JOURNAL OF COMBINATORIAL THEORY, Series A 25, 226–241 (1978)

Bilinear Forms over a Finite Field, with Applications to Coding Theory

PH. DELSARTE

MBLE Research Laboratory, Brussels, Belgium

Communicated by J. H. van Lint

Received December 7, 1976

Let Ω be the set of bilinear forms on a pair of finite-dimensional vector spaces over $GF(q)$. If two bilinear forms are associated according to their q-distance (i.e., the rank of their difference), then Ω becomes an association scheme. The characters of the adjacency algebra of Ω, which yield the MacWilliams transform on q-distance enumerators, are expressed in terms of generalized Krawtchouk polynomials. The main emphasis is put on subsets of Ω and their q-distance structure. Certain q-ary codes are attached to a given $X \subset \Omega$; the Hamming distance enumerators of these codes depend only on the q-distance enumerator of X. Interesting examples are provided by Singleton systems $X \subset \Omega$, which are defined as t-designs of index 1 in a suitable semilattice (for a given integer t). The q-distance enumerator of a Singleton system is explicitly determined from the parameters. Finally, a construction of Singleton systems is given for all values of the parameters.

1. INTRODUCTION

Classical coding theory may be introduced as follows. Let Γ denote a finite-dimensional vector space over the finite field K. The Hamming *weight* $\text{wt}(f)$ of a vector $f \in \Gamma$ is the number of nonzero coordinates of f in a fixed K-basis of Γ. Then (Γ, wt) is a normed space, called *Hamming space*; and a *code* simply is a nonempty subset of Γ endowed with the Hamming distance attached to wt. It is well known that (Γ, wt) has the combinatorial structure of an *association scheme* [2, 6] of which the adjacency algebra is a *Schur ring* [25]. The character table of this ring involves certain Krawtchouk polynomials [5, 23] and plays an important role in coding theory. We especially mention the *MacWilliams identities* [16] on weight enumerators of pairs of dual group codes, as well as the *MacWilliams inequalities* [5, 17] on the distance enumerator of an unrestricted code.

The *Singleton bound* [22] says that the size of a code $C \subset \Gamma$ having minimum distance $s + 1$ cannot exceed $| K |^{n-s}$, with $n = \dim_K(\Gamma)$. Moreover, $| C |$ equals $| K |^{n-s}$ if and only if C is an *orthogonal array* [20] of strength $t = n - s$

0097-3165/78/0253–0226$02.00/0

and index 1. We recall two properties of such *optimal codes* C: The distance distribution of any optimal code is uniquely determined from $(n, t, |K|)$, and the class of optimal group codes is closed under duality [1, 5, 11, 18]. Optimal linear codes are known to exist, for every t, whenever $n \leqslant |K|$ holds; constructions are essentially due to Reed and Solomon [21].

The present paper is concerned with a *q-analog* of coding theory (see [7, 8]). Here the framework is the normed space (Ω, rk), where Ω consists of all *bilinear forms* on two finite-dimensional vector spaces V and V' over the field $F = GF(q)$, the norm $\mathrm{rk}(f)$ of a given bilinear form $f \in \Omega$ being its *F-rank*. Thus the q-analog of a code is a nonempty subset $X \subset \Omega$ provided with the *q-distance* $\mathrm{d}(f, g) = \mathrm{rk}(f - g)$ for all $f, g \in X$.

All features of Hamming schemes recalled above have their counterparts in (Ω, rk). In Section 2 it is shown that the q-distance relations on Ω form an association scheme (corresponding to a Schur ring). This simple fact allows derivation of MacWilliams identities and inequalities [6] on the q-distance enumerators of subsets $X \subset \Omega$ (cf. Section 3). In the Appendix we obtain an explicit formula for the MacWilliams transform (i.e., the character table of the Schur ring), in terms of *generalized Krawtchouk polynomials* [8]. These preliminary results are not really new, but their proofs are quite different from those given in previous papers [6, 7].

In Section 4 certain q-ary codes $C \subset \Gamma = F^W$, with $W = V \times V'$, are attached to subsets $X \subset \Omega$: For a given X, a typical code vector of C is a mapping from W to F which is a sum $f + \psi + \psi' + c$ of a bilinear form $f \in X$, two linear forms ψ and ψ' on V and V', respectively, and a constant $c \in F$. (Note that C is a union of cosets of the first-order generalized Reed–Muller code in the second-order generalized Reed–Muller code [14].) It turns out that the Hamming distance enumerator of C is uniquely determined from the q-distance enumerator of X. At the end of Section 4, a generalization of a class of codes introduced by Camion [4] is also presented.

Assume $m' = \dim_F(V') \geqslant m = \dim_F(V)$. The Singleton bound on a subset $X \subset \Omega$ of minimum q-distance $s + 1$ is the inequality $|X| \leqslant |V'|^{m-s}$. This bound is achieved if and only if X is a *t-design* of strength $t = m - s$ and index 1 in an appropriate semilattice (cf. [7]). Section 5 is devoted to a study of these remarkable sets X, called *Singleton systems.* An explicit formula for the q-distance enumerator of a Singleton system is derived. On the other hand, given a subgroup X of $(\Omega, +)$ which is a Singleton system of strength t, it is shown that the *dual* subgroup $X^\perp$ of X is a Singleton system of strength $m - t$.

Finally, Section 6 is devoted to constructions. For all values of the numbers m, m', and q, linear Singleton systems of any strength t are described. These systems may be viewed as q-analogs of Reed–Solomon codes.

It should be noted that the present theory has many formal analogies with that of alternating bilinear forms over a finite field [3, 10, 12, 15, 19]. The main difference lies in the respective difficulties of both theories; without doubt, the latter (alternating bilinear forms) is much more complicated than the former (unrestricted bilinear forms), especially with regard to construction of Singleton systems.

2. Schur Ring and Association Scheme of Bilinear Forms

Let V and V' be two nonzero finite-dimensional vector spaces over the Galois field $F = GF(q)$. We denote by W the Cartesian product $V \times V'$ and by F^W the set of mappings

$$f\colon W = V \times V' \to F\colon (x, x') \mapsto f(x, x'). \tag{2.1}$$

Put $m = \dim_F(V)$, $m' = \dim_F(V')$, and $n = q^{m+m'}$. Then F^W is an n-dimensional vector space over F (since $n = |W|$ holds).

A given $f \in F^W$ is called a *bilinear form* on V and V', with respect to the field F, if it satisfies the identity

$$f\left(\sum_i x_i\mu_i, \sum_j x_j'\mu_j'\right) = \sum_{i,j} x_i f(\mu_i, \mu_j') x_j', \tag{2.2}$$

for all scalars $x_i, x_j' \in F$ and all vectors $\mu_i \in V$, $\mu_j' \in V'$. Clearly, the set $\Omega = \Omega(m, m')$ of all bilinear forms is an mm'-dimensional subspace of F^W.

The left *radical* $\operatorname{Rad}(f)$ of any $f \in \Omega$ by definition is the subspace of V consisting of all vectors x satisfying $f(x, x') = 0$ for every x' in V'. The *rank* of f is the codimension of the radical, i.e.,

$$\operatorname{rk}(f) = m - \dim_F(\operatorname{Rad}(f)). \tag{2.3}$$

Without loss of generality, we take $m \leqslant m'$ in the sequel. Then $\operatorname{rk}(f)$ assumes all integer values between 0 and m.

Given two F-bases $(\mu_i\colon 1 \leqslant i \leqslant m)$ and $(\mu_j'\colon 1 \leqslant j \leqslant m')$ of the spaces V and V', respectively, it will sometimes be convenient to identify a bilinear form $f \in \Omega$ with the *matrix*

$$[f_{i,j} = f(\mu_i, \mu_j')\colon 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant m'], \tag{2.4}$$

which represents f in these bases (cf. (2.2)). Note that the rank of the matrix (2.4) is equal to $\operatorname{rk}(f)$ as defined in (2.3).

Let $G = \operatorname{Aut}_F(V)$ and $G' = \operatorname{Aut}_F(V')$ be the *automorphism groups* of V and V'. The group $H = G \times G'$ acts on Ω in the following way. For every (α, α') in H, the (α, α')-image of any $f \in \Omega$ by definition is the bilinear form h given by

$$h(x, x') = f(\alpha x, \alpha' x'). \tag{2.5}$$

Thus H acts on Ω as a subgroup of $\mathrm{Aut}_F(\Omega)$, and the *H-orbits* in Ω are the sets of bilinear forms with constant rank, i.e., the sets

$$\Omega_r = \Omega_r(m, m') = \{f \in \Omega: \mathrm{rk}(f) = r\}, \tag{2.6}$$

for $r = 0, 1,..., m$. This result becomes quite clear if we identify automorphisms as well as bilinear forms with their matrices; then (2.5) becomes $h = \alpha^T f \alpha'$.

As usual, we denote by $\mathbb{Z}\Omega$ the *group ring* of the additive group $(\Omega, +)$ over $\mathbb{Z}$. A typical element A of $\mathbb{Z}\Omega$ is a formal sum

$$A = \sum \{A(f) f: f \in \Omega\}, \qquad A(f) \in \mathbb{Z}. \tag{2.7}$$

(By definition, the product fg of any two elements f and g of Ω must be interpreted as their sum $f + g$ in Ω.) By abuse of notation, we identify each $\Omega_r \subset \Omega$ with the formal sum $\sum \Omega_r$ in $\mathbb{Z}\Omega$. Then it turns out that the Ω_r generate a subring R of $\mathbb{Z}\Omega$, called a *Schur ring* [25]; in other words, one has

$$\Omega_i \Omega_j = \sum_{r=0}^{m} p(i, j, r)\, \Omega_r, \qquad 0 \leqslant i, j \leqslant m, \tag{2.8}$$

for some well-defined nonnegative integers $p(i, j, r)$. This property readily follows from the fact that the Ω_r are the H-orbits in Ω.

Let us emphasize the combinatorial meaning of the above result. If two bilinear forms f and g are called ith associates whenever their q-distance $\mathrm{rk}(f - g)$ equals i, for each $i = 0, 1,..., m$, then Ω becomes an *m-class association scheme* [2] the intersection numbers of which are the structure constants $p(i, j, r)$ of the Schur ring R. Note that $p(i, j, 0)$ equals $v_i \delta_{i,j}$, where $v_i = |\, \Omega_i \,|$ is the ith *valency* and is given by

$$v_i = \prod_{l=0}^{i-1} (q^m - q^l)(q^{m'} - q^l)/(q^i - q^l). \tag{2.9}$$

3. MacWilliams Identities and Inequalities

In this section, bilinear forms are identified with their matrices (2.4). We denote by $\mathrm{tr}(fg^T)$ the natural inner product of any two f and g in Ω, i.e., the trace of the square $m \times m$ matrix fg^T. Let ϵ be a primitive pth root of unity over $\mathbb{Z}$, where p is the prime divisor of q, and let $\chi: F \to \mathbb{Z}[\epsilon]$ be a fixed nonprincipal character of the elementary Abelian p-group $(F, +)$. Then, for any $f \in \Omega$, the mapping

$$g \mapsto \langle f, g \rangle = \chi(\mathrm{tr}(fg^T)), \tag{3.1}$$

from Ω to $\mathbb{Z}[\epsilon]$, clearly is a character of the group $(\Omega, +)$. Moreover, all characters of $(\Omega, +)$ can be represented in this way.

As usual, (3.1) is extended to a ring homomorphism $A \mapsto \langle f, A\rangle$ from $\mathbb{Z}\Omega$ to $\mathbb{Z}[\epsilon]$, by linearity:

$$\langle f, A\rangle = \sum \{A(g)\langle f, g\rangle : g \in \Omega\}. \tag{3.2}$$

With each $k \in \{0, 1,..., m\}$ let us now associate the element Δ_k of the group ring $\mathbb{Z}[\epsilon]\Omega$ defined by $\Delta_k(f) = \langle f, \Omega_k\rangle$, i.e.,

$$\Delta_k = \sum \{\langle f, g\rangle f : f \in \Omega, g \in \Omega_k\}. \tag{3.3}$$

THEOREM 3.1. *The Δ_k belong to the Schur ring $R \subset \mathbb{Z}\Omega$ generated by the orbits $\Omega_0, \Omega_1,..., \Omega_m$.*

Proof. We have to show that $\Delta_k(f)$ is an integer depending only on the rank of f. For $a = 1, 2,..., p - 1$, let $u^{(a)}$ denote the ath conjugate of an element $u \in \mathbb{Z}[\epsilon]$, i.e., the image of u resulting from the substitution $\epsilon \mapsto \epsilon^a$. Using (3.1) and (3.3), we obtain

$$(\Delta_k(f))^{(a)} = \sum \{\langle f, ag\rangle : g \in \Omega_k\}. \tag{3.4}$$

Now from $\mathrm{rk}(ag) = \mathrm{rk}(g)$ it follows that the right member of (3.4) is independent of a. This shows that $\Delta_k(f)$ is a rational integer.

On the other hand, let $h \in \Omega$ have the same rank as the given f, so that $h = \alpha^T f \alpha'$ holds, for suitable $\alpha \in G$ and $\alpha' \in G'$ (see (2.5)). Then (3.1) clearly yields

$$\langle h, g\rangle = \langle f, \alpha g \alpha'^T\rangle, \qquad \text{all } g \in \Omega. \tag{3.5}$$

Taking the sum of (3.5) over $g \in \Omega_k$ we obtain $\langle h, \Omega_k\rangle = \langle f, \Omega_k\rangle$, which is the desired result $\Delta_k(h) = \Delta_k(f)$. ▌

In fact, the elements $|\Omega|^{-1} \Delta_k$ are uniquely determined as the *minimal idempotents* of R. To estabilsh this property, it suffices to prove the orthogonality relations

$$\Delta_k \Delta_l = \delta_{k,l} \,|\Omega|\, \Delta_k, \tag{3.6}$$

for all $k, l = 0, 1,..., m$. Let us now sketch the argument leading to (3.6). Using the definition of group characters we obtain

$$\begin{aligned}(\Delta_k \Delta_l)(f) &= \sum \{\langle f - h, \Omega_k\rangle\langle h, \Omega_l\rangle : h \in \Omega\}\\ &= \sum \{\langle f, g\rangle\langle h, g\Omega_l\rangle : g \in \Omega_k, h \in \Omega\}.\end{aligned} \tag{3.7}$$

Now, for fixed g in Ω_k, the sum of $\langle h, g\Omega_l\rangle$ taken over all $h \in \Omega$ is equal to $|\Omega|\, \delta_{k,l}$. (This is a direct consequence of the orthogonality on group characters.) Hence (3.7) yields (3.6).

A derivation of explicit formulas for the integers $\Delta_k(f)$ is postponed to the Appendix. In agreement with Theorem 3.1 we may write

$$\Delta_k(f) = P_k(i), \qquad \text{for every} \quad f \in \Omega_i. \tag{3.8}$$

The matrix $P = [P_k(i): 0 \leqslant i, k \leqslant m]$ whose (i, k)-entry is (3.8) is referred to as the *character matrix* of R. We mention that $P_0(i) = 1$ and $P_k(0) = v_k$ hold (cf. (2.9)). Moreover, $P_k(i)/v_k$ is symmetric with respect to i and k; consequently, the *orthogonality relations* on the character matrix can be written as

$$P^2 = q^{mm'}I. \tag{3.9}$$

We shall not go into the details of the proof of this result, which reflects the fact that R is a *self-dual* Schur ring [6, 24].

Let X be a nonempty subset of Ω. The *q-distance enumerator* of X is defined to be the formal polynomial

$$a(z) = |X|^{-1} \sum \{z^{\text{rk}(f-g)}: f \in X, g \in X\}. \tag{3.10}$$

Thus the coefficient a_r of z^r in (3.10) equals the average number of elements $g \in X$ at a q-distance r from a fixed $f \in X$. In particular, if X is a subgroup of $(\Omega, +)$, then a_r equals $|X \cap \Omega_r|$. We now state q-analogs of the *MacWilliams relations.*

THEOREM 3.2. *Let P be the character matrix of R. The q-distance enumerator $a(z)$ of any $X \subset \Omega$ satisfies the "MacWilliams inequalities"*

$$\sum_{i=0}^{m} a_i P_k(i) \geqslant 0, \qquad \textit{for all } k. \tag{3.11}$$

Proof. This is a particular case of a general result in association schemes [6]. Let us give a specific proof (see [17], for comparison). We identify X with $\sum X$ in $\mathbb{Z}\Omega$ and write X^* for $\sum(-X)$. By definition, for given $h \in \Omega$, the number $(XX^*)(h)$ counts the ordered pairs (f, g) out of X satisfying $f - g = h$; so it is equal to $|X|\, a_i$ whenever h has rank i. Therefore, using (3.2), (3.3), and (3.8), we have

$$\begin{aligned} |X| \sum_{i=0}^{m} a_i P_k(i) &= \sum \{(XX^*)(h)\langle h, \Omega_k\rangle: h \in \Omega\} \\ &= \sum \{\langle g, XX^*\rangle: g \in \Omega_k\}. \end{aligned} \tag{3.12}$$

Now $\langle g, XX^*\rangle$ clearly is a nonnegative real number (namely, the squared absolute value of $\langle g, X\rangle$). Hence the right member of (3.12) is a nonnegative integer. ▮

Note that, according to (3.12), equality holds in (3.11) for a given k if and only if the character $\langle g, X\rangle$ vanishes for every bilinear form g of rank k.

When X is a subgroup of Ω (in fact, of $(\Omega, +)$), its *dual* is the subgroup $X^{\perp} \subset \Omega$, isomorphic to Ω/X, defined by

$$X^{\perp} = \{g \in \Omega : \langle f, g\rangle = 1 \text{ for all } f \in X\}. \tag{3.13}$$

THEOREM 3.3. *The q-distance enumerators $a(z)$ and $a^{\perp}(z)$ of dual subgroups X and $X^{\perp}$ of Ω are related by the "MacWilliams identities"*

$$a_k^{\perp} = |X|^{-1} \sum_{i=0}^{m} a_i P_k(i), \qquad \textit{for all } k. \tag{3.14}$$

Proof (cf. [6]). Using the well-known property $\langle g, X\rangle = |X|$ or 0 according to whether g belongs to $X^{\perp}$ or not, we obtain

$$\begin{aligned}\sum_{i=0}^{m} a_i P_k(i) &= \sum \{\langle g, X\rangle : g \in \Omega_k\}\\ &= |X|\,|\Omega_k \cap X^{\perp}|,\end{aligned} \tag{3.15}$$

as a consequence of (3.12). Now $a_k^{\perp}$ equals $|\Omega_k \cap X^{\perp}|$. Hence (3.15) yields the desired expression (3.14) for $a_k^{\perp}$. ▌

As indicated by the terminology of duality, $(X^{\perp})^{\perp}$ coincides with X, for every subgroup X of Ω. It is interesting to check that, in view of (3.9), Theorem 3.3 agrees with this property of duality.

4. Codes Derived from Sets of Bilinear Forms

We now associate q-ary codes of length $n = q^{m+m'}$ with subsets X of $\Omega(m, m')$. These codes are defined in the Hamming space (F^W, wt), where the weight wt corresponds to the Lagrange basis of F^W. So, in usual coding terminology, the alphabet is the field F, the locating set is the space W $(= V \times V')$, and the weight $\mathrm{wt}(f)$ of a vector $f \in F^W$ is the number of nonzeros of f in W. The *weight enumerator* of any code $C \subset F^W$ by definition is the polynomial $\sum A_i z^i$, where A_i counts the code words $f \in C$ of weight $\mathrm{wt}(f) = i$, while the *distance enumerator* of C is the polynomial

$$B(z) = |C|^{-1} \sum \{z^{\mathrm{wt}(f-g)} : f \in C, g \in C\}. \tag{4.1}$$

Thus the coefficient B_i of z^i in (4.1) equals the average number of code words f at Hamming distance i from a given code word g. Clearly, if C is a group code, i.e., a subgroup of $(F^W, +)$, then the distance enumerator of C coincides with its weight enumerator.

Let $C_1 \subset F^W$ denote the *first-order generalized Reed–Muller code* [14], that is, the set of affine maps from W to F. Thus a typical element of C_1 can be written as $\psi + \psi' + c$, where ψ and ψ' are linear forms on V and V', respectively, while c is a constant function.

For future use, given $r \in \{0, 1,..., m\}$, we define the trinomial

$$A_r(z) = A_{r,0}z^{w_{r,0}} + A_{r,1}z^{w_{r,1}} + A_{r,2}z^{w_{r,2}} \tag{4.2}$$

in the indeterminate z, where the exponents $w_{r,i}$ and the coefficients $A_{r,i}$ are given by the formulas (with $n = q^{m+m'}$ as before):

$$\begin{aligned} w_{r,0} &= (1 - q^{-1})n, & A_{r,0} &= q(n - q^{2r}),\\ w_{r,1} &= (1 - q^{-1})(1 - q^{-r})n, & A_{r,1} &= q^{2r},\\ w_{r,2} &= (1 - q^{-1} + q^{-1-r})n, & A_{r,2} &= (q - 1)\, q^{2r}. \end{aligned}$$

LEMMA 4.1. *Let f be any bilinear form of rank r on V and V'. The weight enumerator of the code $C_1 + f$ is the trinomial $A_r(z)$.*

Proof. We choose F-bases (μ_i) and (μ_j') for V and V' so as to have the matrix f in canonical form (i.e., $f = I \dotplus 0$). Then, for given $x = \sum x_i\mu_i$ in V and $x' = \sum x_j'\mu_j'$ in V', with $x_i, x_j' \in F$, the (x, x')-coordinate of a typical code word $g \in C_1 + f$ is

$$g(x, x') = \sum_{i=1}^{r} x_ix_i' + \sum_{i=1}^{m} b_ix_i + \sum_{j=1}^{m'} b_j'x_j' + c, \tag{4.3}$$

where the b_i, b_j', and c are arbitrary elements of F. To compute the weight of g we shall distinguish two cases.

(i) Assume there exists at least one nonzero element among the b_i and b_i' with $i > r$. For example, let $r < m$ and $b_m \neq 0$. Then the condition $g(x, x') = 0$ can be expressed as

$$x_m = \psi(x_1 ,..., x_{m-1} , x_1' ,..., x_{m'}'),$$

where ψ is a well-defined polynomial function in $m + m' - 1$ variables over F. Hence, $g(x, x') = 0$ has $q^{m+m'-1}$ roots $(x, x') \in W$. And this conclusion clearly is valid whenever the above assumption holds true.

(ii) Next, assume b_i and b_i' vanish for every $i > r$. Then (4.3) can be written in the form

$$g(x, x') = \sum_{i=1}^{r} (x_i' + b_i)\, x_i + \sum_{i=1}^{r} b_i'x_i' + c. \tag{4.4}$$

For every point $x' \in V'$ satisfying $x_1' = -b_1 ,..., x_r' = -b_r$, it follows from

(4.4) that g is identically zero in x when $c = \sum b_i b_i'$ holds and is never zero otherwise. For any of the remaining points x', it is clear that g admits q^{m-1} zeros in x. Hence the number of roots of $g(x, x') = 0$ is

$$q^{m+m'-r} + q^{m-1}(q^{m'} - q^{m'-r}), \qquad \text{when} \qquad c = \sum_{i=1}^{r} b_i b_i',$$

$$q^{m-1}(q^{m'} - q^{m'-r}), \qquad \text{when} \qquad c \neq \sum_{i=1}^{r} b_i b_i'.$$

The theorem now readily follows from the results of (i) and (ii), by definition of the Hamming weight (namely, wt(g) = number of nonzeros of g). The details are left to the reader. ▮

With a nonempty subset X of Ω let us associate the code $C = C_1 + X$ in F^W. By definition, each $g \in C$ may be viewed as a polynomial function of degree two (at most) in $m + m'$ variables over F; hence C is a subcode of the *second-order generalized Reed–Muller code* (cf. [14]). Note also that C is a group code if and only if X is a subgroup of Ω.

THEOREM 4.2. *Let $X \subset \Omega$. The distance enumerator $B(z)$ of the code $C = C_1 + X$ is the linear combination $\sum a_r A_r(z)$ of the trinomials $A_r(z)$, where the coefficients a_r are those of the q-distance enumerator $a(z) = \sum a_r z^r$ of X.*

Proof. Using definition (4.1), and observing that C_1 is a group code, we readily obtain the formula

$$B(z) = |X|^{-1} \sum \{z^{\text{wt}(h+f-g)}: h \in C_1, f \in X, g \in X\}. \tag{4.5}$$

For any given f and g, the sum over h in the right member of (4.5) is the weight enumerator of $C_1 + f - g$. So, by Lemma 4.1, this sum is equal to $A_r(z)$ whenever rk$(f - g) = r$ holds. Therefore, we deduce

$$\left(a(z) = \sum_{r=0}^{m} a_r z^r\right) \Rightarrow \left(B(z) = \sum_{r=0}^{m} a_r A_r(z)\right),$$

since, by definition (3.10), the number $|X|\ a_r$ precisely counts the pairs (f, g) out of X that satisfy rk$(f - g) = r$. ▮

Among other possible applications we now briefly mention a second construction of codes from sets of bilinear forms. Let $k \in \{1, 2,..., m\}$. With any matrix $f \in \Omega$, let us associate the function

$$f^{(k)}: \Omega_k \to F: g \mapsto f^{(k)}(g) = \text{tr}(fg^T).$$

It is easily seen that the correspondence $f \mapsto f^{(k)}$ is an injective map. So, given a nonempty subset X of Ω, its image $X^{(k)}$ is a q-ary code of length v_k and size $|X|$. The case with $X = \Omega$ and $k = m = m'$ was first introduced by Camion [4].

Define $N_k(i)$ to be the number of matrices $g \in \Omega_k$ having nonzero i-trace (i.e., satisfying $g_{1,1} + \cdots + g_{i,i} \neq 0$). From the definitions we deduce

$$N_k(i) = q^{-1}(q-1)(v_k - P_k(i)).$$

Thus the results of the Appendix yield an analytic expression for $N_k(i)$. It turns out that the Hamming distance enumerator $B^{(k)}(z)$ of the code $X^{(k)}$ is obtained from the q-weight enumerator $a(z)$ of X by the formula

$$B^{(k)}(z) = \sum_{i=0}^{m} a_i z^{N_k(i)},$$

where the weights $N_k(i)$ are defined as above. This result immediately follows from the fact that the mapping $f \mapsto f^{(k)}$ yields a vector space isomorphism from Ω to $\Omega^{(k)}$ satisfying $\mathrm{wt}(f^{(k)}) = N_k(i)$ whenever $\mathrm{rk}(f) = i$ holds.

5. Designs, Codesigns, and Singleton Systems

Let $t \in \{0, 1, \ldots, m\}$. A nonempty subset X of $\Omega(m, m')$ is called a *t-design* if it enjoys the following property. For each t-dimensional subspace V_0 of V and for each bilinear form f_0 on V_0 and V', there is a constant number of bilinear forms $f \in X$ whose restriction to $V_0 \times V'$ equals f_0. This constant is denoted by λ and called the *index* of the t-design; it is clearly related to $|X|$ by

$$\lambda = q^{-tm'} \mid X \mid.$$

THEOREM 5.1. *A given $X \subset \Omega$ is a t-design if and only if its q-distance enumerator $a(z)$ satisfies equality in* (3.11) *for $k = 1, 2, \ldots, t$, i.e.,*

$$\sum_{i=0}^{m} a_i P_k(i) = \mid X \mid \delta_{0,k}, \qquad \textit{when} \qquad k \leqslant t. \tag{5.1}$$

Proof. This is a particular case of a general result concerning t-designs in regular semilattices [7]. ∎

Let $s \in \{0, 1, \ldots, m\}$. A nonempty subset X of $\Omega(m, m')$ is called an *s-codesign* if it enjoys the following property. For all distinct bilinear forms f and g in X, the difference $f - g$ has rank bigger than s. (Conventionally, any one-element subset of Ω is an m-codesign.)

THEOREM 5.2. *A given $X \subset \Omega$ is an s-codesign if and only if its q-distance enumerator satisfies $a_i = \delta_{0,i}$ for all $i \leqslant s$.*

Proof. This is an immediate consequence of the definitions. ▮

THEOREM 5.3. *A subgroup X of $(\Omega, +)$ is a t-design if and only if its dual $X^{\perp}$ is a t-codesign.*

Proof. Apply Theorems 3.3, 5.1, and 5.2. ▮

THEOREM 5.4. *Given $X \subset \Omega(m, m')$, let t and s be the largest integers for which X is a t-design and an s-codesign, respectively. The cardinality of X is bounded by*

$$q^{tm'} \leqslant |X| \leqslant q^{(m-s)m'}. \tag{5.2}$$

Moreover, if one of the bounds (5.2) *is achieved, then so is the other; this happens if and only if $s + t = m$ holds.*

First Proof. The result is trivial in the case $|X| = 1$ (with $t = 0$ and $s = m$). Assume now $|X| \geqslant 2$ and choose any two distinct f and g in X. By definition, $\mathrm{Rad}(f - g)$ has dimension less than $m - s$. So, given any $(m - s)$-dimensional subspace V_0 of V, it is clear that f and g must differ on $V_0 \times V'$. Hence $|X|$ cannot exceed the number of bilinear forms on V_0 and V'. This argument proves the right bound in (5.2) and, in addition, it shows that the bound is tight if and only if X is an $(m - s)$-design of index $\lambda = 1$. The rest of the proof contains no difficulty and is omitted. ▮

Second Proof. From the properties of generalized Krawtchouk polynomials (cf. Appendix) we deduce the following identity on the q-distance enumerator $a(z)$ of the s-codesign X:

$$\sum_{k=1}^{m-s} \begin{bmatrix} m-k \\ s \end{bmatrix} \sum_{i=0}^{m} a_i P_k(i) = \begin{bmatrix} m \\ s \end{bmatrix} (q^{(m-s)m'} - |X|), \tag{5.3}$$

where square brackets denote q-binomial coefficients (cf. [10]). Since, by Theorem 3.2, each term of the left sum in (5.3) is nonnegative, this yields the right bound in (5.2). In addition, it then follows from Theorem 5.1 that the bound is tight if and only if X is an $(m - s)$-design. We omit the "dual" part of the proof. ▮

A t-design of index 1 in $\Omega(m, m')$ is called an *(m, m', t, q)-Singleton system.* According to Theorem 5.4, this may also be viewed as an $(m - t)$-codesign of cardinality $q^{tm'}$. (The present terminology comes from a clear analogy with codes achieving the well-known Singleton bound [22].)

THEOREM 5.5. *Let X be an (m, m', t, q)-Singleton system which is a subgroup of $(\Omega, +)$. Then its dual $X^{\perp}$ is an $(m, m', m - t, q)$-Singleton system.*

Proof. Immediate consequence of Theorems 5.3 and 5.4. ▮

THEOREM 5.6. *The coefficients a_{m-i} $(0 \leqslant i \leqslant t-1)$ of the q-distance enumerator $a(z)$ of any (m, m', t, q)-Singleton system X are expressed in terms of q-binomial coefficients $\left[{w \atop k}\right]$ by the formula*

$$a_{m-i} = \begin{bmatrix} m \\ i \end{bmatrix} \sum_{j=0}^{t-i-1} (-1)^j q^{\binom{j}{2}} \begin{bmatrix} m-i \\ j \end{bmatrix} (q^{(t-i-j)m'} - 1). \tag{5.4}$$

Proof. Owing to Theorems 5.1, 5.2, and 5.4, it suffices to show that the solution to (5.1) with $a_j = \delta_{0,j}$ when $j \leqslant m - t$ and $|X| = q^{tm'}$ is uniquely given by (5.4). We shall not go into details of computation (cf. [10]). ▮

6. CONSTRUCTION OF SINGLETON SYSTEMS

In this section we give constructions of linear (m, m', t, q)-Singleton systems, for all values of the parameters m, m', t, and q. Let us identify V' with the extension field $GF(q^{m'})$ of degree m' of $F = GF(q)$, and let us take for V any fixed m-dimensional subspace of V' over F. We denote by T the *trace* from V' onto F, that is, the linear mapping

$$y \in V' \mapsto T(y) = \sum_{j=0}^{m'-1} y^{q^j} \in F.$$

With any m-tuple $\omega = (\omega_0, \omega_1, \ldots, \omega_{m-1})$ of elements $\omega_j \in V'$, we now associate the function f_ω: $W \to F$ given by

$$f_\omega(x, x') = \sum_{i=0}^{m-1} T(\omega_i x^{q^i} x'), \qquad \text{all } x \in V,\ x' \in V'. \tag{6.1}$$

LEMMA 6.1. *The correspondence $\omega \mapsto f_\omega$ yields an F-isomorphism from the vector space $(V')^m$ to the vector space $\Omega(m, m')$.*

Proof. Straightforward verification shows that any f_ω is a bilinear form on V and V'. On the other hand, the correspondence $\omega \mapsto f_\omega$ clearly is F-linear. So it only remains to be proved that $f_\omega = 0$ implies $\omega_i = 0$ for all i. Define the polynomial

$$p_\omega(x) = \sum_{i=0}^{m-1} \omega_i x^{q^i} \tag{6.2}$$

over the field V'. Thus $f_\omega(x, x')$ equals $T(p_\omega(x)x')$ for all $x \in V$ and $x' \in V'$ (cf. (6.1)). Hence, if f_ω is the zero function, $p_\omega(x)$ must vanish for all x in V, which implies that $p_\omega(x)$ is the zero polynomial. This concludes the proof. ▌

LEMMA 6.2. *Given $r \in \{0, 1,..., m\}$, let $\omega = (\omega_0, \omega_1,..., \omega_{m-1})$ be a nonzero m-tuple over V' satisfying $\omega_j = 0$ for all j bigger than r. Then the corresponding bilinear form f_ω has rank at least $m - r$.*

Proof. From $f_\omega(x, x') = T(p_\omega(x)x')$, with $p_\omega(x)$ as in (6.2), it follows that the left radical $\mathrm{Rad}(f_\omega)$ is the set of zeros of $p_\omega(x)$ in V. Now, by assumption, $p_\omega(x)$ has degree q^r at most, so that it cannot have more than q^r zeros. Hence the dimension of $\mathrm{Rad}(f_\omega)$ is less than or equal to r, which is the desired result. ▌

THEOREM 6.3. *Given $t \in \{0, 1,..., m\}$, define X to be the set of bilinear forms $f_\omega \in \Omega(m, m')$ subject to $\omega_j = 0$ when $j \geqslant t$. Then X is an (m, m', t, q)-Singleton system.*

Proof. Observing that X is a vector space we immediately deduce from Lemma 6.2 that $\mathrm{rk}(f - g) > m - t$ holds for all distinct elements f and g of X, which means that X is an $(m - t)$-codesign. On the other hand, $|X|$ clearly equals $q^{tm'}$ (cf. Lemma 6.1). Hence, application of Theorem 5.4 proves the assertion. ▌

EXAMPLE. When $t = 1$, a typical bilinear form f belonging to the set X of Theorem 6.3 is given by $f(x, x') = T(\omega_0 x x')$, where ω_0 is any fixed element of V'. In the case $q = 2$ and $m' = m$ it turns out that the corresponding code $C = C_1 + X$, of length $n = 2^{2m}$ and size $|C| = 2^{3m+1}$, is equivalent to an extended tri-weight BCH code (cf. [9, 13]). The 2-distance enumerator of the $(m, m, 1, 2)$-Singleton system X clearly is

$$a(z) = 1 + (n^{1/2} - 1)\, z^n.$$

Then, by use of Theorem 4.2, we obtain the following expression for the distance enumerator $B(z)$ of the code $C = C_1 + X$:

$$B(z) = 1 + z^n + 2(n - 1)\, z^{n/2} + n(n^{1/2} - 1)(z^{(n-n^{1/2})/2} + z^{(n+n^{1/2})/2}).$$

APPENDIX: CHARACTER TABLE OF THE SCHUR RING

Our explicit expression (Theorem A2) for the integers $P_k(i) = \Delta_k(f)$ appears as the solution to a rather simple recurrence equation (Lemma A1). As usual, we denote by $c \dotplus f$ the direct sum of a scalar $c \in F$ and a matrix f over F.

LEMMA A1. *Given $i, k \in \{0, 1, \ldots, m\}$, and $f \in \Omega_i(m, m')$, one has*

$$\Delta_{k+1}(0 \dotplus f) - \Delta_{k+1}(1 \dotplus f) = q^{m+m'-i+1}\, \Delta_k(f). \tag{A1}$$

Proof. From the definition (3.3) of Δ_k we readily deduce that the left member $\mu_k(f)$ of (A1) is equal to

$$\mu_k(f) = \sum \{\langle 0 \dotplus f, g\rangle (1 - \chi(\hat{g}_{1,1})) \colon \hat{g} \in \Omega_{k+1}(m+1, m'+1)\}. \tag{A2}$$

A matrix $\hat{g} \in \Omega(m+1, m'+1)$ with nonzero entry $\hat{g}_{1,1} = c$ is equivalent to a matrix of the form $c \dotplus g$; more precisely, we refer to the identity

$$\begin{bmatrix} 1 & 0 \\ a\xi & I \end{bmatrix} \begin{bmatrix} c & \xi' \\ \xi & h \end{bmatrix} \begin{bmatrix} 1 & a\xi' \\ 0 & I \end{bmatrix} = \begin{bmatrix} c & 0 \\ 0 & g \end{bmatrix}, \tag{A3}$$

of the type $\alpha^T \hat{g} \alpha' = c \dotplus g$, where $a = -c^{-1}$ and $g = h + a\xi\xi'$. (Thus ξ is an m-column, ξ' an m'-row, while g and h are $m \times m'$ matrices.) For given u in $\Omega(m, m')$, let $N(u)$ be the number of pairs (ξ, ξ') for which $\xi\xi'$ equals u. Then, owing to (A3), it is easily seen that (A2) can be written as

$$\mu_k(f) = \sum \{N(u) \langle f, g + c^{-1}u\rangle (1 - \chi(c)) \colon \\ c \in F \backslash \{0\},\ g \in \Omega_k(m, m'),\ u \in \Omega(m, m')\}. \tag{A4}$$

It is obvious that $N(u)$ only depends on $\operatorname{rk}(u)$ and is zero whenever $\operatorname{rk}(u) \geqslant 2$ holds. Thus, if we write $N_j = N(u)$ for $j = \operatorname{rk}(u)$, then (A4) becomes

$$\mu_k(f) = q\Delta_k(f) \sum_{j=0}^{1} N_j \Delta_j(f), \tag{A5}$$

by definition and by application of $\sum \{\chi(c) \colon c \in F\} = 0$. We now make use of the numerical values of the N_j, namely:

$$N_0 = q^m + q^{m'} - 1, \qquad N_1 = q - 1. \tag{A6}$$

Substitution of (A6) into (A5) with $k = 0$ yields a recurrence formula on the numbers $\Delta_1(g)$. Using the initial value $\Delta_1(0) = v_1$ given by (2.9) we obtain as a solution for $\Delta_1(f)$ the expression

$$\Delta_1(f) = (q^{m+m'-i} - q^m - q^{m'} + 1)/(q - 1). \tag{A7}$$

The details of the verification are left to the reader. (A direct proof of (A7) can also be easily found.) Finally, substituting (A7) into (A5) and using (A6) we arrive at the desired formula (A1). ∎

For future use we now recall the definition of Gaussian polynomials $\left[\begin{smallmatrix} w \\ j \end{smallmatrix}\right]$, also called *q-binomial coefficients*. They are defined for all nonnegative integers w and j from the q-analog of the Pascal triangle formula, i.e.,

$$\begin{bmatrix} w+1 \\ j+1 \end{bmatrix} = \begin{bmatrix} w \\ j+1 \end{bmatrix} + q^{w-j} \begin{bmatrix} w \\ j \end{bmatrix}, \tag{A8}$$

together with $[{w \atop 0}] = 1$ and $[{w \atop j}] = 0$ when $j > w$. (We point out that $[{w \atop j}]$ counts the j-dimensional subspaces of a fixed w-dimensional vector space over $F = GF(q)$.) The explicit solution to (A8) is given by

$$\begin{bmatrix} w \\ j \end{bmatrix} = \prod_{l=0}^{j-1} (q^{w-l} - 1)/(q^{j-l} - 1). \tag{A9}$$

THEOREM A2. *For given i and k in $\{0, 1,..., m\}$, the (i, k)-entry of the character matrix P is expressed in terms of q-binomial coefficients* (A9) *as*

$$P_k(i) = \sum_{j=0}^{m} (-1)^{k-j} q^{jm'+\binom{k-j}{2}} \begin{bmatrix} m-j \\ m-k \end{bmatrix} \begin{bmatrix} m-i \\ j \end{bmatrix}. \tag{A10}$$

Proof. We have to show that $\Delta_k(f)$ coincides with (A10) for all f in $\Omega_i(m, m')$. First, we observe that the "initial value" $v_k = \Delta_k(0)$ is correctly given by (A10) with $i = 0$ (cf. (2.9)). Now let $\pi_{k,j}(i, m, m')$ denote the term of index j in the right member of (A10). As a direct consequence of (A8) we obtain the identity

$$\begin{aligned} \pi_{k+1,j+1}(i, m+1, m'+1) - \pi_{k+1,j+1}(i+1, m+1, m'+1) \\ = q^{m+m'-i+1} \pi_{k,j}(i, m, m'). \end{aligned}$$

Hence (A10) yields the unique solution to the recurrence (A1) with initial values $\Delta_k(0) = v_k$. So the theorem follows from Lemma A1. ▮

It is easily seen from (A10) that $P_k(i)$ is a polynomial of degree k with respect to the variable q^{-i}. In fact, the $P_k(i)$ belong to the family of *generalized Krawtchouk polynomials* (cf. [8]). They satisfy the orthogonality relations

$$\sum_{i=0}^{m} v_i P_k(i) P_l(i) = |\Omega| v_k \delta_{k,l} \tag{A11}$$

for all $k, l = 0, 1,..., m$. We finally mention, without proof, a nice expression of generalized Krawtchouk polynomials in terms of basic hypergeometric functions ${}_2\phi_2$, namely:

$$P_k(i)/v_k = {}_2\phi_2(q^{-k}, q^{-i}; q^{-m}, q^{-m'}; q; q).$$

This obviously yields the symmetry relation $P_k(i)/v_k = P_i(k)/v_i$, which shows that (3.9) is an equivalent version of (A11).

REFERENCES

1. E. F. ASSMUS, JR., H. F. MATTSON, JR. AND R. TURYN, "Cyclic Codes," Air Force Cambridge Res. Lab. Sum. Rept. 4 (1965).
2. R. C. BOSE AND D. M. MESNER, On linear associative algebras corresponding to association schemes of partially balanced designs, *Ann. Math. Statist.* 4 (1959), 31–38.

3. P. J. Cameron and J. J. Seidel, Quadratic forms over $GF(2)$, *Indag. Math.* **35** (1973), 1–8.
4. P. Camion, Linear codes with given automorphism groups, *Discrete Math.* **3** (1972), 33–45.
5. P. Delsarte, Bounds for unrestricted codes, by linear programming, *Philips Res. Rep.* **27** (1972), 272–289.
6. P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.* **10** (1973).
7. P. Delsarte, Association schemes and t-designs in regular semilattices, *J. Combinatorial Theory Ser. A* **20** (1976), 230–243.
8. P. Delsarte, Properties and applications of the recurrence $F(i + 1, k + 1, n + 1) = q^{k+1} F(i, k + 1, n) - q^k F(i, k, n)$, *SIAM J. Appl. Math.* **31** (1976), 262–270.
9. P. Delsarte and J. M. Goethals, Tri-weight codes and generalized Hadamard matrices, *Inform. Contr.* **15** (1969), 196–206.
10. P. Delsarte and J. M. Goethals, Alternating bilinear forms over $GF(q)$, *J. Combinatorial Theory, Ser. A* **19** (1975), 26–50.
11. J. M. Goethals, A polynomial approach to linear codes, *Philips Res. Rep.* **24** (1969), 145–159.
12. J. M. Goethals, Nonlinear codes defined by quadratic forms over $GF(2)$, *Inform. Contr.* **31** (1976), 43–74.
13. T. Kasami, Weight distribution of Bose–Chaudhuri–Hocquenghem codes, *in* "Combinatorial Mathematics and Its Applications" (R. C. Bose and T. A. Dowling, Eds.), pp. 335–357, Univ. of North Carolina Press, Chapel Hill, 1969.
14. T. Kasami, S. Lin, and W. W. Peterson, New generalizations of the Reed–Muller codes. I. Primitive codes, *IEEE Trans. Information Theory* **IT-14** (1968), 189–198.
15. A. M. Kerdock, A class of low-rate nonlinear binary codes, *Inform. Contr.* **20** (1972), 182–187.
16. F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell System Tech. J.* **42** (1963), 79–94.
17. F. J. MacWilliams, N. J. A. Sloane and J. M. Goethals, The MacWilliams identities for nonlinear codes, *Bell System Tech. J.* **51** (1972), 803–819.
18. A. Marguinaud, Codes à distance maximale, *Revue CETHEDEC* **22** (1970), 33–46.
19. N. J. Patterson, A four-dimensional Kerdock set over $GF(3)$, *J. Combinatorial Theory, Ser. A* **20** (1976), 365–366.
20. C. R. Rao, Factorial experiments derivable from combinatorial arrangements of arrays, *J. Roy. Statist. Soc. Suppl.* **9** (1947), 128–139.
21. I. S. Reed and G. Solomon, Polynomial codes over certain finite fields, *J. SIAM* **8** (1960), 300–304.
22. R. C. Singleton, Maximum distance Q-nary codes, *IEEE Trans. Information Theory* **IT–10** (1964), 116–118.
23. G. Szegö, "Orthogonal Polynomials," American Mathematical Society Colloquium Publications, Vol. 23, Amer. Math. Soc., Providence, R.I., 1959.
24. O. Tamaschke, Zur Theorie der Permutationsgruppen mit regulärer Untergruppe, *Math. Z.* **80** (1963), 328–352.
25. O. Tamaschke, "Schur–Ringe," B.I-Hochschulskripten 735 a*, Bibliographisches Institut, Mannheim, 1970.