Linear Codes associated to Grassmann and Flag Varieties

Sudhir R. Ghorpade

Department of Mathematics
Indian Institute of Technology Bombay
Powai, Mumbai 400076, India
http://www.math.iitb.ac.in/∼srg/

AGCT–2017
CIRM, Luminy, France
June 20, 2017

Dedicatory

This talk is dedicated to the memory of

Alexey Zykin (13 June 1984 – 23 April 2017).

Review of Coding Theory

- $[n,k]_q$-code: a k-dimensional subspace C of $\mathbb{F}_q^n$.
- Hamming weight of $c = (c_1, \dots, c_n) \in \mathbb{F}_q^n$: $\quad \mathrm{wt}(c) := |\{i : c_i \neq 0\}|$.
- Hamming weight of a subcode D of C:

$$\mathrm{wt}(D) := |\{i : \exists\, c = (c_1, \dots, c_n) \in D \text{ with } c_i \neq 0\}|.$$

- Minimum distance of a (linear) code C:

$$d(C) := \min\{\mathrm{wt}(c) : c \in C,\ c \neq 0\}.$$

- The r^{th} higher weight of C ($1 \le r \le k$):

$$d_r(C) := \min\{\mathrm{wt}(D) : D \subseteq C,\ \dim D = r\}.$$

- C is nondegenerate if $C \not\subseteq$ coordinate hyperplane of $\mathbb{F}_q^n$, i.e., $d_k(C) = n$.
- Dual of C: $\quad$ the $[n-k, n]_q$-code $C^\perp := \{x \in \mathbb{F}_q^n : x \cdot c = 0\ \forall\, c \in C\}$.

Automorphisms of a Linear Code

The automorphisms of a $[n,k]_q$-code C come in three flavours:

1. Permutation Automorphism Groups:

$$\begin{aligned}\mathrm{PAut}(C) &= \left\{\sigma \in S_n : \left(c_{\sigma(1)}, \ldots, c_{\sigma(n)}\right) \in C \;\forall\, (c_1, \ldots, c_n) \in C\right\} \\ &= \{P \in \mathrm{PermMat}_n(\mathbb{F}_q) : cP \in C \;\forall\, c \in C\}\end{aligned}$$

2. Monomial Automorphism Groups:

$$\mathrm{MAut}(C) = \{M \in \mathrm{MonMat}_n(\mathbb{F}_q) : cM \in C \;\forall c \in C\}$$

   Both $\mathrm{PAut}(C)$ and $\mathrm{MAut}(C)$ are subgroups of $\mathrm{GL}(n, \mathbb{F}_q)$.

3. (Semilinear) Automorphism Groups:

$$\Gamma\mathrm{Aut}(C) = \{M\mu : M \in \mathrm{MonMat}_n(\mathbb{F}_q),\ \mu \in \mathrm{Aut}(\mathbb{F}_q) \text{ and } cM\mu \in C \;\forall c \in C\}$$

   $\Gamma\mathrm{Aut}(C)$ is a subgroup of the group $\Gamma\mathrm{L}(n, \mathbb{F}_q)$ of semilinear transformations of $\mathbb{F}_q^n$.

What is a good code?

Often, one likes to construct $[n,k]_q$-codes that satisfy one or more of the following requirements (some of which may conflict with each other):

- $d = d(C)$ is large vis-a-vis n, e.g., it's nice if $\delta = d/n$ is close to 1.
- k is also large vis-a-vis n, e.g., it's nice if $R = k/n$ is close to 1.
- C admits "good encoding and decoding"
- Automorphism group(s) of C are known and have a fairly large size.
- The higher weights $d_r(C)$ are known for $1 \le r \le k$.
- The "spectrum" of C is known.
- C is a LDPC code; this is typically the case when $d(C^\perp)$ is small and the minimum weight codewords of $C^\perp$ generate $C^\perp$
- . . .

A Geometric Language for Codes

Projective Systems à la Tsfasman-Vlăduţ

A $[n,k]_q$-projective system is a collection $\mathcal{P}$ of n not necessarily distinct points in $\mathbb{P}^{k-1}$; this is nondegenerate if it is not contained in a hyperplane.

$$[n,k]_q\text{-code } \mathcal{C} \rightsquigarrow [n,k]_q\text{-projective system } \mathcal{P}$$

Conversely a nondegenerate $[n,k]_q$-projective system gives rise to a nondegenerate $[n,k]_q$-code, and the resulting correspondence is a bijection, up to equivalence. Note that

$$d(\mathcal{C}) = n - \max\{|\mathcal{P} \cap H| : H \text{ hyperplane of } \mathbb{P}^{k-1}\}.$$

and for $r = 1, \ldots, k$,

$$d_r(\mathcal{C}) = n - \max\{|\mathcal{P} \cap E| : E \text{ linear subvariety of codim } r \text{ in } \mathbb{P}^{k-1}\}.$$

Automorphisms of Projective Systems

- Let $\mathcal{P}$ be a $[n,k]_q$-projective system.
- The automorphism group $\Gamma\mathrm{Aut}(\mathcal{P})$ of $\mathcal{P}$ is the subgroup of $\mathrm{P\Gamma L}(k,\mathbb{F}_q)$ of transformations taking $\mathcal{P}$ to itself. Note that $\mathrm{P\Gamma L}(k,\mathbb{F}_q)$ is the group of all semilinear isomorphisms of $\mathbb{P}^{k-1}_{\mathbb{F}_q}$. Elements of $\mathrm{P\Gamma L}(k,\mathbb{F}_q)$ are known in the classical literature as *collineations*.
- If $\mathcal{C}$ is the linear $[n,k]_q$-code corresponding to $\mathcal{P}$, then $\Gamma\mathrm{Aut}(\mathcal{C})$ is closely related to $\Gamma\mathrm{Aut}(\mathcal{P})$. In fact, $\Gamma\mathrm{Aut}(\mathcal{C})$ is a central extension of $\Gamma\mathrm{Aut}(\mathcal{P})$ by $\mathbb{F}_q^\times$, i.e., $\Gamma\mathrm{Aut}(\mathcal{P}) \simeq \Gamma\mathrm{Aut}(\mathcal{C})/\mathbb{F}_q^\times$, where $\mathbb{F}_q^\times$ is the subgroup of scalar matrices in $\mathrm{GL}(n,\mathbb{F}_q)$.
- The projective linear isomorphisms (known in the classical literature as *projectivities*) among $\Gamma\mathrm{Aut}(\mathcal{P})$ form a subgroup $\mathrm{MAut}(\mathcal{P})$ of $\mathrm{PGL}(k,\mathbb{F}_q)$ that corresponds to $\mathrm{MAut}(\mathcal{C})$.

Grassmann Varieties : A Quick Introduction

V : vector space of dimension m over a field $\mathbb{F}$

For $1 \le \ell \le m$, we have the Grassmann variety:

$$G_{\ell,m} = G_\ell(V) := \{\ell\text{-dimensional subspaces of } V\}.$$

Plücker embedding: $G_{\ell,m} \hookrightarrow \mathbb{P}^{k-1}$, where $k := \binom{m}{\ell}$.

Explicitly, $\mathbb{P}^{k-1} = \mathbb{P}(\wedge^\ell V)$ and

$$W = \langle w_1, \dots, w_\ell \rangle \longleftrightarrow [w_1 \wedge \cdots \wedge w_\ell] \in \mathbb{P}(\wedge^\ell V).$$

For example, $G_{1,m} = \mathbb{P}^{m-1}$. In terms of coordinates,

$$W = \langle w_1, \dots, w_\ell \rangle \in G_\ell(V) \longleftrightarrow p(W) = \left(p_\alpha(A_W)\right)_{\alpha \in I(\ell,m)},$$

where $A_W = (a_{ij})$ is a $\ell \times m$ matrix whose rows are (the coordinates of) a basis of W and $p_\alpha(A_W)$ is the α^{th} minor of A_W, viz., $\det\left(a_{i\alpha_j}\right)_{1 \le i,jj \le \ell}$.

Introduction to Grassmann Varieties Contd.

Notation: $I(\ell,m) := \left\{\alpha = (\alpha_1,\ldots,\alpha_\ell) \in \mathbb{Z}^\ell : 1 \le \alpha_1 < \cdots < \alpha_\ell \le m\right\}$.

Facts:

- $G_{\ell,m}$ is a projective algebraic variety given by the common zeros of certain quadratic homogeneous polynomials in k variables. As a projective algebraic variety $G_{\ell,m}$ is nondegenerate, irreducible, nonsingular, and rational.
- There is a natural transitive action of GL_m on $G_{\ell,m}$ and if P_ℓ denotes the stabilizer of a fixed $W_0 \in G_{\ell,m}$, then P_ℓ is a maximal parabolic subgroup of GL_m and $G_{\ell,m} \simeq \mathrm{GL}_m/P_\ell$.
- If $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, then $G_{\ell,m}$ is a (real or complex) manifold, and its cohomology spaces and Betti numbers are explicitly known. In fact, $b_\nu = \dim H^{2\nu}(G_{\ell,m};\mathbb{C})$ is precisely the number of partitions of ν into at most ℓ parts, each part $\le m-\ell$,

Grassmannian Over Finite Fields

Suppose $\mathbb{F} = \mathbb{F}_q$ is the finite field with q elements. Then $G_{\ell,m} = G_{\ell,m}(\mathbb{F}_q)$ is a finite set and its cardinality is given by the Gaussian binomial coefficient:

$$\begin{bmatrix} m \\ \ell \end{bmatrix}_q := \frac{(q^m - 1)(q^m - q)\cdots(q^m - q^{\ell-1})}{(q^\ell - 1)(q^\ell - q)\cdots(q^\ell - q^{\ell-1})}.$$

This is a polynomial in q of degree $\delta := \ell(m-\ell)$ and in fact,

$$|G_{\ell,m}(\mathbb{F}_q)| = \begin{bmatrix} m \\ \ell \end{bmatrix}_q = \sum_{\nu=0}^{\delta} b_\nu q^\nu = q^\delta + q^{\delta-1} + 2q^{\delta-2} + \cdots + 1.$$

Note that

$$\lim_{q\to 1} \begin{bmatrix} m \\ \ell \end{bmatrix}_q = \binom{m}{\ell}.$$

Grassmann Codes

Thanks to the Plücker embedding,

$$G_{\ell,m}(\mathbb{F}_q) \hookrightarrow \mathbb{P}^{k-1} \rightsquigarrow [n,k]_q\text{-code } C(\ell,m).$$

Length n is the Gaussian binomial coefficient:

$$n = \begin{bmatrix} m \\ \ell \end{bmatrix}_q := \frac{(q^m-1)(q^m-q)\cdots(q^m-q^{\ell-1})}{(q^\ell-1)(q^\ell-q)\cdots(q^\ell-q^{\ell-1})}.$$

and the dimension k is the binomial coefficient:

$$k = \binom{m}{\ell}.$$

Theorem (Ryan (1990, $q=2$), Nogin (1996, any q))

$$d\left(C(\ell,m)\right) = q^\delta \quad \textit{where} \quad \delta := \ell(m-\ell).$$

It may be noted that δ is the dimension of $G_{\ell,m}$ as a projective variety.

Higher Weights of Grassmann Codes

Let $\mu := \max\{\ell, m-\ell\} + 1$.

Theorem (Nogin (1996), G-Lachaud(2000))

For $1 \le r \le \mu$, *we have*

$$d_r\left(C(\ell, m)\right) = q^\delta + q^{\delta-1} + \cdots + q^{\delta-r+1}.$$

One has the following counterpart from the other end.

Theorem (Hansen-Johnsen-Ranestad (2007))

On the other hand, for $0 \le r \le \mu$,

$$d_{k-r}\left(C(\ell, m)\right) = n - (1 + q + \cdots + q^{r-1}).$$

These results cover several initial and terminal elements of the weight hierarchy of $C(\ell, m)$. Yet, a considerable gap remains.

Narrowing the gap

Examples:

- $(\ell, m) = (2, 5)$. Here $k = 10$, $\mu = 4$ and we know:

  $$d_1, \ldots, d_4 \quad \text{as well as} \quad d_6, \ldots, d_{10}.$$

  But d_5 seems to be unknown.
- $(\ell, m) = (2, 6)$. Here $k = 15$, $\mu = 5$ and $d_6, \ldots, d_9$ are not known.
- For $C(2, m)$ with $m \geq 2$, the values of d_r for $m \leq r < \binom{m-1}{2}$ do not seem to be known.

Theorem (Hansen-Johnsen-Ranestad (2007))

$$d_5(C(2,5)) = q^6 + q^5 + 2q^4 + q^3 = d_4 + q^4.$$

Conjecture (Hansen-Johnsen-Ranestad (2007))

$d_r - d_{r-1}$ is always a power of q.

One step forward

Theorem (G-Patil-Pillai (2009))

Assume that $\ell = 2$ *and* $m \geq 4$ *so that*

$$\mu = \max\{2, m-2\} + 1 = m - 1 \text{ and } k = \binom{m}{2}.$$

Then

$$d_{\mu+1}(C(2,m)) = d_\mu + q^{\delta-2} \text{ and } d_{k-\mu-1}(C(2,m) = n - \left(1 + q + \cdots + q^\mu + q^2\right).$$

Corollary. Complete weight hierarchy of $C(2,5)$.

Remark. The proof of the above theorem uses a characterization of decomposable subspaces of $\wedge^\ell V$ where V is an m-dimensional vector space, or in geometric terms, a characterization of linear subvarieties of the Grassmannian $G_{\ell,m}$.

Complete weight hierarchy of $C(2, m)$

Consider the (strict) Young tableau $Y = Y_m$ corresponding to the partition $(m-1, m-2, \ldots, 2, 1)$ of $k = \binom{m}{2}$ with

$$Y_{ij} = 2i + j - 3 \quad \text{for } 1 \le i \le m-1 \text{ and } 1 \le j \le m-i.$$

Then

$$n = \mathsf{C}_q(Y) = \sum_{\nu \ge 0} c_\nu(Y) q^\nu,$$

where $c_\nu(Y)$= $\#$ of times ν appears in Y.

Theorem (G-Patil-Pillai)

If $T_1, \ldots, T_h$ are strict subtableaux of Y of area $r = k - s$, and

$$g_s(2, m) := \max\{\mathsf{C}_q(T_1), \ldots, \mathsf{C}_q(T_h)\},$$

then

$$d_s\left(C(2, m)\right) = n - g_s(2, m) \quad \text{for } 1 \le s \le k.$$

Schubert Unions and Grassmann Codes

Hansen-Johnsen-Ranestad (2007, 2009) also considered:

Schubert Unions: These are subsets of $G_{\ell,m}$ of the form

$$\Omega_U = \bigcup_{\alpha \in U} \Omega_\alpha \quad \text{for } U \subseteq I(\ell, m).$$

It is easy to see that Schubert unions are linear sections of $G_{\ell,m}$.

Schubert Union Conjecture (Hansen-Johnsen-Ranestad)

The higher weights of $C(\ell, m)$ are are always computed by Schubert unions.

It turns out that there is a one-to-one correspondence between the strict subtableaux T of Y and Schubert unions Ω_U in such a way that $C_q(T) = |\Omega_U(\mathbb{F}_q)|$. This leads to:

Theorem (G-Johnsen-Patil-Pillai)

The Schubert Union Conjecture holds in the affirmative when $\ell = 2$.

Automorphisms of Grassmann Codes

Let ℓ, m be positive integers such that $1 \le \ell < m$. Consider the Grassmann code $C(\ell, m)$ corresponding to the projective system

$$\mathcal{P} = G_{\ell,m}(\mathbb{F}_q) \hookrightarrow \mathbb{P}^{k-1}, \quad \text{where} \quad k = \binom{m}{\ell}.$$

Theorem (Chow, 1949; G-Kaipa, 2013)

If $m \neq 2\ell$, then

$$\mathrm{Aut}(\mathcal{P}) \simeq \mathrm{P\Gamma L}(m, \mathbb{F}_q) \hookrightarrow \mathrm{P\Gamma L}(k, \mathbb{F}_q),$$

whereas if $m = 2\ell$, then

$$\mathrm{Aut}(\mathcal{P}) \simeq \mathrm{P\Gamma L}(m, F) \rtimes_{-t} \mathbb{Z}/2\mathbb{Z},$$

where the generator of $\mathbb{Z}/2\mathbb{Z}$ acts on $\mathrm{P\Gamma L}(m, F)$ by the "inverse transpose outer automorphism" $-t$.

As noted earlier, $\Gamma\mathrm{Aut}(\mathcal{C})$ is a central extension of $\Gamma\mathrm{Aut}(\mathcal{P})$ by $\mathbb{F}_q^\times$. A more precise description can be given using group cohomology.

Automorphisms of Grassmann Codes Contd.

Theorem (G-Kaipa, 2013)

The automorphism group of $\mathcal{C} = C(\ell, m)$ *is given by*

$$\mathrm{Aut}(\mathcal{C}) = \begin{cases} \mathcal{G} & \text{if } m \neq 2\ell, \\ \mathcal{G} \rtimes_{-t} \mathbb{Z}/2\mathbb{Z} & \text{if } m = 2\ell. \end{cases}$$

where $\mathcal{G}$ *is a central extension of* $(\mathrm{P\Gamma L}(m, \mathbb{F}_q) \times \mu_\lambda)$ *by* $\mu_{\lambda'}$*, corresponding to the class*

$$[\alpha] \otimes 1 + 1 \otimes [\beta] \in H^2((\mathrm{P\Gamma L}(m, \mathbb{F}_q) \times \mu_\lambda), \mu_{\lambda'}),$$

where $[\alpha] \in H^2(\mathrm{P\Gamma L}(m, \mathbb{F}_q), \mu_{\lambda'})$ *and* $[\beta] \in H^2(\mu_\lambda, \mu_{\lambda'})$ *are classes representing the* $\mu_{\lambda'}$*-extensions* $(\Gamma\mathrm{L}(m, \mathbb{F}_q)/\mu_\lambda)$ *and* $\mathbb{F}_q^\times$*, where* $\lambda = \mathrm{GCD}(q-1, \ell)$*,* $\lambda' = (q-1)/\lambda$*, and* μ_λ *and* $\mu_{\lambda'}$ *denote the groups of* λ*-th and* λ'*-th roots of unity in* $\mathbb{F}_q^\times$*.*

More on Grassmann Codes

The duals of Grassmann codes have a very low minimum distance, and a nice structure.

Theorem (Beelen-Piñero, 2015)

$d\left(C(\ell,m)^{\perp}\right)=3$. *Moreover,* $C(\ell,m)^{\perp}$ *is generated by its minimum weight codewords.*

We mention briefly some other results on Grassmann and related codes.

- The spectrum of the Grassmann code $C(\ell,m)$ is known when $\ell=2$ [Nogin, 1996] and when $(\ell,m)=(3,6)$ [Nogin, 1997], and also when $(\ell,m)=(3,7)$ [Kaipa-Pillai, 2013].
- Permutation decoding of Grassmann codes, capable of correcting up to n/k errors, has recently been described [G-Piñero, 2017].

Codes associated to (generalized) flag varieties

Fix an m-dimensional vector space V and a sequence

$$\underline{\ell} = (\ell_1, \ldots, \ell_s) \in \mathbb{Z}^s \text{ with } 0 \le \ell_1 \le \cdots \le \ell_s < m.$$

We can consider the variety of (generalized) partial flags:

$$\mathcal{F}_{\underline{\ell}}(V) := \{(V_1, \ldots, V_s) : V_1 \subseteq \cdots \subseteq V_s,\ \dim V_i = \ell_i,\ i = 1, \ldots, s\}.$$

Thanks to Plücker and Segre,

$$\mathcal{F}_{\underline{\ell}}(V) \hookrightarrow \prod_{i=1}^{s} G_{\ell_i,m} \hookrightarrow \prod_{i=1}^{s} \mathbb{P}^{k_i-1} \hookrightarrow \mathbb{P}^{(k_1\cdots k_s)-1} = \mathbb{P}(\bigotimes_{i=1}^{s} \bigwedge^{\ell_i} V) =: T_{\underline{\ell}}(V)$$

where $k_i = \binom{m}{\ell_i}$. As before,

$$\mathcal{F}_{\underline{\ell}}(V)\,(\mathbb{F}_q) \rightsquigarrow [n_{\underline{\ell}}, k_{\underline{\ell}}]_q\text{-code } C(\underline{\ell}; m).$$

We may call $C(\underline{\ell}; m)$ as the flag code or s-step flag code corresponding to $\underline{\ell}$.

Flag varieties and associated codes

- The variety $\mathcal{F}_{\underline{\ell}}(V)$ of (generalized) partial flags can also be viewed as

$$\mathcal{F}_{\underline{\ell}}(V) = \left\{ \left[\bigotimes_{i=1}^{s} v_1 \wedge \cdots \wedge v_{\ell_i} \right] : v_1, \ldots, v_{\ell_s} \in V \text{ linearly indep.} \right\}.$$

- $\mathcal{F}_{\underline{\ell}}(V)$ is a projective variety of dimension

$$\delta(\underline{\ell}) := \sum_{i=1}^{s} (\ell_i - \ell_{i-1})(m - \ell_i).$$

- Let

$$T_{\underline{\ell}}(V) = \bigotimes_{i=1}^{s} \bigwedge^{\ell_i} V \quad \text{and} \quad T^*_{\underline{\ell}}(V) = \bigotimes_{i=1}^{s} \bigwedge^{m-\ell_i} V \simeq T_{\underline{\ell}}(V)^*$$

- The code $C(\underline{\ell}; m)$ corresponding to $\mathcal{F}_{\underline{\ell}}(V)$ can be viewed as the image of

$$\mathrm{Ev} : T^*_{\underline{\ell}}(V) \to \mathbb{F}_q^{n_{\underline{\ell}}} \quad \text{given by} \quad \mathrm{Ev}(f) := \big(f(P_1), \ldots, f(P_{\underline{\ell}})\big)$$

  where $P_1, \ldots, P_{\underline{\ell}}$ are fixed representatives in $T_{\underline{\ell}}(V)$ of points of $\mathcal{F}_{\underline{\ell}}(V)(\mathbb{F}_q)$.

Special partial flags: Line-Hyperplane Incidence

Theorem (Rodier, 2003)

If $s = 2$ and $\underline{\ell} = (1, m-1)$, then

$$n_{\underline{\ell}} = \frac{(q^m - 1)(q^{m-1} - 1)}{(q-1)^2} \text{ and } k_{\underline{\ell}} = m^2 - 1.$$

Moreover,

$$d(C(\underline{\ell}; m)) = q^{2m-3} - q^{m-2} = q^{m-2}(q^{m-1} - 1).$$

Theorem (Hana, 2010)

$$q^{\delta(\underline{\ell})} \left(\frac{q-1}{q}\right)^{\ell_s - 1} \leq d(C(\underline{\ell}; m)) \leq q^{\delta(\underline{\ell})}.$$

Further, if $s = 2$, $\ell_1 < \ell_2$ and $\ell_1 + \ell_2 \leq m$, then

$$d(C(\underline{\ell}; m)) \leq q^{\ell_2(m-\ell_2) - \ell_1^2}(q^{\ell_2} - 1)(q^{\ell_2} - q) \cdots (q^{\ell_2} - q^{\ell_1 - 1}).$$

The length $n_{\underline{\ell}}$ of $C(\underline{\ell}, m)$

$$n_{\underline{\ell}} = \begin{bmatrix} m \\ \ell_1,\ \ell_2 - \ell_1, \ldots, \ell_{s+1} - \ell_s \end{bmatrix} = \prod_{i=1}^{s} \begin{bmatrix} m - \ell_{i-1} \\ \ell_i - \ell_{i-1} \end{bmatrix}$$

where, by convention, $\ell_0 := 0$ and $\ell_{s+1} := m$.

Equivalently, the length $n_{\underline{\ell}}$ is given by

$$n_{\underline{\ell}} = \sum_{\sigma \in W_{\underline{\ell}}} q^{\mathrm{inv}(\sigma)} = \sum_{\tau \in M_{\underline{\ell}}} q^{\mathrm{inv}(\tau)}$$

where $W_{\underline{\ell}}$: permutations $\sigma \in S_m$ satisfying

$$\sigma(\ell_{i-1} + 1) < \sigma(\ell_{i-1} + 2) < \cdots < \sigma(\ell_i),$$

for $i = 1, \ldots, s+1$, and $M_{\underline{\ell}}$: permutations of the multiset

$$\{1^{\ell_1}, 2^{\ell_2 - \ell_1}, \ldots, s^{\ell_s - \ell_{s-1}}, (s+1)^{m - \ell_s}\}$$

and inv denotes the number of inversions.

See, for example, [G-Lachaud, 2002].

The case of 2-step flags

- For $0 \le t \le m$, set $\mathbb{I}(t,m) := \{I = (i_1, \ldots, i_t) : 1 \le i_1 < \ldots < i_t \le m\}$.
- Fix a basis $\{e_1, \ldots, e_m\}$ of V. For $I = (i_1, \ldots, i_t) \in \mathbb{I}(t,m)$, put $e_I := e_{i_1} \wedge \cdots \wedge e_{i_t} \in \wedge^t V$.
- For any $0 \le t_2 \le t_1 \le m$ and $I \in \mathbb{I}(t_1, m)$ and $J \in \mathbb{I}(t_2, m)$, define

$$I = (i_1, \ldots, i_{t_1}) \le J = (j_1, \ldots, j_{t_2}) \iff i_r \le j_r \text{ for } r = 1, \ldots, t_1$$

Theorem (G, Singh, Piñero, 2017)

Let $s = 2$. A basis for the flag code $C(\underline{\ell}; m) = \mathrm{Ev}(T^*_{\underline{\ell}}(V))$ is given by

$$\{\mathrm{Ev}(e_I \otimes e_J) : (I,J) \in \mathbb{I}(m-\ell_1, m) \times \mathbb{I}(m-\ell_2, m),\ I \le J\}.$$

Consequently, the dimension of the 2-step flag code $C(\underline{\ell}; m)$ is given by

$$k_{\underline{\ell}} = \binom{m}{\ell_1}\binom{m}{\ell_2} - \binom{m}{\ell_1 - 1}\binom{m}{\ell_2 + 1}.$$

Minimum Distance for 2-step flags

Lemma

Assume that $s = 2$ and $\ell_1 + \ell_2 \leq m$. Then

$$d(C(\underline{\ell}; m)) \leq q^{\ell_2(m-\ell_2)-\ell_1^2}|GL_{\ell_1}(\mathbb{F}_q)||G_{\ell_1,\ell_2}(\mathbb{F}_q)|.$$

Theorem (G, Singh, Piñero, 2017)

Assume that $s = 2$ and $\ell_1 + \ell_2 \leq m$. Write $\underline{\ell} = (\ell_1, \ell_2)$ and $\underline{\ell'} = (\ell_1, \ell_1)$. If the minimum distance of the code $C(\underline{\ell'}; m)$ is $q^{\ell_1(m-\ell_1)-\ell_1^2}|\mathrm{GL}_{\ell_1}(\mathbb{F}_q)|$, then

$$d(C(\underline{\ell}; m)) = q^{\ell_2(m-\ell_2)-\ell_1^2}|GL_{\ell_1}(\mathbb{F}_q)||G_{\ell_1,\ell_2}(\mathbb{F}_q)|.$$

Corollary

If $s = 2$, $1 \leq \ell < m$, and $\underline{\ell} = (1, \ell)$, then

$$d(C(\underline{\ell}; m)) = q^{\ell(m-\ell)-1}(q^\ell - 1).$$

A General Formula for the dimension $k_{\underline{\ell}}$ of $C(\underline{\ell}, m)$

Given $\underline{\ell} = (\ell_1, \dots, \ell_s)$, consider the partition

$$m - \ell_1 \geq m - \ell_2 \geq \cdots \geq m - \ell_s \geq 1$$

and let λ be the conjugate partition.

For example if $m = 8$ and $\underline{\ell} = (1, 3, 6, 7)$, then the associated partition is $(7, 5, 2, 1)$ and the conjugate partition is $\lambda = (4, 3, 2, 2, 2, 1, 1)$. These partitions can be viewed as folllows.

Description of $k_{\underline{\ell}}$ Contd.

For each box (i,j) in the (Young diagram of) λ, let $h_{(i,j)}$ be the hook length at (i,j), that is, the number of boxes in the hook at (i,j). For example the hook at $(2,2)$ in the partition $\lambda = (4,3,2,2,2,1,1)$ is shown by shaded boxes and we have $h_{(2,2)} = 5$.

Theorem

The dimension $k_{\underline{\ell}}$ of $C(\underline{\ell}, m)$ is given by

$$k_{\underline{\ell}} = \prod_{(i,j)\in\lambda} \frac{m+j-i}{h_{(i,j)}}.$$

Idea: Use the connection between flag varieties and representations of linear groups together with classical results from Combinatorial Representation Theory. However, one should be careful in applying classical results to the case of finite ground field $\mathbb{F}_q$; in particular, it is better to assume $s \leq q$.

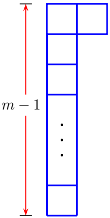
Example (2-Step Flag Code of Rodier): If $\underline{\ell} = (1, m-1)$, then

$$\lambda = \text{conjugate of } (m-1, 1) = (2, \underbrace{1, 1, \ldots, 1}_{m-2 \text{ times}}).$$

Hence by the above formula

$$\begin{aligned} k_{\underline{\ell}} &= \frac{m(m+1)(m-1)(m-2)\cdots(m-(m-2))}{m(1)(m-2)(m-3)\cdots 1} \\ &= (m+1)(m-1) = m^2 - 1, \end{aligned}$$

as is to be expected.



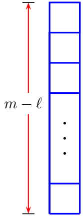
Another Example (Grassmann codes): If $\underline{\ell} = (\ell)$, then

$$\lambda = \text{conjugate of } (m-\ell) = (\underbrace{1, 1, \ldots, 1}_{m-\ell \text{ times}}).$$

Hence by the above formula

$$\begin{aligned} k_{\underline{\ell}} &= \frac{m(m-1)(m-2)\cdots(m-(m-\ell)+1)}{(m-\ell)(m-\ell-1)\cdots 1} \\ &= \frac{m!}{\ell!(m-\ell)!} = \binom{m}{\ell} \end{aligned}$$

as is to be expected.



Thank you!