On the Delsarte inequalities

Report 96-87

Alexey Ashikhmin
Juriaan Simonis

TU Delft
Technische Universiteit Delft
Delft University of Technology

Faculteit der Technische Wiskunde en Informatica
Faculty of Technical Mathematics and Informatics

ISSN 0922-5641

Copyright © 1996 by the Faculty of Technical Mathematics and Informatics, Delft, The Netherlands.
No part of this Journal may be reproduced in any form, by print, photoprint, microfilm, or any other means without permission from the Faculty of Technical Mathematics and Informatics, Delft University of Technology, The Netherlands.

Copies of these reports may be obtained from the bureau of the Faculty of Technical Mathematics and Informatics, Julianalaan 132, 2628 BL Delft, phone $+31152784568$.
A selection of these reports is available in PostScript form at the Faculty's anonymous ftp-site. They are located in the directory /pub/publications/tech-reports at ftp.twi.tudelft.nl

On the Delsarte Inequalities

Alexey Ashikhmin and Juriaan Simonis
Delft University of Technology,
Faculty of Technical Mathematics and Informatics,
Department of Pure Mathematics,
Mekelweg 4,
2600 GA Delft, the Netherlands

September 10, 1996

Abstract

In this paper, two new proofs of the Delsarte inequalities for unrestricted codes over an arbitrary alphabet are presented. These inequalities are strengthened for the case that the size of the code is not divisible by the alphabet size.

1 The Delsarte inequalities

Let F be a finite set of size $q > 1$. We identify the direct product F^n of n copies of F with the set F^S of all mappings of the coordinate index set $S := \{1, 2, \ldots, n\}$ into F. This will be convenient later on, when we shall consider arbitrary subsets of S. The set F^S is a metric space with respect to the *Hamming distance*

$$d(x, y) := |\{i \in S \mid x_i \neq y_i\}|.$$

We shall call this metric space a q-ary *Hamming space* of length n.

Definition 1 *A code $\mathcal{C}$ in F^S is a multiset consisting of elements of F^S. (A multiset is an unordered list, with repetitions allowed.)*

Remark 1 *Most authors use the term "code" for* subsets *of F^S. But our extension will turn out to be very useful in some of the proofs.*

Definition 2 *The* distance distribution *of $\mathcal{C}$ is the sequence*

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

with

$$A_i(\mathcal{C}) := \frac{1}{|\mathcal{C}|}|\{(x,y) \mid x,y \in \mathcal{C} \text{ and } d(x,y) = i\}|.$$

The Delsarte inequalities are a set of linear inequalities in the $A_i(\mathcal{C})$. The coefficients involved are the so-called *Krawtchouk numbers.*

Definition 3 *The q-ary* Krawtchouk numbers *are the integers*

$$K_\alpha(j;q) := \sum_{i=0}^{\alpha} (-1)^i (q-1)^{\alpha-i} \binom{j}{i} \binom{n-j}{\alpha-i}.$$

Theorem 1 *(The Delsarte inequalities. Cf. [4].) The codes $\mathcal{C}$ in F^S satisfy the $n+1$ inequalities*

$$\sum_{j=0}^{n} K_\alpha(j;q) A_j(\mathcal{C}) \geq 0, \qquad \alpha = 0, 1, \ldots, n.$$

Since $K_0(j;q) = 1$ for $j = 0, 1, \ldots, n$, we can replace the first inequality can be replaced by the (obvious) equality

$$\sum_{j=0}^{n} A_j(\mathcal{C}) = |\mathcal{C}|.$$

The Delsarte inequalities are the basis of the linear programming bound for the maximum size of codes that satisfy certain conditions on the weight distribution. A nice survey paper is [5].

2 Known proofs of the Delsarte inequalities

Delsarte proved his result within the context of the theory of association schemes. The metric space F^S is an association scheme. Let Q be its second eigenmatrix, and let a be the row vector

$$a := (A_0(\mathcal{C}), A_1(\mathcal{C}), \ldots, A_n(\mathcal{C})).$$

Then the components of the vector aQ are nonnegative (Theorem 3.3 in [4]) and the entries of Q are the Krawtchouk numbers (section 4.1 in [4]) The

latter fact is proved using a group structure on the set F and an isomorphism of F into its character group F^*.

Introductory texts like [7] usually simplify the proof above by avoiding any reference to association schemes and taking advantage of the particularly simple structure of the Hamming scheme. Yet these proofs need the introduction of a group structure on F and the fact that the sum of the values of a character over a group F is either $|F|$ or 0.

A third approach uses a generalized Plotkin type argument which runs as follows. The zeroth Delsarte inequality follows from

$$\sum_{j=0}^{n} A_j(\mathcal{C}) = |\mathcal{C}|$$

and the first Delsarte inequality

$$\sum_{j=0}^{n} \{(q-1)n - qj\} A_j(\mathcal{C}) \geq 0$$

can be derived by a combinatorial argument which usually is applied to derive the Plotkin bound. Now, using an identification $F = \mathbb{Z}_q$, for each $\alpha > 1$ one can create a new (and much longer) code $\mathcal{C}_\alpha$ such that the first Delsarte inequality for $\mathcal{C}_\alpha$ yields the αth Delsarte inequality for $\mathcal{C}$. This approach is described in [6].

All proofs known to the authors use some algebra to derive a purely combinatorial result. Since this fact may block generalizations, for instance in the direction of linear programming bounds for generalized weights of unrestricted codes, a purely combinatorial proof might be of interest.

3 Binary Hamming spaces in a q-ary Hamming space

For any choice of n 2-element subsets $B_i \in \binom{F}{2}$, $i \in S$, the product

$$\mathcal{D} := \prod_{i \in S} B_i \subseteq F^S$$

is a subspace of the q-ary Hamming space which is isometric to the *binary* Hamming spaces of length n.

Example 1 *Take* $F := \{0,1,2\}$, $S := \{1,2\}$, $B_1 := \{0,1\}$ *and* $B_2;= \{1,2\}$. *Then*

$$F^S = \begin{bmatrix} 00 \\ 01 \\ 02 \\ 10 \\ 11 \\ 12 \\ 20 \\ 21 \\ 22 \end{bmatrix} \text{ and } \mathcal{D} = \begin{bmatrix} 01 \\ 02 \\ 11 \\ 12 \end{bmatrix}.$$

Definition 4

$$\mathfrak{B} = \mathfrak{B}(F^S) := \{\prod_{i\in S} B_i \mid B_i \in \tbinom{F}{2}, i \in S\}.$$

Note that the size of $\mathfrak{B}$ is equal to $\binom{q}{2}^n$.

We give two characterizations of the elements of $\mathfrak{B}$. They are not relevant for the proof of the main result, but may turn out to be useful in other contexts.

Proposition 1 *A nonempty subset* $\mathcal{D} \in F^S$ *is isometric to a binary Hamming space of length* n *if and only if* $\mathcal{D} \in \mathfrak{B}$.

Proof. The "if" part is obvious. Suppose that $\mathcal{D}$ is isometric to a binary Hamming space of length n. Let a be any element of $\mathcal{D}$ and let b be the (unique) element of $\mathcal{D}$ with $d(a,b) = n$. Then for all $x \in D$ we have

$$d(a,x) + d(b,x) = n.$$

This equality implies that for all $i \in S$ either $x_i = a_i$ or $x_i = b_i$. ■

Proposition 2 *A nonempty subset* $\mathcal{D} \subseteq F^S$ *is an element of* $\mathfrak{B}$ *if and only if* $\mathcal{D}$ *is distance invariant and* $A_i(\mathcal{D}) = \binom{n}{i}$ *for* $i \in S$.

Proof. The "only if" part is clear. As to the "if" part, choose an element $a \in \mathcal{D}$ and let b be the element of $\mathcal{D}$ with $d(a,b) = n$. So $a_i \neq b_i$ for $i \in S$. The total number of coordinates in $\mathcal{D}$ is equal to $n2^n$. The number of coordinates in $\mathcal{D}$ that are equal to the corresponding coordinate of a is equal to

$$\sum_i (n-i)\binom{n}{i} = \frac{n}{2}2^n.$$

Likewise the number of coordinates in $\mathcal{D}$ that are equal to the corresponding coordinate of b is equal to $\frac{n}{2}2^n$. So

$$\mathcal{D} = \prod_{i \in S} \{a_i, b_i\}.$$

■

Remark 2 *The following example shows that the condition of distance invariance is necessary: Take* $F := \{0, 1, 2\}$, $n := 2$ *and* $\mathcal{D} := \{00, 11, 21, 01\}$. *Then* $A_0(\mathcal{D}) = A_2(\mathcal{D}) = 1$ *and* $A_1(\mathcal{D}) = 2$, *but* $\mathcal{D} \notin \mathfrak{B}$.

Remark 3 *In general, we could, for arbitrary* r, *consider sets of the form*

$$\mathfrak{B}_r := \{\prod_{i \in S} B_i \mid B_i \in \tbinom{F}{r}, i \in S\}.$$

One might be tempted to conjecture that each distance invariant subset $\mathcal{D} \in F^S$ *with* $A_i(\mathcal{D}) = (r-1)^i \binom{n}{i}$, $i = 0, 1, \ldots, n$, *is an element of* $\mathfrak{B}_r$. *However the following example shows that this is not true. Take* $F := \{1, 2, \ldots, 12\}$, *and let* $\mathcal{D} \in F^2$ *the code consisting of the 36 words*

1 2	2 2	3 2	4 1	5 1	6 1	7 1	8 1	9 1	10 1	11 1	12 1
1 3	2 3	3 3	4 3	5 3	6 3	7 2	8 2	9 2	10 2	11 2	12 2
1 4	2 4	3 4	4 4	5 4	6 4	7 4	8 4	9 4	10 3	11 3	12 3

Then $\mathcal{D}$ *is a distance invariant code with* $A_i(\mathcal{D}) = (6-1)^i \binom{2}{i}$, $i = 0, 1, 2$, *but* $\mathcal{D} \notin \mathfrak{B}_6$. *Another counterexample to the conjecture has been communicated to the authors by E.M. Gabidulin.*

Back to the binary case. In a *binary* Hamming space, the relation

$$x \backsim y \Longleftrightarrow d(x, y) \equiv 0 (\text{mod } 2)$$

is an equivalence relation. There are exactly two equivalence classes, which have the same size. So for each $\mathcal{D} \in \mathfrak{B}$, we define $\{\mathcal{D}_0, \mathcal{D}_1\}$ to be the partition induced by the equivalence relation

$$x \backsim y \Longleftrightarrow d(x, y) \equiv 0 (\text{mod } 2)$$

on $\mathcal{D}$.

Example 2 *(Continuation of example 1.) The two equivalence classes in* $\mathcal{D}$ *are the subsets* $\{01, 12\}$ *and* $\{02, 11\}$.

4 Restrictions of codes

Let I be a subset of S of size α. For any $x \in F^S$, we denote by x_I the restriction of x to I. More generally, if $\mathcal{C}$ is a code in F^S, then $\mathcal{C}_I$ is the code in F^I consisting of the restrictions c_I, $c \in \mathcal{C}$. Note that $|\mathcal{C}_I| = |\mathcal{C}|$. Observe that the multiset $\mathcal{C}_I$ generally will have multiple elements even if $\mathcal{C}$ is a *set*. So here we can take advantage of our more general definition of a code.

The weight distribution of a code and those of its restrictions to sets of a given size are linked by a simple equation.

Proposition 3

$$\sum_{j=0}^{n} \binom{j}{i}\binom{n-j}{\alpha-i} A_j(\mathcal{C}) = \sum_{I \in \binom{S}{\alpha}} A_i(\mathcal{C}_I). \tag{1}$$

Proof. The *support* $\operatorname{supp}(c, c')$ of a pair $(c, c') \in \mathcal{C} \times \mathcal{C}$ is defined to be the subset of S consisting of the indices $u \in S$ for which $c_u \neq c'_u$. So $d(c, c') = |\operatorname{supp}(c, c')|$. Suppose that the pair $(c, c') \in \mathcal{C} \times \mathcal{C}$ contributes to $|\mathcal{C}|A_j(\mathcal{C})$, i.e. that $|\operatorname{supp}(c, c')| = j$. The restricted pair (c_I, c'_I) contributes to $|\mathcal{C}|A_i(\mathcal{C}_I)$ if and only if the intersection $I \cap \operatorname{supp}(c, c')$ has size i. There are exactly $\binom{j}{i}\binom{n-j}{\alpha-i}$ subsets $I \in \binom{S}{\alpha}$ for which this holds. Summing over all pairs $(c, c') \in \mathcal{C} \times \mathcal{C}$, we obtain

$$\sum_{j=0}^{n} \binom{j}{i}\binom{n-j}{\alpha-i} |\mathcal{C}|A_j(\mathcal{C}) = \sum_{I \in \binom{S}{\alpha}} |\mathcal{C}|A_i(\mathcal{C}_I).$$

■

5 A new proof of the Delsarte inequalities

Lemma 1 *Let F, I be finite sets of size q, α respectively, and let $\mathcal{C}$ be a code in F^I. Then*

$$\sum_{i=0}^{\alpha} (-1)^i (q-1)^{\alpha-i} |\mathcal{C}|A_i(\mathcal{C}) = \sum_{\mathcal{D} \in \mathfrak{B}(F^I)} (|\mathcal{C} \cap \mathcal{D}_0| - |\mathcal{C} \cap \mathcal{D}_1|)^2.$$

Proof. For $c \in \mathcal{C}$ and $\mathcal{D} = \mathcal{D}_0 \cup \mathcal{D}_1 \in \mathfrak{B}(F^I)$, put

$$\delta(c, \mathcal{D}_i) := \begin{cases} 1 & \text{if} \quad c \in \mathcal{D}_i, \\ 0 & \text{if} \quad c \notin \mathcal{D}_i. \end{cases}.$$

Then

$$|\mathcal{C} \cap \mathcal{D}_i| = \sum_{c \in \mathcal{C}} \delta(c, \mathcal{D}_i), \quad i = 0, 1,$$

and

$$\sum_{\mathcal{D} \in \mathfrak{B}(F^I)} (|\mathcal{C} \cap \mathcal{D}_0| - |\mathcal{C} \cap \mathcal{D}_1|)^2 = \sum_{\mathcal{D} \in \mathfrak{B}(F^I)} \{\sum_{c \in \mathcal{C}} \delta(c, \mathcal{D}_0) - \sum_{c \in \mathcal{C}} \delta(c, \mathcal{D}_1)\}^2.$$

Changing the order of summation in the right hand side of this identity and expanding the squares we obtain

$$\sum_{\mathcal{D} \in \mathfrak{B}(F^I)} (|\mathcal{C} \cap \mathcal{D}_0| - |\mathcal{C} \cap \mathcal{D}_1|)^2 = \sum_{c, c' \in \mathcal{C}} \sum_{\mathcal{D} \in \mathfrak{B}(F^I)} \Delta(c, c', \mathcal{D}),$$

with

$$\begin{aligned} \Delta(c, c', \mathcal{D}) &= \delta(c, \mathcal{D}_0)\delta(c', \mathcal{D}_0) + \delta(c, \mathcal{D}_1)\delta(c', \mathcal{D}_1) - \\ &\quad \delta(c, \mathcal{D}_0)\delta(c', \mathcal{D}_1) - \delta(c, \mathcal{D}_1)\delta(c', \mathcal{D}_0). \end{aligned}$$

If $\{c, c'\} \not\subseteq \mathcal{D}$, the value of $\Delta(c, c', \mathcal{D})$ is 0. If not, it is equal to $(-1)^{d(c,c')}$. Moreover, the number of binary Hamming spaces $\mathcal{D} \subseteq F^I$ that contain a fixed pair $\{c, c'\}$ is equal to $(q-1)^{\alpha - d(c,c')}$. Hence

$$\sum_{\mathcal{D} \in \mathfrak{B}(F^I)} (|\mathcal{C} \cap \mathcal{D}_0| - |\mathcal{C} \cap \mathcal{D}_1|)^2 = \sum_{i=0}^{\alpha} (-1)^i (q-1)^{\alpha - i} |\mathcal{C}| A_i(\mathcal{C}).$$

■

Theorem 2 *Let F, S be finite sets of size q, n respectively. Then the codes $\mathcal{C}$ in F^S satisfy the $n+1$ identities*

$$|\mathcal{C}| \sum_{j=0}^{n} K_\alpha(j; q) A_j(\mathcal{C}) = \sum_{I \in \binom{S}{\alpha}} \sum_{\mathcal{D} \in \mathfrak{B}(F^I)} (|\mathcal{C}_I \cap \mathcal{D}_0| - |\mathcal{C}_I \cap \mathcal{D}_1|)^2. \qquad (2)$$

Proof. Apply lemma 1 to the codes $\mathcal{C}_I$, $I \in \binom{S}{\alpha}$:

$$\sum_{i=0}^{\alpha} (-1)^i (q-1)^{\alpha - i} |\mathcal{C}| A_i(\mathcal{C}_I) = \sum_{\mathcal{D} \in \mathfrak{B}(F^I)} (|\mathcal{C}_I \cap \mathcal{D}_0| - |\mathcal{C}_I \cap \mathcal{D}_1|)^2.$$

(Note that $|\mathcal{C}_I| = |\mathcal{C}|$ for all subsets $I \subseteq S$.) Substitution of the resulting expression for $A_i(\mathcal{C}_I)$ in the identity 1 yields

$$\sum_{j=0}^{n} (-1)^i (q-1)^{\alpha - i} \binom{j}{i} \binom{n-j}{\alpha - i} |\mathcal{C}| A_j(\mathcal{C}) = \sum_{I \in \binom{S}{\alpha}} \sum_{\mathcal{D} \in \mathfrak{B}(F^I)} (|\mathcal{C}_I \cap \mathcal{D}_0| - |\mathcal{C}_I \cap \mathcal{D}_1|)^2.$$

Finally, recall definition 3:

$$K_\alpha(j;q) := \sum_{i=0}^{\alpha}(-1)^i(q-1)^{\alpha-i}\binom{j}{i}\binom{n-j}{\alpha-i}.$$

■

Corollary 1 *Since the right hand side of equation 2 is a sum of squares, we immediately have the Delsarte inequalities:*

$$\sum_{j=0}^{n} K_\alpha(j;q)A_j(\mathcal{C}) \geq 0.$$

Remark 4 *For a given α, we have*

$$\sum_{j=0}^{n} K_\alpha(j;q)A_j(\mathcal{C}) = 0$$

if and only if for all α-subsets $I \subseteq S$ and for all binary Hamming spaces $\mathcal{D} \subset F^I$ the equality

$$|\mathcal{C}_I \cap \mathcal{D}_0| = |\mathcal{C}_I \cap \mathcal{D}_1|$$

holds.

6 Another proof

In this section, we present a proof of the Delsarte inequalities that is closely related to the fact that the Hamming scheme of length n is the Kronecker product of n Hamming schemes of length 1. Cf. [4], p. 18, or [3], section 5.1.2..

Let F be a finite set of size q, and let $\mathbb{R}^F$ be the real vector space of the q-tuples indexed by F.

Definition 5 *The quadratic form Q on $\mathbb{R}^F$ is defined by*

$$Q(\boldsymbol{\xi}) := \sum_{x,y\in F} \delta(x,y)\xi_x\xi_y,$$

with

$$\delta(x,y) := \begin{cases} q-1 & \text{if } x = y, \\ -1 & \text{otherwise.} \end{cases}$$

Example 3 *If $F := \{0, 1, 2\}$, then the matrix of Q with respect to the standard basis of $\mathbb{R}^F$ is*

$$\begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}.$$

Proposition 4

$$Q(\boldsymbol{\xi}) \geq 0 \text{ for all } \boldsymbol{\xi} \in \mathbb{R}^F.$$

Proof. The result immediately follows from the fact that the eigenvalues of Q are nonnegative. In fact, they are equal to 0 (with multiplicity 1) and q (with multiplicity $q-1$). A second proof runs as follows:
For each set $B := \{u, v\} \in \binom{F}{2}$, we define a quadratic form R_B on $\mathbb{R}^F$ by

$$R_B(\boldsymbol{\xi}) := (\xi_u - \xi_v)^2.$$

Then

$$Q = \sum_{B \in \binom{F}{2}} R_B. \tag{3}$$

■

Example 4 *The matrix in the preceding example can be written as*

$$\begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{bmatrix}.$$

Now, let I be a finite set of size α. We consider the vector space $\mathbb{R}^{(F^I)} \cong \otimes_I \mathbb{R}^F$.

Definition 6 *The quadratic form Q^I on $\mathbb{R}^{(F^I)}$ is defined by*

$$Q^I(\boldsymbol{\xi}) := \sum_{x,y \in F^I} \prod_{j \in I} \delta(x_j, y_j) \xi_x \xi_y = \sum_{i=0}^{\alpha} (-1)^i (q-1)^{\alpha - i} \sum_{d(x,y)=i} \xi_x \xi_y.$$

We can identify Q^I with the α-fold tensor product $\otimes_I Q$ on the space $\otimes_I \mathbb{R}^F$. The matrix of Q^I with respect to the standard basis of $\mathbb{R}^{(F^I)}$ is the α-fold Kronecker product of the standard matrix of Q.

Example 5 *If $F := \{0,1,2\}$, $I := \{1,2\}$, the matrix of Q^I is*

$$\begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}^{\otimes 2} = \begin{bmatrix} 4 & -2 & -2 & -2 & 1 & 1 & -2 & 1 & 1 \\ -2 & 4 & -2 & 1 & -2 & 1 & 1 & -2 & 1 \\ -2 & -2 & 4 & 1 & 1 & -2 & 1 & 1 & -2 \\ -2 & 1 & 1 & 4 & -2 & -2 & -2 & 1 & 1 \\ 1 & -2 & 1 & -2 & 4 & -2 & 1 & -2 & 1 \\ 1 & 1 & -2 & -2 & -2 & 4 & 1 & 1 & -2 \\ -2 & 1 & 1 & -2 & 1 & 1 & 4 & -2 & -2 \\ 1 & -2 & 1 & 1 & -2 & 1 & -2 & 4 & -2 \\ 1 & 1 & -2 & 1 & 1 & -2 & -2 & -2 & 4 \end{bmatrix}.$$

(The rows and columns are parametrized by F^I in lexicographical order.)

Remark 5 *With a binary Hamming space $\mathcal{D} := \prod_{i\in I} B_i$ we can associate the quadratic form*

$$R_{\mathcal{D}} := \bigotimes_{i\in I} R_{B_i}, \tag{4}$$

on $\mathbb{R}^{(F^I)}$. Then formula 3 implies that

$$Q^I = \bigotimes_{i\in I} \sum_{B_i \in \binom{F}{2}} R_{B_i} = \sum_{\prod_{i\in I} B_i \in \binom{F}{2}^I} \bigotimes_{i\in I} R_{B_i} = \sum_{\mathcal{D}\in\mathfrak{B}(F^I)} R_{\mathcal{D}}. \tag{5}$$

Example 6 *(Continuation of the preceding example). Take $B_1 := \{0,1\}$, $B_2 := \{1,2\}$ and $\mathcal{D} := B_1 \times B_2$. Then, again using the matrix notation, we have*

$$R_{B_1} = \begin{bmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad R_{B_2} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{bmatrix}$$

and

$$R_{\mathcal{D}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

This is one of the nine matrices that sum up to the matrix of Q^I.

Proposition 5

$$Q^I(\boldsymbol{\xi}) \geq 0 \text{ for all } \boldsymbol{\xi} \in \mathbb{R}^{(F^I)}.$$

Proof. The eigenvalues of the tensor product of α copies of a quadratic form Q are all possible products of α eigenvalues of Q. ■

Now we consider codes in F^I.

Definition 7 *The* characteristic vector *of a code $\mathcal{C}$ in F^I is the element $\chi_{\mathcal{C}}$ of $\mathbb{R}^{(F^I)}$ defined by*

$$(\chi_{\mathcal{C}})_x := |\{c \in \mathcal{C} \mid c = x\}|.$$

Lemma 2 *Let F, I be finite sets of size q, α respectively, and let $\mathcal{C}$ be a code in F^I. Then*

$$\sum_{i=0}^{\alpha} (-1)^i (q-1)^{\alpha-i} |\mathcal{C}| A_i(\mathcal{C}) = Q^I(\chi_{\mathcal{C}}).$$

Proof. The right hand side is equal to

$$\sum_{i=0}^{\alpha} (-1)^i (q-1)^{\alpha-i} \sum_{d(x,y)=i} (\chi_{\mathcal{C}})_x (\chi_{\mathcal{C}})_y,$$

and

$$\begin{aligned} \sum_{d(x,y)=i} (\chi_{\mathcal{C}})_x (\chi_{\mathcal{C}})_y &= |\{(x,y) \mid x, y \in \mathcal{C} \text{ and } d(x,y) = i\}| \\ &= |\mathcal{C}| A_i(\mathcal{C}). \end{aligned}$$

■

Remark 6 *In view of equation 5, we can rewrite this result in the form*

$$\sum_{i=0}^{\alpha} (-1)^i (q-1)^{\alpha-i} |\mathcal{C}| A_i(\mathcal{C}) = \sum_{\mathcal{D} \in \mathfrak{B}(F^I)} R_{\mathcal{D}}(\chi_{\mathcal{C}}).$$

Theorem 3 *Let F, S be finite sets of size q, n respectively. Then the codes $\mathcal{C}$ in F^S satisfy the $n+1$ identities*

$$|\mathcal{C}| \sum_{j=0}^{n} K_\alpha(j; q) A_j(\mathcal{C}) = \sum_{I \in \binom{S}{\alpha}} Q^I(\chi_{\mathcal{C}}) = \sum_{I \in \binom{S}{\alpha}} \sum_{\mathcal{D} \in \mathfrak{B}(F^I)} R_{\mathcal{D}}(\chi_{\mathcal{C}}). \qquad (6)$$

Proof. Simply repeat the argument in the proof of theorem 2, replacing lemma 1 by 2. ■

Corollary 2 *Since the right hand side of equation 6 is a nonnegative integer, we again obtain the Delsarte inequalities*

$$\sum_{j=0}^{n} K_\alpha(j;q)A_j(\mathcal{C}) \geq 0.$$

7 The connection between the proofs

Let F, I be finite sets of size q, α respectively, and let $\mathcal{C}$ be a code in F^I. From lemma 1 and lemma 6, we know that

$$\sum_{\mathcal{D}\in\mathfrak{B}(F^I)} R_{\mathcal{D}}(\chi_{\mathcal{C}}) = \sum_{\mathcal{D}\in\mathfrak{B}(F^I)} (|\mathcal{C}\cap\mathcal{D}_0| - |\mathcal{C}\cap\mathcal{D}_1|)^2.$$

Our aim is to understand why

$$R_{\mathcal{D}}(\chi_{\mathcal{C}}) = (|\mathcal{C}\cap\mathcal{D}_0| - |\mathcal{C}\cap\mathcal{D}_1|)^2.$$

In the proof of proposition 4, we have seen that

$$R_B(\boldsymbol{\xi}) = (\xi_u - \xi_v)^2$$

for $B := \{u, v\}$. So R_B is the square of a *linear form* on the vector space $\mathbb{R}^F$. This linear form is determined by R_B up to sign. To avoid ambiguity, we choose an arbitrary fixed ordering of the set F and define

$$l_{u,v}(\boldsymbol{\xi}) := \begin{cases} \xi_u - \xi_v & \text{if } u < v, \\ \xi_v - \xi_u & \text{if } u > v. \end{cases}$$

Now, if $B_i := \{u_i, v_i\}$, $i \in I$, and $\mathcal{D} := \prod_{i\in I} B_i$, we observe that

$$R_{\mathcal{D}} = \bigotimes_{i\in I} R_{B_i} = \bigotimes_{i\in I} (l_{u_i,v_i})^2 = (\bigotimes_{i\in I} l_{u_i,v_i})^2.$$

So $R_{\mathcal{D}}$ is the square of the linear form

$$l_{u,v} := \bigotimes_{i\in I} l_{u_i,v_i}$$

on $\mathbb{R}^{(F^I)}$. The elements $u, v \in F^I$ have Hamming distance α. They completely determine the binary Hamming space $\mathcal{D}$. Conversely, for any two elements $x, y \in F^I$ with $d(x, y) = \alpha$ we have

$$R_{\mathcal{D}} = (l_{x,y})^2.$$

Example 7 *(Continuation of example 6.) Using the obvious vector notation for the linear forms, we have*

$$l_{0,1} = [1, -1, 0], \quad l_{1,2} = [0, 1, -1]$$

and

$$l_{01,12} = [0, 1, -1, 0, -1, 1, 0, 0, 0],$$

i.e.

$$l_{01,12}(\xi) = \xi_{01} - \xi_{02} - \xi_{11} + \xi_{12}.$$

All entries of $l_{u,v}$, being products of 0, 1 and -1, are equal to 0, 1 or -1. In fact, $(l_{u,v})_x = 0$ if and only if $x \notin \mathcal{D}$, and if $x \in \mathcal{D}$, then $(l_{u,v})_x = (-1)^{d(u,x)}$. So

$$\{\{x \in \mathcal{D} \mid (l_{u,v})_x = 1\}, \{x \in \mathcal{D} \mid (l_{u,v})_x = -1\}\}$$

actually is the partition $\{\mathcal{D}_0, \mathcal{D}_1\}$ of the binary Hamming space $\mathcal{D}$ that we defined at the end of section 3.

Corollary 3

$$l_{u,v}(\chi_{\mathcal{C}}) = \pm(|\mathcal{C} \cap \mathcal{D}_0| - |\mathcal{C} \cap \mathcal{D}_1|),$$

whence

$$R_{\mathcal{D}}(\chi_{\mathcal{C}}) = (|\mathcal{C} \cap \mathcal{D}_0| - |\mathcal{C} \cap \mathcal{D}_1|)^2.$$

Let us index the binary Hamming spaces $\mathcal{D} \in \mathfrak{B}(F^I)$ by assigning to each $\mathcal{D}$ a unique pair $(x, y) \in F^I \times F^I$. Remember that we have fixed an ordering of F. This ordering induces on F^I the *partial ordering*

$$x \prec y \Longleftrightarrow x_i < y_i \text{ for all } i \in I.$$

Now observe that each binary Hamming space $\mathcal{D}$ contains exactly one pair of elements x, y with $x \prec y$. Hence we can write

$$Q^I = \sum_{\mathcal{D} \in \mathfrak{B}(F^I)} R_{\mathcal{D}} = \sum_{x \prec y} (l_{x,y})^2.$$

So lemma 2 takes the form

$$\sum_{i=0}^{\alpha} (-1)^i (q-1)^{\alpha - i} |\mathcal{C}| A_i(\mathcal{C}) = \sum_{x \prec y} (l_{x,y}(\chi_{\mathcal{C}}))^2. \tag{7}$$

8 The size of the right hand side

In this section, we continue to use the notations of the preceding one. Obviously, the right hand side of equation 7 is equal to zero if and only if

$$l_{x,y}(\chi_{\mathcal{C}}) = 0$$

for all $x, y \in F^I$ with $x \prec y$. But the next proposition shows that, for $q > 2$, these $\binom{q}{2}^{\alpha}$ conditions are dependent. Consider the vector space

$$V := \text{span}\{l_{u,v} \mid u, v \in F \text{ and } u \neq v\} \subseteq (\mathbb{R}^F)^*.$$

Its dimension is $q - 1$. In fact, for any fixed $u \in F$, the set

$$\{l_{u,v} \mid u \neq v\}$$

is a basis for V. Since the dimension of the tensor product of vector spaces is the product of the dimensions of these vector spaces, we immediately have the

Proposition 6 *The vector space*

$$V^I := \text{span}\{l_{x,y} \mid x, y \in F^I \text{ and } d(x,y) = \alpha\} \subseteq (\mathbb{R}^{(F^I)})^*$$

has dimension $(q-1)^{\alpha}$. *Indeed, if we fix an arbitrary element* $x \in F^I$, *then*

$$\{l_{x,y} \mid y \in F^I \text{ and } d(x,y) = \alpha\}$$

is a basis of V^I.

Corollary 4 *The right hand side of equation 7 is equal to zero if and only if, for any fixed* $x \in F^I$

$$l_{x,y}(\chi_{\mathcal{C}}) = 0$$

for all $y \in F^I$ *with* $d(x,y) = \alpha$.

Now we turn to cases when we can predict that the right hand side equation 7 is unequal to zero. We want to generalize a result in [1], where it is shown that for $q = 2$ and $|\mathcal{C}| \not\equiv 0 (\text{mod } 2)$ the Delsarte inequalities are strict inequalities.

Proposition 7 *If* $|\mathcal{C}| \not\equiv 0 (\text{mod } q)$, *then for any* $x \in F^I$ *a* $y \in F^I$ *with* $d(x,y) = \alpha$ *exists such that* $l_{x,y}(\chi_{\mathcal{C}}) \neq 0$.

Proof. Note that

$$\sum_{d(x,y)=\alpha} l_{x,y}(\chi_{\mathcal{C}}) = \sum_{z\in F^I} (-1)^{d(x,z)}(q-1)^{\alpha-d(x,z)}(\chi_{\mathcal{C}})_z \equiv \sum_{z\in F^I} (\chi_{\mathcal{C}})_z (\mathrm{mod}\, q)$$

and that

$$\sum_{z\in F^I} (\chi_{\mathcal{C}})_z = |\mathcal{C}|.$$

■

This result can be considerably improved.

Lemma 3 *Consider the list*

$$L := [l_{u,v}(\xi)]_{(u,v)\in J}$$

parametrized by the set $J := \{(u,v) \in F \times F \mid u \prec v\}$. *If one of its elements is nonzero, at least* $q-1$ *are nonzero.*

Proof. A number $l_{u,v}(\xi)$ is zero if and only if $\xi_u = \xi_v$. If more then $\binom{q}{2} - (q-1)$ of the numbers $l_{u,v}(\xi)$ are zero, then all of them are zero. (This corresponds to the fact that the edge connectivity of the complete graph K_q is equal to $q-1$.) ■

Proposition 8 *If* $|\mathcal{C}| \not\equiv 0 (\mathrm{mod}\, q)$, *then at least* $(q-1)^\alpha$ *pairs* $(x,y) \in F^I \times F^I$ *with* $x \prec y$ *exist such that* $l_{x,y}(\chi_{\mathcal{C}}) \neq 0$.

Proof. Identify

$$J^I := \{(x,y) \in F^I \times F^I \mid x \prec y\}$$

with the Cartesian product $\prod_I J$ under the mapping

$$(x,y) \mapsto \prod_{i\in I} (x_i, y_i).$$

Then

$$L^I := [l_{x,y}(\chi_{\mathcal{C}})]_{(x,y)\in J^I}$$

can be viewed as an array of size $\binom{q}{2} \times \binom{q}{2} \times \ldots \times \binom{q}{2}$ (α times). Each "line" parallel to the "coordinate axes" is a list of the type described in lemma 3. From proposition 7, we know that at least one entry of L^I is nonzero. So an induction argument shows that L^I has at least $(q-1)^\alpha$ nonzero entries. (This is the same kind of argument as in the standard proof that the minimum distance of a product code is the product of the minimum distances of its factors, cf. [2], Theorem 10.1.2.) ■

Lemma 4 *Let $\boldsymbol{\xi} \in \mathbb{R}^F$ be a vector with nonnegative integer entries, and let k be the residue of $N := \sum_{u \in F} \xi_u$ modulo q. Then*

$$\sum_{u<v} (l_{u,v}(\boldsymbol{\xi}))^2 \geq k(q-k).$$

Proof. Let $a, b \in F$ be elements such that $\xi_a > \xi_b$. Consider the vector $\boldsymbol{\eta} \in \mathbb{R}^F$ defined by

$$\eta_t := \begin{cases} \xi_t - 1 & \text{if } t = a, \\ \xi_t + 1 & \text{if } t = b, \\ \xi_t & \text{otherwise.} \end{cases}$$

Then $\sum_{u \in F} \eta_u = N$ and

$$\begin{aligned} \sum_{u<v} (l_{u,v}(\boldsymbol{\xi}))^2 - \sum_{u<v} (l_{u,v}(\boldsymbol{\eta}))^2 &= (\xi_a - \xi_b)^2 - (\xi_a - \xi_b - 2)^2 + \\ &\quad \sum_{t \neq a,b} (\xi_a - \xi_t)^2 - (\xi_a - \xi_t - 1)^2 + \\ &\quad \sum_{t \neq a,b} (\xi_b - \xi_t)^2 - (\xi_b - \xi_t + 1)^2 \\ &= 4(\xi_a - \xi_b - 1) + \sum_{t \neq a,b} 2(\xi_a - \xi_b - 1) \\ &\geq 0. \end{aligned}$$

Continuing this procedure, we eventually wind up with a vector $\boldsymbol{\varsigma} \in \mathbb{R}^F$ such that

$$\sum_{u<v} (l_{u,v}(\boldsymbol{\xi}))^2 \geq \sum_{u<v} (l_{u,v}(\boldsymbol{\varsigma}))^2$$

and for which $n - k$ entries are equal to $\left\lfloor \frac{N}{q} \right\rfloor$ and k entries are equal to $\left\lfloor \frac{N}{q} \right\rfloor + 1$. Now observe that

$$\sum_{u<v} (l_{u,v}(\boldsymbol{\varsigma}))^2 = k(q-k).$$

■

Proposition 9 *Let k be the residue of $|\mathcal{C}|$ modulo q. Then*

$$\sum_{x \prec y} (l_{x,y}(\chi_{\mathcal{C}}))^2 \geq k(q-k)(q-1)^{\alpha-1}. \tag{8}$$

Proof. We use the notation of proposition 8, and consider the array

$$[(l_{x,y}(\chi_{\mathcal{C}}))^2]_{(x,y)\in J^I}.$$

All entries are nonnegative integers and their sum is the left hand side of inequality 8. By lemma 3, each nonzero "line" parallel to the "coordinate axes" has at least $q-1$ nonzero entries, and, by lemma 4, their sum is not smaller then $k(q-k)$. Now an induction argument perfectly similar to that in proposition 8 finishes the proof. ■

From this proposition we infer the following strengthening of the Delsarte inequalities.

Theorem 4 *Let F, S be finite sets of size q, n respectively, let $\mathcal{C}$ be a code in F^S and let k be the residue of $|\mathcal{C}|$ modulo q. Then*

$$|\mathcal{C}| \sum_{j=0}^{n} K_\alpha(j;q) A_j(\mathcal{C}) \geq k(q-k)(q-1)^{\alpha-1} \binom{n}{\alpha}$$

for $\alpha = 1, \ldots, n$.

Proof. Apply proposition 9 to all restrictions $\mathcal{C}_I, I \in \binom{F}{\alpha}$, and add the inequalities. Using equation 7, we obtain

$$\sum_{i=0}^{\alpha} (-1)^i (q-1)^{\alpha-i} \sum_{I\in\binom{F}{\alpha}} |\mathcal{C}| A_i(\mathcal{C}_I) \geq k(q-k)(q-1)^{\alpha-1} \binom{n}{\alpha}.$$

The left hand side can be transformed into

$$|\mathcal{C}| \sum_{j=0}^{n} K_\alpha(j;q) A_j(\mathcal{C})$$

in the same way as in theorem 2. ■

References

[1] M.R. Best, A.E. Brouwer, F.J. MacWilliams, A.M.. Odlyzko and N.J.A. Sloane, Bounds for binary codes of length less than 25. *IEEE Transactions on Information theory* 24: 81-93 (1978).

[2] R.E. Blahut, *Theory and practice of error control codes.* Addison-Wesley (1983).

[3] P. Camion, Codes and association Schemes, in *Handbook of Coding Theory* (preprint).

[4] P. Delsarte, An algebraic approach to the association schemes of coding theory. Philips Res. Repts Suppl. 10 (1973).

[5] P. Delsarte, Application and generalization of the MacWilliams transform in coding theory, in *Proceedings of the Fifteenth Symposium on Information Theory in the Benelux* (1994).

[6] J. Simonis and C. de Vroedt, A simple proof of the Delsarte inequalities, *Designs, Codes and Cryptography* 1:77-82 (1991).

[7] J.H. Van Lint, *Introduction to coding theory.* Springer Verlag, New-York etc. (1982).