Contributions to Discrete Mathematics

Volume 3, Number 1, Pages 39–46
ISSN 1715-0868

CONSTRUCTION OF A 3-DIMENSIONAL MDS-CODE

ANGELA AGUGLIA AND LUCA GIUZZI

Dedicated to the centenary of the birth of Ferenc Kárteszi (1907–1989).

Abstract. In this paper, we describe a procedure for constructing q–ary $[N, 3, N-2]$–MDS codes, of length $N \leq q+1$ (for q odd) or $N \leq q+2$ (for q even), using a set of non–degenerate Hermitian forms in $PG(2, q^2)$.

1. Introduction

The well–known Singleton bound states that the cardinality M of a code of length N with minimum distance d over a q–ary alphabet always satisfies

$$M \leq q^{N-d+1}; \tag{1.1}$$

see [8]. Codes attaining the bound are called *maximum distance separable codes*, or *MDS* codes for short.

Interesting families of maximum distance separable codes arise from geometric and combinatorial objects embedded in finite projective spaces. In particular linear $[N, k, N-k+1]$–MDS codes, with $k \geq 3$, and N–arcs in $PG(k-1, q)$ are equivalent objects; see [1].

A general method for constructing a q–ary code is to take N polynomials $f_1, \ldots, f_N$ in n indeterminates, defined over $\mathrm{GF}(q)$, and consider the set $\mathcal{C}$ given by

$$\mathcal{C} = \{(f_1(x), \ldots, f_N(x)) \mid x \in \mathcal{W}\},$$

where $\mathcal{W}$ is a suitable subset of $\mathrm{GF}(q)^n$. In this paper, we deal with the case $|\mathcal{W}| = q^t$ and also assume that the *evaluation function*

$$\begin{array}{rccc} \Theta & : & \mathcal{W} & \to & \mathcal{C} \\ & & x & \mapsto & (f_1(x), f_2(x), \ldots, f_N(x)) \end{array}$$

is injective.

If $\mathcal{C}$ attains the Singleton bound then the restrictions of all the codewords to any given $t = N - d + 1$ places must all be different, namely in any t positions all possible vectors occur exactly once. This means that a necessary condition for $\mathcal{C}$ to be MDS is that any t of the varieties $V(f_m)$ for $m = 1, \ldots, N$ meet in exactly one point in $\mathcal{W}$. Here $V(f)$ denotes the algebraic variety associated to f.

2000 *Mathematics Subject Classification.* 05B25, 11E39.
Key words and phrases. Hermitian form, MDS-code.

Applying the above procedure to a set of non–degenerate Hermitian forms in $PG(2,q^2)$ we construct some q–ary $[N,3,N-2]$–MDS codes, of length $N\leq q+1$ (for q odd) or $N\leq q+2$ (for q even). The codes thus obtained can also be represented by sets of points in $\mathrm{PG}(3,q)$; this representation is used in Section 4 in order to devise an algebraic decoding procedure, based upon polynomial factorisation; see [10].

2. Preliminaries

Let $\mathcal{A}$ be a set containing q elements. For any integer $N\geq 1$, the function $d_H:\mathcal{A}^N\times\mathcal{A}^N\mapsto\mathbb{N}$ given by

$$d_H(\mathbf{x},\mathbf{y})=|\{i:x_i\neq y_i\}|,$$

is a metric on $\mathcal{A}^N$. This function is called the *Hamming distance* on $\mathcal{A}^N$. A q–ary (N,M,d)–code $\mathcal{C}$ over the alphabet $\mathcal{A}$ is just a collection of M elements of $\mathcal{A}^N$ such that any two of them are either the same or at Hamming distance at least d; see [4, 6]. The elements of $\mathcal{C}$ are called *codewords* whereas the integers d and N are respectively the *minimum distance* and the *length* of $\mathcal{C}$.

If $\mathcal{A}=GF(q)$ and $\mathcal{C}$ is a k–dimensional vector subspace of $GF(q)^N$, then $\mathcal{C}$ is said to be a *linear* $[N,k,d]$–code. Under several communication models, it is assumed that a received word $\mathbf{r}$ should be decoded as the codeword $\mathbf{c}\in\mathcal{C}$ which is nearest to $\mathbf{r}$ according to the Hamming distance; this is the so–called maximum likelihood decoding. Under these assumptions the following theorem, see [4, 6], provides a basic bound on the guaranteed error correction capability of a code.

Theorem 2.1. *If $\mathcal{C}$ is a code of minimum distance d, then $\mathcal{C}$ can always either detect up to $d-1$ errors or correct $e=\lfloor(d-1)/2\rfloor$ errors.*

Observe that the theorem does not state that it is not possible to decode a word when more than e errors happened, but just that in this case the correction may fail. Managing to recover from more than e errors for some given received codewords is called "correcting beyond the bound".

The *weight* of an element $\mathbf{x}\in GF(q)^N$ is the number of non–zero components x_i of $\mathbf{x}$. For a linear code the minimum distance d equals the minimum weight of the non–zero codewords.

The parameters of a code are not independent; in general it is difficult to determine the maximum number of words a code of prescribed length N and minimum distance d may contain. For any arbitrary linear $[N,k,d]$–code, condition (1.1) may be rewritten as

$$d\leq N-k+1; \tag{2.1}$$

thus $\mathcal{C}$ is a linear MDS code if and only if equality holds in (2.1).

In Section 3 we shall make extensive use of some non–degenerate Hermitian forms in $PG(2,q^2)$.

Consider the projective space $PG(d, q^2)$ and let V be the underlying vector space of dimension $d+1$. A *sesquilinear Hermitian form* is a map

$$h : V \times V \longrightarrow GF(q^2)$$

additive in both components and satisfying

$$h(k\mathbf{v}, l\mathbf{w}) = kl^q h(\mathbf{v}, \mathbf{w})$$

for all $\mathbf{v}, \mathbf{w} \in V$ and $k, l \in GF(q^2)$. The form is *degenerate* if and only if the subspace $\{\mathbf{v} \mid h(\mathbf{v}, \mathbf{w}) = 0 \ \forall \mathbf{w} \in V\}$, the *radical* of h, is different from $\{\mathbf{0}\}$. Given a sesquilinear Hermitian form h, the associated Hermitian variety $\mathcal{H}$ is the set of all points of $PG(d, q^2)$ such that $\{\langle \mathbf{v} \rangle \mid \mathbf{0} \neq \mathbf{v} \in V, \ h(\mathbf{v}, \mathbf{v}) = 0\}$. The variety $\mathcal{H}$ is *degenerate* if h is degenerate; non–degenerate otherwise. If h is a sesquilinear Hermitian form in $PG(d, q^2)$ then the map $F : V \longrightarrow GF(q)$ defined by

$$F(\mathbf{v}) = h(\mathbf{v}, \mathbf{v}),$$

is called *the Hermitian form on V associated to h*. The Hermitian form F is *non–degenerate* if and only if h is non–degenerate. Complete introductions to Hermitian forms over finite fields may be found in [2, 7].

3. Construction

Let S be a representative system for the cosets of the additive subgroup T_0 of $\mathrm{GF}(q^2)$ given by

$$T_0 = \{y \in \mathrm{GF}(q^2) : \mathrm{T}\,(y) = 0\},$$

where

$$\begin{array}{cccc} \mathrm{T} & : & \mathrm{GF}(q^2) & \rightarrow & \mathrm{GF}(q) \\ & & y & \mapsto & y^q + y \end{array}$$

is the trace function. Denote by Λ a subset of $GF(q^2)$ satisfying

$$\left(\frac{\alpha - \beta}{\gamma - \beta}\right)^{q-1} \neq 1 \tag{3.1}$$

for any $\alpha, \beta, \gamma \in \Lambda$. Choose a basis $B = \{1, \varepsilon\}$ of $GF(q^2)$, regarded as a 2–dimensional vector space over $GF(q)$; hence, it is possible to write each element $\alpha \in GF(q^2)$ in components $\alpha_1, \alpha_2 \in \mathrm{GF}(q)$ with respect to B. We may thus identify the elements of $GF(q^2)$ with the points of $AG(2, q)$, by the bijection which maps $(x, y) \in AG(2, q)$ to $x + \varepsilon y \in GF(q^2)$. Condition (3.1) corresponds to require that Λ, regarded as point–set in $AG(2, q)$, is an arc. Thus, setting $N = |\Lambda|$, we have

$$N \leq \begin{cases} q+1 & \text{for } q \text{ odd}, \\ q+2 & \text{for } q \text{ even}; \end{cases} \tag{3.2}$$

see [5, Theorem 8.5].

Now, consider the non–degenerate Hermitian forms $\mathcal{F}_\lambda(X, Y, Z)$ on $GF(q^2)^3$

$$\mathcal{F}_\lambda(X, Y, Z) = X^{q+1} + Y^q Z + Y Z^q + \lambda^q X^q Z + \lambda X Z^q,$$

as λ varies in Λ. Label the elements of Λ as $\lambda_1, \dots, \lambda_N$ and let $\Omega = GF(q^2) \times S$.

Theorem 3.1. *The set*

$$\mathcal{C} = \{(\mathcal{F}_{\lambda_1}(x,y,1), \mathcal{F}_{\lambda_2}(x,y,1), \dots, \mathcal{F}_{\lambda_N}(x,y,1)) | (x,y) \in \Omega\}$$

is a q-ary linear $[N,3,N-2]$–MDS code.

Proof. We first show that $\mathcal{C}$ consists of q^3 tuples from $GF(q)$. Let $(x_0,y_0),\ (x_1,y_1) \in \Omega$ and suppose that for any $\lambda \in \Lambda$,

$$\mathcal{F}_\lambda(x_0,y_0,1) = \mathcal{F}_\lambda(x_1,y_1,1).$$

Then,

$$\mathrm{T}\,(\lambda(x_1 - x_0)) = x_0^{q+1} - x_1^{q+1} + \mathrm{T}\,(y_0 - y_1). \tag{3.3}$$

In particular,

$$\mathrm{T}\,(\lambda(x_1 - x_0)) = \mathrm{T}\,(\alpha(x_1 - x_0)) = \mathrm{T}\,(\gamma(x_1 - x_0)) \tag{3.4}$$

for any $\alpha, \lambda, \gamma \in \Lambda$.

If it were $x_1 \neq x_0$, then (3.4) would imply

$$\left(\frac{\alpha - \beta}{\gamma - \beta}\right)^{q-1} = 1,$$

contradicting the assumption made on Λ. Therefore, $x_1 = x_0$ and from (3.3) we get $\mathrm{T}\,(y_0 - y_1) = 0$. Hence, y_0 and y_1 are in the same coset of T_0; by definition of S, it follows that $y_0 = y_1$, thus $\mathcal{C}$ has as many tuples as $|\Omega|$.

We are now going to show that $\mathcal{C}$ is a vector subspace of $\mathrm{GF}(q)^N$. Take $(x_0,y_0), (x_1,y_1) \in \Omega$. For any $\lambda \in \Lambda$,

$$\mathcal{F}_\lambda(x_0,y_0,1) + \mathcal{F}_\lambda(x_1,y_1,1) = \mathcal{F}_\lambda(x_2,y_2,1), \tag{3.5}$$

where $x_2 = x_0 + x_1$ and $y_2 = y_0 + y_1 - x_0^q x_1 - x_1^q x_0$. Likewise, for any $\kappa \in \mathrm{GF}(q)$,

$$\kappa \mathcal{F}_\lambda(x_0,y_0,1) = \mathcal{F}_\lambda(x,y,1), \tag{3.6}$$

where $x = \kappa x_0$ and y is a root of

$$y^2 + y = (\kappa - \kappa^2) x_0^{q+1} + \kappa(y_0^q + y_0).$$

Therefore, $\mathcal{C}$ is a vector subspace of $\mathrm{GF}(q)^N$; as it consists of q^3 tuples, $\mathcal{C}$ is indeed a 3–dimensional vector space.

Finally we prove that the minimum distance d of $\mathcal{C}$ is $N-2$. Since $\mathcal{C}$ is a vector subspace of $\mathrm{GF}(q)^N$, its minimum distance is $N - z$, where

$$z = \max_{\substack{\mathbf{c} \in \mathcal{C}, \\ \mathbf{c} \neq \mathbf{0}}} |\{i : c_i = 0\}|.$$

Furthermore, $z \geq 2$ because of Singleton bound (2.1). In order to show that $z = 2$ we study the following system

$$\begin{cases} \mathcal{F}_\alpha(x,y,1) = 0, \\ \mathcal{F}_\beta(x,y,1) = 0, \\ \mathcal{F}_\gamma(x,y,1) = 0, \end{cases} \tag{3.7}$$

for α, β, γ distinct elements of Λ. Set $U = x^{q+1} + y^q + y$, $V = x^q$ and $W = x$; then, (3.7) becomes

$$\begin{cases} U + \alpha^q V + \alpha W = 0, \\ U + \beta^q V + \beta W = 0, \\ U + \gamma^q V + \gamma W = 0. \end{cases} \tag{3.8}$$

Since $\left(\frac{\alpha-\beta}{\gamma-\beta}\right) \neq 1$, the only solution of (3.8) is $U = V = W = 0$, that is $x = 0$ and $y + y^q = 0$. In particular, there is just one solution to (3.7) in Ω, that is $\mathbf{x} = (0,0)$. This implies that a codeword which has at least three zero components is the zero vector, hence $z = 2$ and thus the minimum distance of $\mathcal{C}$ is $N - 2$. □

Example 3.2. *When q is odd, a representative system S for the cosets of T_0 is given by the subfield* GF(q) *embedded in* GF(q^2). *In this case it is then extremely simple to construct the code. For $q = 5$, a computation using GAP* [3]*, shows that in order for Λ to satisfy property* (3.1)*, we may take $\Lambda = \{\varepsilon^3, \varepsilon^4, \varepsilon^8, \varepsilon^{15}, \varepsilon^{16}, \varepsilon^{20}\}$, where ε is a root of the polynomial $X^2 - X + 2$, irreducible over $GF(5)$. The corresponding Hermitian forms are*

$$\begin{array}{lllllllll}
X^{q+1} & + & Y^qZ & + & yZ^q & + & \varepsilon^{15}X^qZ & + & \varepsilon^3XZ^q, \\
X^{q+1} & + & Y^qZ & + & YZ^q & + & \varepsilon^{20}X^qZ & + & \varepsilon^4XZ^q, \\
X^{q+1} & + & Y^qZ & + & YZ^q & + & \varepsilon^{16}X^qZ & + & \varepsilon^8XZ^q, \\
X^{q+1} & + & Y^qZ & + & YZ^q & + & \varepsilon^{3}X^qZ & + & \varepsilon^{15}XZ^q, \\
X^{q+1} & + & Y^qZ & + & YZ^q & + & \varepsilon^{8}X^qZ & + & \varepsilon^{16}XZ^q, \\
X^{q+1} & + & Y^qZ & + & YZ^q & + & \varepsilon^{4}X^qZ & + & \varepsilon^{20}XZ^q.
\end{array}$$

A generator matrix for the $[6,3,4]$–MDS code obtained applying Theorem 3.1 to these Hermitian forms is

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 2 & 1 & 2 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{pmatrix}$$

Remark 3.3. In $PG(2,q^2)$, take the line $\ell_\infty : Z = 0$ as the line at infinity. Then, in the affine plane $AG(2,q^2) = PG(2,q^2) \setminus \ell_\infty$, any two Hermitian curves $V(F_\lambda)$ have q^2 affine points in common, q of which in $\Omega \subset AG(2,q^2)$. Likewise, the full intersection

$$\bigcap_{\lambda \in \Lambda} V(F_\lambda)$$

consists of the q affine points $\{(0,y) \mid y^q + y = 0\}$, corresponding to just a single point in Ω.

Remark 3.4. Denote by A_i the number of words in $\mathcal{C}$ of weight i. Since $\mathcal{C}$ is an MDS code, we have

$$A_i = \binom{N}{i}(q-1)\sum_{j=0}^{i-N+2}(-1)^j\binom{i-1}{j}q^{i-j-N+2};$$

see [9]. Thus,

$$\begin{aligned} A_{N-2} &= \frac{1}{2}(N^2-N)(q-1), \\ A_{N-1} &= Nq^2-(N^2-N)q+N^2-2N, \\ A_N &= q^3-Nq^2+\frac{1}{2}\left((N^2-N)q-N^2+3N\right). \end{aligned}$$

4. Decoding

In this section it will be shown how the code $\mathcal{C}$ we constructed may be decoded by geometric means.

Our approach is based upon two remarks:

(1) Any received word $\mathbf{r} = (r_1, \dots, r_N)$ can be uniquely represented by a set $\widetilde{\mathbf{r}}$ of N points of $\mathrm{PG}(3,q)$

$$\widetilde{\mathbf{r}} = \left\{\left(\lambda_i^1, \lambda_i^2, r_i, 1\right) : \lambda = \lambda_i^1 + \varepsilon\lambda_i^2 \in \Lambda\right\}.$$

These points all lie on the cone Ψ of basis

$$\Xi = \left\{\left(\lambda_i^1, \lambda_i^2, 0, 1\right) : \lambda = \lambda_i^1 + \varepsilon\lambda_i^2 \in \Lambda\right\}$$

and vertex $Z_\infty = (0,0,1,0)$.

(2) For any $a, b \in \mathrm{GF}(q^2)$, the function

$$\phi_{(a,b)}(x,y,z,t) = \left(a^{q+1} + \mathrm{T}(b)\right)t + \mathrm{T}\left((x+\varepsilon y)a\right)$$

is a homogeneous linear form with domain $\mathrm{GF}(q)^4$.

Recall that the codeword $\mathbf{c}$ corresponding to a given $(a,b) \in \Omega$ is

$$\mathbf{c} = \left(\phi_{(a,b)}(\lambda_1^1, \lambda_1^2, 0, 1), \phi_{(a,b)}(\lambda_2^1, \lambda_2^2, 0, 1), \dots, \phi_{(a,b)}(\lambda_N^1, \lambda_N^2, 0, 1)\right);$$

thus, $\widetilde{\mathbf{c}}$, the set containing the points $(\lambda_i^1, \lambda_i^2, c_i, 1)$, is the full intersection of the plane $\pi_{a,b} : z = \phi_{(a,b)}(x,y,z,t)$ with the cone Ψ.

It is clear that knowledge of the plane $\pi_{(a,b)}$ is enough to reconstruct the codeword $\mathbf{c}$. In the presence of errors, we are looking for the nearest codeword $\mathbf{c}$ to a vector $\mathbf{r}$; this is the same as to determine the plane $\pi_{(a,b)}$ containing most of the points of $\widetilde{\mathbf{r}}$. In order to obtain such a plane, we adopt the following approach. Assume ℓ to be a line of the plane $\pi_{0,0} : z = 0$ external to Ξ and denote by π_∞ the plane at infinity of equation $t = 0$. For any $P \in \ell$, let $\widetilde{\mathbf{r}}^P$ be the projection from P of the set $\widetilde{\mathbf{r}}$ on π_∞. Write $\mathcal{L}_{\mathbf{r}}^P$ for a curve of π_∞ of minimum degree containing $\widetilde{\mathbf{r}}^P$. Observe that $\deg \mathcal{L}_{\mathbf{r}}^P \leq q+1$ and $\deg \mathcal{L}_{\mathbf{r}}^P = 1$ if, and only if, all the points of $\widetilde{\mathbf{r}}$ lie on a same plane through

P, that is $\widetilde{\mathbf{r}}$ corresponds to a codeword associated with that plane passing through P.

We now can apply the following algorithm using, for example, [3].

(1) Take $P \in \ell$;
(2) Determine the projection $\mathbf{r}^P$ and compute the curve $\mathcal{L}_{\mathbf{r}}^P$;
(3) Factor $\mathcal{L}_{\mathbf{r}}^P$ into irreducible factors, say $\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_v$;
(4) Count the number of points in $\widetilde{\mathbf{r}}^P \cap V(\mathcal{L}_i)$ for any factor $\mathcal{L}_i$ of $\mathcal{L}_{\mathbf{r}}^P$ with $\deg \mathcal{L}_i = 1$;
(5) If for some i we have $n_i > (N+1)/2$, then return the plane spawned by P and two points of L_i; else, as long as not all the points of ℓ have been considered, return to point 1;
(6) If no curve with the required property has been found, return failure.

Remark 4.1. The condition on n_i in point (5) checks if the plane contains more than half of the points corresponding to the received word $\mathbf{r}$; when this is the case, a putative codeword $\mathbf{c}$ is constructed, with $d(\mathbf{c}, \mathbf{r}) \leq (N-3)/2$; thus, when $\mathbf{c} \in \mathcal{C}$, then it is indeed the unique word of $\mathcal{C}$ at minimum distance from $\mathbf{r}$. However, the aforementioned algorithm may be altered in several ways, in order to be able to try to correct errors beyond the bound; possible approaches are:

(1) iterate the procedure for all the points on ℓ and return the planes containing most of the points corresponding to the received vector;
(2) use some further properties of the cone Ψ; in particular, when Ξ is a conic it seems possible to improve the decoding by considering also the quadratic components of the curve $\mathcal{L}_{\mathbf{r}}^P$.

Remark 4.2. The choice of P on a line ℓ is due to the fact that any line of $\pi_{0,0}$ meets all the planes of $\mathrm{PG}(3,q)$. In general, we might have chosen ℓ to be just a blocking set disjoint from Ξ. If q is odd and $|\Lambda| = q+1$, then the line ℓ is just an external line to a conic of $\pi_{0,0}$.

References

1. E. F. Assmus, Jr. and J. D. Key, *Designs and their codes*, Cambridge University Press, 1992.
2. S. N. Bose and I. M. Chakravarti, *Hermitian varieties in a finite projective space $PG(N, q^2)$*, Canad J. Math. **18** (1966), 1161–1182.
3. *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2006, `http://www.gap-system.org`.
4. L. Giuzzi, *Codici correttori*, Springer-Verlag, 2006.
5. J. W. P. Hirschfeld, *Projective geometries over finite fields*, 2 ed., Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1998.
6. R. McEliece, *Theory of information and coding*, Cambridge University Press, 2002.
7. B. Segre, *Forme e geometrie hermitiane, con particolare riguardo al caso finito*, Ann. Mat. Pura Appl. (4) **70** (1965), 1–201.
8. R. C. Singleton, *Maximum distance q–nary codes*, IEEE Trans. Inf. Theory **10** (1964), no. 2, 116–118.
9. L. Staiger, *On the weight distribution of linear codes having dual distance $d' > k$*, IEEE Trans. Inf. Theory **35** (1989), no. 1, 186–188.

10. M. Sudan, *Decoding Reed Solomon codes beyond the error-correction bound*, Journal of Complexity **13** (1997), no. 1, 180–193.

Dipartimento di Matematica, Politecnico di Bari,
Via G. Amendola 126/B, 70126 Bari, Italy
E-mail address: a.aguglia@poliba.it
E-mail address: l.giuzzi@poliba.it