Codes from Flag Varieties over a Finite Field

F. Rodier

Institut de Mathématiques de Luminy – C.N.R.S. – Marseille – France

Abstract

We show how to construct error-correcting codes from flag varieties on a finite field $\mathbb{F}_q$. We give some examples. For some codes, we give the parameters and give the weights and the number of codewords of minimal weight.

Key words: error-correcting codes, flag varieties, projective systems
1991 MSC: 94B27, 14M15

1 Introduction

I will study some error-correcting codes constructed from flag varieties over a finite field $\mathbb{F}_q$. After V. Goppa, the consideration of codes constructed from algebraic curves is now classical. Thanks to Y. Manin [8], we can consider codes built from higher dimensional algebraic varieties.

Some of such codes have already been studied. Among others, projective Reed-Muller codes have been studied by G. Lachaud [6] and A. Sørensen [14], codes on grassmannians by D. Nogin [9], and G. Lachaud and S. Ghorpade [3], codes on hermitian hypersurfaces by I.M. Chakravarti [1], and J.W.P. Hirschfeld, M. Tsfasman and S. Vladut [5], Reed-Muller codes on complete intersections by Duursma, Renteria and Tapia-Recillas [2]. In [7], G. Lachaud has given some general bounds for the parameters of codes associated with multi-dimensional varieties, in particular complete intersections. S. Hansen has studied codes from higher-dimensional varieties, especially Deligne-Lusztig varieties [4].

Flag varieties are examples of varieties having a large number of points over a finite field and can therefore be used as guinea-pigs for trying to construct

Email address: `rodier@iml.univ-mrs.fr` (F. Rodier).

efficient codes. Indeed they can be viewed as sets of rational points of Deligne-Lusztig varieties and these varieties have the maximal number of rational points relatively to their geometrical structure, which is given for instance by their Betti numbers (cf. [10] and [11]). Moreover the flag varieties have a large group of automorphism, therefore the associated codes provides many symmetries.

This paper is organized as follows. We first define a flag variety, then we show how to embed a flag variety into a projective space and we get the code construction by the method of M. Tsfasman and S. Vladut [15]. Then in sections 4 and 5, we give examples, and we conclude in the last section by a comparison of the codes obtained with Reed-Muller codes of order 2.

2 Flag Varieties

A *flag* over a finite field $\mathbb{F}_q$ is a sequence X of strictly embedded subspaces $V_{i_1} \subset V_{i_2} \subset \cdots \subset V_{i_s}$ of dimension $i_1,\ i_2,\ \ldots,\ i_s$ of an m-dimensional vector space $V = (\mathbb{F}_q)^m$. A *flag variety* of type $(i_1, i_2, \ldots, i_s)$ is the variety of all flags $X = \{(V_{i_1}, V_{i_2}, \ldots, V_{i_s})\}$ with $(i_1, i_2, \ldots, i_s)$ given.

Equivalently we can describe it as the set G/P where $G = GL(m, \mathbb{F}_q)$ and P is a parabolic subgroup (that is a subgroup consisting of upper triangular matrices in blocks or of conjugates of such a matrix). The variety of $(V_{i_1}, V_{i_2}, \ldots, V_{i_s})$ with $V_{i_1} \subset V_{i_2} \subset \cdots \subset V_{i_s}$ is isomorphic to the variety G/P with

$$P = \begin{pmatrix} M_1 & * & * & \cdots & * \\ 0 & M_2 & * & \cdots & * \\ 0 & 0 & M_3 & \cdots & * \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & M_{s+1} \end{pmatrix}$$

such that

$$M_r \in GL(\dim V_{i_r} - \dim V_{i_{r-1}}, \mathbb{F}_q) = GL(i_r - i_{r-1}, \mathbb{F}_q)$$

for $2 \leq r \leq s+1$, with $V_{i_{s+1}} = V = (\mathbb{F}_q)^m$. The group G acts transitively on the set of flags $\{(V_{i_1}, V_{i_2}, \ldots, V_{i_s})\}$. The stabilizer of the flag

$$\Big\{\Big(\langle e_1, e_2, \cdots, e_{i_1}\rangle, \langle e_{i_1+1}, e_{i_1+2}, \cdots, e_{i_2}\rangle, \cdots, \langle e_{i_s+1}, e_{i_s+2}, \cdots, e_m\rangle\Big)\Big\}$$

is the subgroup P where $(e_i)_{1\leq i\leq m}$ is the canonical basis of the vector space V. In that case, we shall say that P is a parabolic subgroup of type $(i_1, i_2, \ldots, i_s)$.

As an example, we can take P of type (l) with $l \leq m$. The flag variety is the variety of all flags $X = \{(V_l)\}$, that is the grassmannian $Gr(l, m)$ of l-subspaces of V.

3 Code Construction

3.1 General Construction

We construct a code C in a usual way by embedding X into a projective space and evaluating the linear forms on X as is described in the book of Tsfasman and Vladut [15], chapter 1.1.

We build thus a $[n, k]$-projective system $X \longrightarrow \mathbb{P}_{k-1}$ which gives rise to an associated code by the following process. Let $x_1, \ldots, x_n$ be the images of the elements of X into $\mathbb{P}_{k-1}$ and let $y_1, \ldots, y_n$ be their liftings in the vector space minus the origin $E^\times = (\mathbb{F}_q^k)^\times$.

We defines a map from linear forms f on E to n-uplets of elements of $\mathbb{F}_q$ by

$$\begin{aligned} \underline{\mathrm{ev}} : E^* &\longrightarrow (\mathbb{F}_q)^n \\ f &\longmapsto (f(y_1), \ldots, f(y_n)) \end{aligned}$$

whose image is the code C. The length of C is equal to n. The dimension of C is equal to $k - \dim \ker \underline{\mathrm{ev}}$. The minimum distance of C is equal to the minimum for all the f in $\#X - \#(X \cap \ker f)$ where $\ker f$ is an hyperplane of $\mathbb{P}_{k-1}$ not containing X.

3.2 The Flag case

Let P be a parabolic subgroup of G, G_1 be a subgroup of G and $P_1 = P \cap G_1$. We embed $X = G/P$ and the subset $X_1 = G_1/P_1$ into a projective space $\mathbb{P}_N$ by a sequence of 3 embeddings that we will describe.

A flag $(V_{i_1}, V_{i_2}, \ldots, V_{i_s})$ is a sequence of subspaces V_{i_l} which are elements of the grassmannian $Gr(i_l, m)$. We deduce from this fact a morphism from the flag variety $X = G/P$ to the product of grassmannians $Gr(i_1, m) \times \cdots \times Gr(i_s, m)$. One can embed each grassmannian $Gr(i_l, m)$ into the projective space $\mathbb{P}(\bigwedge^l V_{i_l}) = \mathbb{P}_{r_l}$ where $r_l = \binom{m}{i_l} - 1$ thanks to the Plücker embedding ([13], p. 42), which is obtained from the map which sends a basis $f_1, \ldots, f_{i_l}$ of V_{i_l} to the exterior product $f_1 \wedge \cdots \wedge f_{i_l}$ of $\bigwedge^{i_l} V$ and noticing that different basis give proportional elements of $\bigwedge^{i_l} V$, therefore they give the same point in $\mathbb{P}_{r_l}$.

Then we can embed the product of projective spaces $\mathbb{P}_{r_1}\times\cdots\times\mathbb{P}_{r_s}$ into another projective space $\mathbb{P}_r$ with $r=(r_1+1)(r_2+1)\dots(r_s+1)-1$ by the Segré embedding which corresponds to the mapping of the elements $(v_1,\dots,v_s)$ of the product of the vector spaces $V_{r_1+1}\times\dots\times V_{r_s+1}$ to the tensor product $v_1\otimes\dots\otimes v_s$ which is an element of the vector space V_{r+1}. Indeed the following diagram is commutative and defines a mapping from $\mathbb{P}_{r_1}\times\cdots\times\mathbb{P}_{r_s}$ to $\mathbb{P}_r$ where we denote $V^\times$ the vector space V minus the origin:

$$\begin{array}{ccccc} (v_1,\dots,v_s) & \in & V^\times_{r_1+1}\times\dots\times V^\times_{r_s+1} & \longrightarrow & \mathbb{P}_{r_1}\times\cdots\times\mathbb{P}_{r_s} \\ \downarrow & & \downarrow & & \downarrow \\ v_1\otimes\dots\otimes v_s & \in & (V_{r_1+1}\otimes\dots\otimes V_{r_s+1})^\times & \longrightarrow & \mathbb{P}_r \ . \end{array}$$

One can embed further the projective space $\mathbb{P}_r$ into another projective space by means of the Veronèse embedding of order h which sends $\mathbb{P}_r$ to $\mathbb{P}_N$ with $N=\binom{r+h}{h}-1$. This embedding comes from the map $V_{r+1}\longrightarrow V_{N+1}$ which sends the element of coordinates $(u_1,u_2,\dots,u_{r+1})$ to the element of coordinates $(\dots,u_1^{j_1}u_2^{j_2}\cdots u_{r+1}^{j_{r+1}},\dots)$ of V_{N+1}, with $j_1+j_2+\cdots+j_{r+1}=h$.

If we restrict ourselves to the subgroup G_1 of G and we take $P_1=P\cap G_1$ and $X_1=G_1/P_1$ we get the following diagram.

$$\begin{tikzcd}[arrows=-]
GL(m)/P \arrow[d, "" , ->] & \supset & G_1/P_1 \arrow[dddd, ->] & = & & & \{x_1,x_2,\dots,x_n\} \arrow[dddd, ->] \\
Gr(i_1,m)\times\cdots\times Gr(i_s,m) \arrow[d, ->] & & & & & & \\
\mathbb{P}_{r_1}\times\cdots\times\mathbb{P}_{r_s} \arrow[d, ->] & & & & & & \\
\mathbb{P}_r \arrow[d, ->] & & & & & & \\
\mathbb{P}_N & \supset & \mathbb{P}_N & \leftarrow & V^\times_{N+1} & \ni & \{y_1,y_2,\dots,y_n\}
\end{tikzcd} \tag{1}$$

For $f\in V_{N+1}(\mathbb{F}_q)^*$ let $\underline{\mathrm{ev}}: f\longmapsto (f(y_1),\dots\ f(y_n))$. The image of $\underline{\mathrm{ev}}$ is a code

$$[\#X\ ,\ N+1-\dim\ker\underline{\mathrm{ev}}\ ,\ \#X-\max\#(X\cap H)]$$

where $X=G_1/P_1$ and H runs over the set of hyperplanes of $\mathbb{P}_N$.

4 Examples

4.1 Reed-Muller projective codes

We take the matrices $P = \begin{pmatrix} a & * \\ 0 & M \end{pmatrix}$ where $a \in \mathbb{F}_q^\times$, the $*$ denotes any element of $(\mathbb{F}_q)^{m-1}$, and M is a square matrix of order $m-1$. The diagram (1) simplifies to

$$\begin{array}{ccc} GL(m)/P & \ni & \{x_1, x_2, \ldots, x_n\} \\ \downarrow & & \\ \mathbb{P}_{m-1} & & \Big\downarrow \\ \downarrow & & \\ \mathbb{P}_N & \longleftarrow & V_{N+1} - \{0\} \end{array}$$

We thus obtain a code of order h whose parameters are, when $\underline{\text{ev}}$ is injective that is when $h \leq q$ (cf. Lachaud [6]):

$$\left[\frac{q^m - 1}{q-1} \quad , \quad \binom{h+m-1}{h} \quad , \quad (q-h+1)q^{m-2}\right]$$

where h is the order of the Veronese embedding. When $\underline{\text{ev}}$ is not injective, the parameters are more intricate (cf. Sørensen [14]).

4.2 Codes on Grassmannian

We take the matrices $P = \begin{pmatrix} M_1 & * \\ 0 & M_2 \end{pmatrix}$ where M_1 stands for a square matrix of order l, and M_2 stands for a square matrix of order $m-l$. We now get the diagram

$$\begin{array}{ccc} GL(m)/P & = & \{x_1, x_2, \ldots, x_n\} \\ \downarrow & & \\ Gr(l,m) & & \Big\downarrow \\ \downarrow & & \\ \mathbb{P}_N & \longleftarrow & V_{N+1} - \{0\} \end{array}$$

where $N = \binom{m}{l} - 1$.

Nogin has computed the parameters of the code that we obtain ([9]):

$$\left[\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{l-1})}{(q^l-1)(q^l-q)\cdots(q^l-q^{l-1})} \; , \; \binom{m}{l} \; , \; q^{(m-l)l}\right]$$

Consider the subgroup $G_1 = U(m+1, \mathbb{F}_{q^2})$ of the group $G = GL(m+1, \mathbb{F}_{q^2})$ with $m \geq 2$. The subgroup $U(m+1, \mathbb{F}_{q^2})$ is the unitary group for the hermitian form on $\mathbb{F}_{q^2}^{m+1}$

$$\langle x, y \rangle = x_0 y_m^q + x_1 y_{n-1}^q + \cdots + x_m y_0^q$$

We take the parabolic subgroup

$$P = \begin{pmatrix} a & * & \dots & * \\ 0 & & & \\ \vdots & & \Big(GL(m)\Big) & \\ 0 & & & \end{pmatrix}$$

where $a \in \mathbb{F}_{q^2}^{\times}$, the $*$ denote the coefficients of matrix in $GL(m+1)$ which are allowed to take any value in $\mathbb{F}_{q^2}$, and $P_1 = U(m+1, \mathbb{F}_{q^2}) \cap P$. We get the following diagram

$$\begin{array}{ccccccc}
GL(m+1)/P & \supset & U(m+1)/P_1 & = & \{x_1, x_2, \dots, x_n\} \\
\downarrow & & & & \\
\mathbb{P}_m & & \Big\downarrow & & \Big\downarrow \\
\text{Véronèse} \downarrow & & & & \\
\mathbb{P}_N(\mathbb{F}_{q^2}) & \supset & \mathbb{P}_N(\mathbb{F}_{q^2}) & \leftarrow & V_{N+1}(\mathbb{F}_{q^2}) - \{0\}
\end{array}$$

Letting $h \leq q^2 - q$ be the order of Véronèse's embedding, we get the codes C_h on $\mathbb{F}_{q^2}$ with parameters

$$\left[\frac{(q^{m+1} - (-1)^{m+1})(q^m - (-1)^m)}{(q^2 - 1)} \ , \ \binom{m+h}{h} \ , \ d\right]$$

where a bound for the minimal distance d can be easily computed by the general construction (3.1) and Proposition 2.3 in [7] which gives a bound for the number of rational points over $\mathbb{F}_{q^2}$ of an hyperplane section of the set G_1/P_1. We get

$$\begin{aligned}
d \geq \frac{(q^{m+1} - (-1)^{m+1})(q^m - (-1)^m)}{(q^2 - 1)} - (q+1)h\,\frac{q^{2m-2} - 1}{q^2 - 1} = \\
\frac{(q^{m+1} - (-1)^{m+1})(q^m - (-1)^m) - (q+1)h(q^{2m-2} - 1)}{q^2 - 1} \\
\geq q^{2m-1} + (1-h)q^{2m-3} - hq^{2m-4} + (1-h)q^{2m-5} - \cdots
\end{aligned}$$

For $h = 1$, Chakravarti ([1]) has actually computed the exact minimum distance

$$d = \begin{cases} q^{2m-1} & \text{for } m \text{ odd} \\ q^{2m-1} - q^{m-1} & \text{for } m \text{ even} \end{cases} .$$

For $h = 2$ and $m = 3$, we get the code with parameters

$$[(q^2 + 1)(q^3 + 1), 10, \geq q^5 - q^3 - q^2 - 2q - 1].$$

By a conjecture of Sørensen (cf. [7], [14]), the parameters would be

$$[(q^2 + 1)(q^3 + 1), 10, \geq q^5 - q^3 - q^2 + q].$$

For $h = 2$ and $m = 4$, we get the code with parameters

$$[(q^5 + 1)(q^2 + 1), 15, \geq q^7 - q^5 - 2q^4 - 2q^3 - q^2 - 2q - 1].$$

This is better than the bound obtained by other methods by S. Hansen ([4], Remark 5.23).

4.4 Codes on Deligne-Lusztig variety on the group $SU(5)$

As before, we consider the subgroup $G_1 = U(5, \mathbb{F}_{q^2})$ of the group $G = GL(5, \mathbb{F}_{q^2})$. The subgroup $U(5, \mathbb{F}_{q^2})$ is the unitary group for the hermitian form on $(\mathbb{F}_{q^2})^5$

$$\langle x, y \rangle = x_0 y_4^q + x_1 y_3^q + x_2 y_2^q + x_3 y_1^q + x_4 y_0^q \ .$$

We now take the parabolic subgroup

$$Q = \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & * \\ 0 & 0 & * & * & * \\ 0 & 0 & * & * & * \\ 0 & 0 & * & * & * \end{pmatrix}$$

and $Q_1 = U(m+1, \mathbb{F}_{q^2}) \cap Q$. The variety G_1/Q_1 can be viewed as the Deligne-Lusztig variety on the group $SU(5)$ (cf. [11]).

The diagram (1) simplifies to:

$$\begin{array}{ccccc} GL(5)/Q \supset & G_1/Q_1 & = & \{x_1, x_2, \ldots, x_n\} \\ \downarrow & & & \\ Gr(2,5) & \Big\downarrow & & \Big\downarrow \\ \text{Plücker} \downarrow & & & \\ \mathbb{P}_9 \quad = & \mathbb{P}_9(\mathbb{F}_{q^2}) & \longleftarrow & V_{10}(\mathbb{F}_{q^2}) - \{0\} \end{array} .$$

We get a code with parameters

$$[(q^5+1)(q^3+1), 10, q^8 - q^6] \qquad \text{on} \qquad \mathbb{F}_{q^2}$$

whose weights are $q^8 - q^6, q^8 - q^6 + q^5 - q^3, q^8 - q^6 + q^5, q^8 - q^6 + q^5 + q^3, q^8$. (Cf. [12]). For $q = 2$ we get a code $[297, 10, 192]$ on $\mathbb{F}_4$ whose weights are $256,\ 232,\ 224,\ 216,\ 192$.

5 One more Example

5.1 The Flag Variety of type $(1, m-2)$

Let us consider the variety of flags $X = \{(V_1, V_{m-1})\}$ made up by the lines V_1 and the hyperplanes V_{m-1}. We identify by duality the hyperplanes V_{m-1} with the elements $V_{m-1}^{\perp}$ of the projective space associated to the dual V^*.

The following diagram is commutative and defines the Segré embedding from $\mathbb{P}_{m-1} \times \mathbb{P}^*_{m-1}$ to $\mathbb{P}_{m^2-1}$:

$$\begin{array}{ccccc} (a, \beta) & \in & V^\times \times (V^*)^\times & \longrightarrow & (V \otimes V^*)^\times \\ \downarrow & & \downarrow & & \downarrow \\ (V_1, V_{m-1}^{\perp}) & \in & \mathbb{P}_{m-1} \times \mathbb{P}^*_{m-1} & \longrightarrow & \mathbb{P}_{m^2-1} \end{array} .$$

The flag (V_1, V_{m-1}) is in X if and only if $\langle V_1, V_{m-1}^{\perp} \rangle = 0$. Therefore a point x in $\mathbb{P}_{m^2-1}$ is in the image of X if and only if it is the image of $(a, \beta) \in V^\times \times (V^*)^\times$ with $\beta(a) = 0$. Two elements (a, β) and (a', β') of $V^\times \times (V^*)^\times$ give the same image in X if and only if $a' \in \mathbb{F}_q^\times a$ and $\beta' \in \mathbb{F}_q^\times \beta$. Let us denote by $\overline{a \otimes \beta}$ the image of (a, β) under the application $V^\times \times (V^*)^\times \longrightarrow \mathbb{P}_{m^2-1}$. Let us define a linear form Tr on $V \otimes V^*$ by $\mathrm{Tr}(a \otimes \beta) = \beta(a)$.

5.2 The Code

We consider the code C associated to the embedding $X \longrightarrow \mathbb{P}_{m^2-1}$. Let us choose a lifting of X into $V^\times \times (V^*)^\times$: $\overline{a \otimes \beta} \longmapsto (a, \beta)$. The codewords are the sequences $(f(a \otimes \beta))_{(a,\beta)}$ for (a, β) in the image of this given lifting and

$$f \in \{x \in V \otimes V^* \mid \mathrm{Tr}(x) = 0\}^* = \{x \in V \otimes V^*\}^* / \mathbb{F}_q \,\mathrm{Tr} \quad .$$

Theorem 1 *The code C is a code*

$$\left[\frac{(q^m - 1)(q^{m-1} - 1)}{(q-1)^2}, m^2 - 1, q^{2m-3} - q^{m-2} \right] \; .$$

The weights of C are given by

$$w = q^{m-2}\Big(q^m - 1 - \sum_{\lambda \in \mathbb{F}_q} (q^{a_\lambda} - 1) \Big) \Big/ (q-1)$$

where the $(a_\lambda)_{\lambda \in \mathbb{F}_q}$ are integers submitted to the following conditions:

$$0 \le a_\lambda \quad \text{and} \quad \sum_{\lambda \in \mathbb{F}_q} a_\lambda \le m.$$

Proof — The proof of this theorem is a consequence of the following propositions.

5.3 Computation of the Length of the Code C

Proposition 2 *The length of the code C is $n = (q^{m-1} - 1)(q^m - 1)/(q-1)^2$.*

Proof — Let us count the number of elements $(a, \beta) \in V^\times \times (V^*)^\times$ such that $\beta(a) = 0$. We have

$$\{(a, \beta) \in V^\times \times (V^*)^\times \mid \beta(a) = 0\} = \bigcup_{\beta \neq 0} ((a, \beta) \mid a \in \beta^\perp - \{0\}) \; .$$

Therefore

$$\#\{(a, \beta) \in V^\times \times (V^*)^\times \mid \beta(a) = 0\} = (q^{m-1} - 1)(q^m - 1) \; .$$

We assimilate $(V \otimes V^*)^*$ to $\mathrm{End}(V, V)$

$$\begin{aligned}(V \otimes V^*)^* &\longrightarrow \mathrm{End}(V, V)\\ f &\longmapsto e_f\end{aligned}$$

where e_f is defined by the condition $f(a \otimes \beta) = \beta(e_f(a))$ with $a \in V$, $\beta \in V^*$, for $f \in (V \otimes V^*)^*$. So we have $e_{\mathrm{Tr}} = Id_V$.

The weight of an element $\underline{\mathrm{ev}}(f) \in C$ is

$$w_f = \#\{(a, \beta) \in V^\times \times (V^*)^\times \mid f(a \otimes \beta) \neq 0, \beta(a) = 0\}/(q-1)^2 \ .$$

Let E_f be the image of the endomorphism e_f. We have

$$\begin{aligned}
&\{(a, \beta) \in V^\times \times (V^*)^\times \mid f(a \otimes \beta) = 0, \beta(a) = 0\}\\
&\quad = \{(a, \beta) \in V^\times \times (V^*)^\times \mid \beta(e_f(a)) = 0, \beta(a) = 0\}\\
&\quad = \bigcup_\beta \{(a, \beta) \in V^\times \times (V^*)^\times \mid e_f(a) \in \beta^\perp, a \in \beta^\perp\}\\
&\quad = \bigcup_{\beta \in (E_f^\perp)^\times} \{(a, \beta) \mid a \in \beta^\perp - \{0\}\} \cup\\
&\qquad\qquad \bigcup_{\beta \notin E_f^\perp} \Big(\{(a, \beta) \mid a \in e_f^{-1}\beta^\perp \cap \beta^\perp\} - \{0\}\Big) \ . \qquad (2)
\end{aligned}$$

Lemma 3 *The following equivalences are true.*

$$\begin{aligned}
\beta \in E_f^\perp &\Longleftrightarrow {}^t e_f(\beta) = 0\\
e_f^{-1}\beta^\perp = \beta^\perp &\Longleftrightarrow \exists \lambda \in \mathbb{F}_q^\times \ {}^t e_f(\beta) = \lambda\beta \ .
\end{aligned}$$

Proof — One has ${}^t e_f(\beta) = \beta \circ e_f$ and the first equivalence is trivial.

For the second, $e_f^{-1}\beta^\perp = \beta^\perp$ implies $\beta^\perp \cap E_f = e_f(\beta^\perp)$, whence $\beta(e_f(\beta^\perp)) = 0$ or ${}^t e_f(\beta)(\beta^\perp) = 0$, which means that there exists λ such that ${}^t e_f(\beta) = \lambda\beta$.

If $\lambda \neq 0$, ${}^t e_f(\beta) = \lambda\beta$ implies that for all x in V, $e_f(x) \in \beta^\perp \Longrightarrow \beta(x) = 0$ hence $e_f^{-1}(\beta^\perp) \subset \beta^\perp$ and $e_f^{-1}(\beta^\perp) = \beta^\perp$ for dimension reasons.

If $\lambda = 0$, ${}^t e_f(\beta) = 0$ implies that $e_f(V) \subset \beta^\perp$ therefore $V \subset e_f^{-1}(e_f(V)) \subset e_f^{-1}(\beta^\perp)$ hence $V = e_f^{-1}(\beta^\perp)$.

Proposition 4 *The weight of codeword* $\underline{\mathrm{ev}}(f)$ *in* C *is given by*

$$w_f = q^{m-2}(q^m - 1 - S_f)/(q-1)$$

where $S_f = \sum_{\lambda \in \mathbb{F}_q} (q^{a_\lambda} - 1)$ *where* a_λ *is the dimension the eigenspace of* ${}^t e_f$ *for the eigenvalue* λ.

Proof — The decomposition (2) and the equivalence in lemma 3 yield

$$\begin{aligned}&\{(a,\beta) \in V^\times \times (V^*)^\times \mid f(a \otimes \beta) = 0, \beta(a) = 0\} = \\ &\bigcup_{\lambda \in \mathbb{F}_q} \bigcup_{\substack{\beta \in f_\lambda \\ \beta \neq 0}} \Big(\big(\beta^\perp - \{0\}\big), \beta\Big) \cup \bigcup_{\text{other } \beta \neq 0} \Big(\big(e_f^{-1}\beta^\perp \cap \beta^\perp - \{0\}\big), \beta\Big) \ .\end{aligned}$$

where f_λ is the space of eigenvectors of ${}^t e_f$ for the eigenvalue λ. If β is not an eigenvector of e_f and if $\beta \neq 0$, the codimension of $e_f^{-1}\beta^\perp \cap \beta^\perp$ in V is 2 by lemma 3. Hence

$$\begin{aligned}&\#\{(a,\beta) \in V^\times \times (V^*)^\times \mid f(a \otimes \beta) = 0, \beta(a) = 0\} = \\ &\qquad S_f(q^{m-1} - 1) + (q^m - S_f - 1)(q^{m-2} - 1) \ .\end{aligned}$$

where S_f is the number of nonzero eigenvectors of ${}^t e_f$ belonging to an eigenvalue in $\mathbb{F}_q$.

$$S_f = \sum_{\lambda \in \mathbb{F}_q} \#(f_\lambda - \{0\}) = \sum_{\lambda \in \mathbb{F}_q} (q^{a_\lambda} - 1)$$

with $a_\lambda = \dim f_\lambda$. We have $0 \leq a_\lambda$ and $\sum a_\lambda \leq m$.

So the weights are given by

$$\begin{aligned}w_f = \#\{(a,\beta) \in V^\times \times (V^*)^\times \mid f(a \otimes \beta) \neq 0, \beta(a) = 0\}/(q-1)^2 = \\ q^{m-2}(q^m - 1 - S_f)/(q-1) \ .\end{aligned}$$

Remark 5 *For any* f*, the integers* a_λ *are only submitted to the following conditions:* $0 \leq a_\lambda$ *and* $\sum a_\lambda \leq m$.

5.5 Computation of the Dimension of the Code C

Proposition 6 *The dimension of the code* C *is* $k = m^2 - 1$.

Proof — A linear form belongs to the kernel of $\underline{\mathrm{ev}} : f \longmapsto (f(x_1), \ldots, f(x_n))$ if and only if $w_f = 0$ which means $S_f = q^m - 1$ that is ${}^t e_f \in \mathbb{F}_q \mathrm{Id}$. Therefore $k = m^2 - 1$.

5.6 Computation of the Minimal Distance of the Code C

Proposition 7 *The minimal distance of the code C is $d = q^{2m-3} - q^{m-2}$.*

Proof — The minimal distance corresponds to $w_f \neq 0$ minimum. This is equivalent to $S_f \neq q^m - 1$ maximum; that is ${}^t e_f \neq \mathbb{F}_q \mathrm{Id}$ has a maximal number of eigenvectors that is $(q^{m-1} - 1) + (q - 1)$ nonzero eigenvectors.

In this case, one has

$$\#\{(a, \beta) \in V^\times \times (V^*)^\times \mid f(a \otimes \beta) \neq 0, \beta(a) = 0\} = (q^{2m-3} - q^{m-2})(q-1)^2 \ .$$

5.7 Computation of the Number of Codewords of Minimum Weight

Proposition 8 *The number of codewords of minimum weight is $(q^m - 1)q^{m-1}$.*

Proof — We have to compute the number of e_f with $(q^{m-1} - 1) + (q - 1)$ nonzero eigenvectors. Such an e_f is semi-simple (the eigenvectors generate V). It may be defined by its eigenspace of dimension 1 (let us call it U_1) belonging to the eigenvalue λ_1, and its eigenspace of dimension $m - 1$ (let us call it U_2) belonging to the eigenvalue λ_2.

The set of possible line U_1 corresponds to the projective space $\mathbb{P}_{m-1}$. For every U_1, the set of subspace of dimension $m - 1$ such that $U_1 \cap U_2 = 0$ (that is $U_1 \not\subset U_2$), is equal to the set of linear forms ψ on V such that $\psi(U_1) \neq 0$. Therefore it corresponds to the affine space $\mathbb{A}_{m-1}$ of dimension $m - 1$.

So there are $\#(\mathbb{P}_{m-1} \times \mathbb{A}_{m-1})$ systems of eigenspace of e_f belonging to $q(q-1)$ systems of distinct eigenvalues (λ_1, λ_2).

We find therefore $\#\mathbb{P}_{m-1} \times \#\mathbb{A}_{m-1} \times q(q - 1) = (q^m - 1)q^{m-1}q$ possibilities for $e_f \in \mathrm{End}V$. Two functions e_f and e_g coincide on

$$\{(a, \beta) \in V^\times \times (V^*)^\times \mid \beta(a) = 0\}$$

if and only if $f - g \in \mathbb{F}_q \, \mathrm{Tr}$.

So we find $(q^m - 1)q^{m-1}$ possibilities for the f in

$$f \in \{x \in V \otimes V^* \mid \mathrm{Tr}(x) = 0\}^* \ .$$

6 Comparison with other classes of codes

6.1 *The code associated to the Flag Variety of type* $(1, m-2)$

We can compare this code to Reed-Muller codes.

6.1.1 $m = 3$

For $m = 3$, the flag variety is $X = GL(3)/B$ where B is a Borel subgroup of $GL(3)$. We get a code

$$[q^3 + 2q^2 + 2q + 1, 8, q^3 - q]$$

whose weights are, for $q \geq 3$: $q^3 + q^2 + q$, $q^3 + q^2$, $q^3 + q^2 - q$, $q^3 + q^2 - 2q$, q^3, $q^3 - q$.

It is comparable to the projective Reed-Muller code of order 2 which has for parameters

$$[q^3 + q^2 + q + 1, 10, q^3 - q^2].$$

6.1.2 $m = 4$

For $m = 4$, the flag variety is $X = GL(4)/P$ where P is the following subgroup of $GL(4)$:

$$P = \begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & 0 & 0 & * \end{pmatrix} .$$

We get a code

$$[q^5 + 2q^4 + 3q^3 + 3q^2 + 2q + 1, 15, q^5 - q^2]$$

whereas the projective Reed-Muller code of order 2 has for parameters

$$[q^5 + q^4 + q^3 + q^2 + q + 1, 21, q^5 - q^4].$$

6.2 *The codes on Deligne-Lusztig varieties on the group* $SU(5)$

For q a square, we obtain a code on $\mathbb{F}_q$ with parameters

$$[q^4 + \sqrt{q}^5 + \sqrt{q}^3 + 1, 10, q^4 - q^3]$$

as the projective Reed-Muller code of order 2 has for parameters

$$[q^4 + q^3 + q^2 + q + 1, 15, q^4 - q^3].$$

References

[1] Chakravarti, I.M.: Families of codes with few distinct weights from singular and nonsingular Hermitian varieties and quadrics in projective geometries and Hadamard difference sets and designs associated with two-weight codes. In Coding theory and design theory, Part I, IMA Vol. Math. Appl. **20** Springer-Verlag, New York (1990) 35-50.

[2] Duursma, I., Renteria, C., Tapia-Recillas, H.: Reed-Muller codes on complete intersections , AAECC, vol. **11** (2001), pp. 455-462.

[3] Ghorpade, S., Lachaud, G.: Higher Weights of Grassmann Codes. In Coding theory, cryptography and related areas (Guanajuato, 1998), Springer, Berlin (2000), pp. 122–131.

[4] Hansen, S.: Error-correcting codes from higher-dimensional varieties. To be published in Finite Fields and Applications.

[5] Hirschfeld, J.W.P., Tsfasman, M., Vladut, S.: The weight hierarchy of higher dimensional Hermitian codes. IEEE Trans. Inf. Theory **40**, No.1, (1994) 275-278.

[6] Lachaud, G.: The parameters of projective Reed-Muller codes. Discrete Math. **81** , no. 2, (1990) 217–221.

[7] Lachaud, G.: Number of points of plane sections and linear codes defined on algebraic varieties. In Arithmetic, geometry and coding theory (Luminy, 1993), de Gruyter, Berlin, (1996) 77-104.

[8] Manin, Y. , Vladut S.: Linear codes and modular curves. Itogi nauki i techniki, **25**, (1984), 209-257; english translation J. Soviet Math., **30**, (1985), 2611-2643.;

[9] Nogin, D.: Codes associated to Grassmannians. In Arithmetic, geometry and coding theory (Luminy, 1993), de Gruyter, Berlin, (1996) 77-104.

[10] Rodier, F.: Nombre de points des surfaces de Deligne-Lusztig. C. R. Acad. Sci. Paris, **322**, Série I, (1996) 563-566.

[11] Rodier, F.: Nombre de points des surfaces de Deligne-Lusztig. Journal of Algebra **227**, (2000), pp. 706-766.

[12] Rodier, F.: Sur les codes obtenus à l'aide des surfaces de Deligne-Lusztig, (in preparation).

[13] Shafarevitch, I.: Basic Algebraic Geometry, Springer-Verlag, 1994.

[14] Sørensen, A.: Projective Reed-Muller codes. IEEE Trans. Inform. Theory **37** no. 6, (1991),1567–1576.

[15] Tsfasman, M. , Vladut, S.: Algebraic-geometric codes, Mathematics and its Applications (Soviet Series), 58. Kluwer Academic Publishers Group, Dordrecht, 1991.