 8, 24]$-*code has weight distribution* $A_{24} = 204$ *and* $A_{32} = 51$ *(cf. [18]). This code is self-dual with respect to* σ_+.

Example 9 *Let* G *be an incidence matrix of the finite projective plane* $\mathfrak{P} := \mathbb{P}(\mathbb{F}_p^3)$, p *prime, and let* $\mathcal{C}$ *be the* q-*ary code with generator matrix* G. *It is well known [26] that* $\mathcal{C}$ *is a* $[p^2+p+1, \frac{1}{2}(p^2+p+2), p+1]$-*code for which the words of minimum weight are the nonzero multiples of the rows of* G. *Let* σ *be the function with* $\sigma(p+1) := 1$ *and* $\sigma(w) := 0$ *for* $w \in W_{\mathcal{C}} \setminus \{p+1\}$. *The existence of correlations in* $\mathfrak{P}$ *implies that the transpose* G^t *is a permutation of* G. *Hence* $\mathcal{C}$ *is self-dual with respect to* σ.

If the transform function σ has degree *one*, it is easy to derive strong conditions on the parameters of self-dual codes with respect to σ :

Proposition 6 *Let* $\mathcal{C}$ *be* q-*ary* $[n, k, d]$-*code which is self-dual with respect to the function* $\sigma : j \mapsto aj + b$. *If* $\mathcal{C}$ *is not a replicated simplex code, then*

$$a = \pm q^{1-\frac{k}{2}}, \;\; b = -\frac{q-1}{1+q^{k-1}a}n. \tag{12}$$

Proof. Let $(w_1, w_2, \ldots, w_r)$ be the ordered weight set of $\mathcal{C}$ (and $\mathcal{C}^\sigma$), and let $(m_1, m_2, \ldots, m_r)$ be the ordered multiplicity set of $\gamma_{\mathcal{C}}$ (and $\gamma_{\mathcal{C}^\sigma}$). Since $\mathcal{C}$ is self-dual with respect to σ,the sizes of these sets are equal: $r = s$. Moreover (3) and (11) imply that either

$$\begin{aligned} w_i &= q^{k-2}am_i + q^{-1}((q-1)n + b), \\ m_i &= aw_i + b \end{aligned}$$

or

$$\begin{aligned} w_i &= q^{k-2}am_{r-i} + q^{-1}((q-1)n + b), \\ m_i &= aw_{r-i} + b, \end{aligned}$$

for $i = 1, 2, \ldots, r$. Eliminating m_i, we find that

$$w_i = q^{k-2}a^2w_i + q^{k-2}ab + q^{-1}((q-1)n + b).$$

If $r > 1$, then

$$q^{k-2}a^2 = 1 \text{ and } q^{k-2}ab + q^{-1}((q-1)n + b) = 0,$$

which immediately gives (12). If $r = 1$, then $\mathcal{C}$ is an m_1-fold replicated simplex code. This code is self-dual with respect to the constant function $\sigma = m_1$. ■

Example 10 *A. Brouwer [3] constructed a family of q-ary two-weight projective codes with parameters*

$$n = (q^{e-1} - 1)(q^{de-e} + q^{\frac{de}{2}-e})/(q-1), k = de,$$

where d and e are arbitrary integers, d even and $e > 1$. The weights are

$$w_1 = (q^{e-1} - 1)q^{de-e-1}, w_2 = w_1 + q^{\frac{de}{2}-1}.$$

These codes satisfy the conditions (12) with respect to σ_-. It is not known if they are self-dual with respect to σ_-.

Remark 7 *Choose $q = 2$, $d = 2$ in the above construction. Then the resulting code $\mathcal{C}_1(e)$ has parameters*

$$n = 2^{2e-1} - 2^{e-1}, k = 2e$$

and

$$w_1 = 2^{2e-2} - 2^{e-1}, w_2 = 2^{2e-2}.$$

The code $\mathcal{C}(e) := \langle \mathcal{C}_1(e), \mathbf{1} \rangle$, spanned by $\mathcal{C}_1(e)$ and the all-one vector $\mathbf{1}$, is a projective self-complementary $[n, k+1, w_1]$-code with weight set $\{w_1, w_2, n\}$. It meets the Grey-Rankin bound. Since it is projective, the code

$$\mathcal{D}(e) := RM(1, 2e) \backslash \mathcal{C}(e)$$

(the column set of the first order Reed-Muller code with the columns of $\mathcal{C}(e)$ deleted) has parameters

$$[2^{2e-1} + 2^{e-1}, 2e + 1],$$

and the weight set

$$\{2^{2e-2}, 2^{2e-2} + 2^{e-1}, 2^{2e-1} + 2^{e-1}\}.$$

It also meets the Grey-Rankin bound. For an alternative construction of codes with the above parameters see [20]. The partition

$$RM(1, 2e) = (\mathcal{C}(e) \mid \mathcal{D}(e))$$

shows that the number of nonequivalent projective self-complementary codes with parameters

$$[2^{2e-1} - 2^{e-1}, 2e + 1, 2^{2e-2} - 2^{e-1}]$$

coincides with the number of nonequivalent projective self-complementary codes with parameters

$$[2^{2e-1} + 2^{e-1}, 2e + 1, 2^{2e-2}].$$

In particular, since there are exactly 4 non-equivalent projective self-comple-mentary $[28, 7, 12]$-codes (cf.[11], [29]), it follows that there are exactly 4 nonequivalent projective self-complementary $[36, 6, 16]$-codes (cf.[29]).

Remark 8 *Tonchev showed in [30] and [31] that there are exactly* 5 *nonequivalent* $[27, 6, 12]$ *two-weight codes, with weight* $A_{12} = 36$ *and* $A_{16} = 27$. *All these codes satisfy the conditions (12) with respect to* σ_+. *As a matter of fact, Boukliev and Kapralov managed to show that they are self-dual with respect to* σ_+. *In general, however, it is not clear whether the conditions (12) imply self-duality in the case of transforms* σ *of degree 1.*

Acknowledgments

This work was completed during the visit of S. Dodunekov to the Faculty of Technical Mathematics and Informatics, Delft University of Technology. He would like to thank Dr. Juriaan Simonis and Dr. Jan van Zanten for their support and hospitality and Mrs. C.A. van Baar for her assistance.

The paper was partially supported by the Bulgarian NSF grant MM502/95.

References

[1] Bonisoli, A. Every equidistant linear code is a sequence of dual Hamming codes. *Ars Combin.* **18** (1984), 181–186.

[2] Boukliev, I.; Dodunekov, S. M.; Helleseth, T.; Ytrehus, Ø. On the $[162, 8, 80; 2]$ codes. *IEEE Trans. Inform. Theory* **43** (1997), no. 6, 2055–2057.

[3] Brouwer, A. E. Some new two-weight codes and strongly regular graphs. *Discrete Appl. Math.* **10** (1985), no. 4, 455–461.

[4] Brouwer, A. E.; Verhoeff, T. An updated table of minimum-distance bounds for binary linear codes. *IEEE Trans. Inform. Theory* **39** (1993), no. 2, 662–676. Online version: http://www.win.tue.nl/math/dw/voorlincod.html.

[5] Brouwer, A. E.; van Eupen, M. The correspondence between projective codes and 2-weight codes. *Des. Codes Cryptogr.* **11** (1997), no. 3, 262–266.

[6] Calderbank, A. R.; Kantor, W. M. The geometry of two-weight codes. *Bull. London Math. Soc.* **18** (1986), 97–122.

[7] Cherdieu, J. P.; Delcroix, A.; Mado, J. C.; Mercier, D. J. Weight distribution of the Hermition forms codes. *Appl. Alg. Engrg. Comm. Comput.* **8** (1997), no. 4, 307–314.

[8] Delsarte, P. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.* No. 10 (1973), vi+97 pp.

[9] Dodunekov, S. M.; Manev, N. L. An improvement of the Griesmer bound for some small minimum distances. *Discrete Appl. Math.* **12** (1985), no. 2, 103–114.

[10] Dodunekov, S. M.; Encheva, S. B. Uniqueness of some linear subcodes of the binary extended Golay code. *Problems Inform. Transmission* **29** (1993), no. 1, 38–43; *translated from Problemy Peredachi Informatsii* **29** (1993), no. 1, 45–51 (Russian).

[11] Dodunekov, S. M.; Encheva, S. B.; Kapralov, S. N. On the $[28, 7, 12]$ binary self-complementary codes and their residuals. *Des. Codes Cryptogr.* **4** (1994), no. 1, 57–67.

[12] Goppa, V. D. Codes on algebraic curves. *Soviet Math. Doklady* **24**, 170–172; *translated from Dokl. Akad. Nauk SSSR* **259** (1981), no. 6, 1289–1290 (Russian).

[13] Hamada, N.; Tamari, F. On a geometrical method of construction of maximal t-linearly independent sets. *J. Combin. Theory Ser. A* **25** (1978), no. 1, 14–28.

[14] Hamada, N. A characterization of some $[n, k, d; q]$-codes meeting the Griesmer bound using a minihyper in a finite projective geometry. *Discrete Math.* **116** (1993), no. 1-3, 229–268.

[15] Hill, R. Caps and codes. *Discrete Math.* **22** (1978), no. 2, 111–137.

[16] Hill, R. Optimal linear codes. *Cryptography and coding, II (Cirencester, 1989),* 75-104, Inst. Math. Appl. Conf. Ser. New Ser., 33, *Oxford Univ. Press, New York,* 1992.

[17] Hirschfeld, J. W. P.; Storme, L. The packing problem in statistics, coding theory and finite projective spaces. To appear in *J. Statist. Plann. Inference* .(*Proceedings of the Bose Memorial conference, Colorado,* June 1995).

[18] Jaffe, D. B. Binary linear codes: new results on nonexistence. *Draft version accessible through the author's web page: http://www.math.unl.edu/~djaffe/*, November 10,1997 (Version 0.5). Dept. of Math. and Statistics, University of Nebraska, Lincoln.

[19] Jaffe, D. B.; Simonis, J. New binary linear codes which are dual transforms of good codes. submitted to *IEEE Trans. Inform. Theory.* Online preprint available at http://www.math.unl.edu/~djaffe/.

[20] Jungnickel, D.; Tonchev, V. D. Exponential number of quasi-symmetric SDP designs and codes meeting the Grey-Rankin bound. *Des. Codes Cryptogr.* **1** (1991), no. 3, 247–253.

[21] Krawtchouk, M. Sur une généralisation des polynomes d'Hermite. *Comptes Rendus* **189** (1929), 620-622.

[22] Landgev, I. N. Linear codes over finite fields and finite projective geometries. To appear in *Discrete Math.*.

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

[24] MacWilliams, F. J.; Sloane, N. J. A. The theory of error-correcting codes. 2nd reprint. North-Holland Mathematical Library, Vol. 16. *North-Holland Publishing Co., Amsterdam - New York - Oxford,* 1983, xx+762 pp. ISBN: 0-444-85009-0 and 0-444-85010-4.

[25] Peterson, W. W.; Weldon, E. J., Jr. Error-correcting codes. Second edition. *The M.I.T. Press, Cambridge, Mass. - London,* 1972. xi+560 pp.

[26] Sachar, H. The $\mathbb{F}_p$ span of the incidence matrix of a finite projective plane. *Geom. Dedicata* **8** (1979), 407–415.

[27] Slepian, D. A class of binary signaling alphabets. *Bell System Tech. J.* **35** (1956), 203–234.

[28] Tamari, F. On linear codes which attain the Solomon-Stiffler bound. *Discrete Math.* **49** (1984), no. 2, 179–191.

[29] Tonchev, V. D. Quasi-symmetric designs, codes, quadrics, and hyperplane sections. *Geom. Dedicata* **48** (1993), no. 3, 295–308.

[30] Tonchev, V. D. The uniformly packed binary $[27, 21, 3]$ and $[35, 29, 3]$ codes. *Proc. Int. Workshop on Optimal Codes and Related Topics, Sozopol, Bulgaria, May 26 - June 1,* 1995, 130-136.

[31] Tonchev, V. D. The uniformly packed binary $[27, 21, 3]$ and $[35, 29, 3]$ codes. *Discrete Math.* **149** (1996), 283-288.

[32] Tsfasman, M. A.; Vladut, S. G. Algebraic-geometric codes. Translated from the Russian by the authors. Mathematics and its Applications (Soviet Series), 58. *Kluwer Academic Publishers Group, Dordrecht,* 1991 xxiv+667 pp. ISBN: 0-7923-0727-5.

[33] Ward, H. N. Divisible codes. *Arch. Math.* (Basel) 36 (1981), no. 6, 485–494.