Linear Codes associated to Determinantal Varieties

Peter Beelen[1] Sudhir R. Ghorpade[2] Sartaj Ul Hasan[3]

Technical University of Denmark, Lyngby, Denmark

Indian Institute of Technology Bombay, Powai, Mumbai, India

Scientific Analysis Group, DRDO, Delhi, India

ACCT-14

Svetlogorsk (Kaliningrad region), Russia

September 11, 2014

http://www.math.iitb.ac.in/∼srg/

(Linear) Codes

- $\mathbb{F}_q$: finite field with q elements.
- $[n,k]_q$-code: a k-dimensional subspace C of $\mathbb{F}_q^n$.
- C is nondegenerate if $C \not\subseteq$ coordinate hyperplane of $\mathbb{F}_q^n$.
- Hamming weight of $c = (c_1, \dots, c_n) \in \mathbb{F}_q^n$:

$$w_H(c) := \#\{i : c_i \neq 0\}.$$

- Hamming weight of a subset D of $\mathbb{F}_q^n$:

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

- Minimum distance of a (linear) code C:

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

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

$$d_r(C) := \min\{w_H(D) : D \text{ subspace of } C,\ \dim D = r\}.$$

- Spectrum or the Weight distribution of a code C:

the sequence $(A_i)_{i \geq 0}$ where $A_i := \#\{c \in C : w_H(c) = i\}$.

- $[n, k]_q$-projective system: collection $\mathcal{P}$ of n not necessarily distinct points in $\mathbb{P}^{k-1}$;
- $\mathcal{P}$ is nondegenerate if $\mathcal{P} \not\subseteq$hyperplane in $\mathbb{P}^{k-1}$.
- Every nondegenerate $[n, k]_q$-code $\mathcal{C}$ gives rise to a nondegenerate $[n, k]_q$-projective system $\mathcal{P}$, and vice-versa. The resulting correspondence is a bijection, up to equivalence.

In this set-up,

$$\text{codeword } c \text{ of } \mathcal{C} \leftrightsquigarrow \text{hyperplanes } H_c \text{ of } \mathbb{P}^{k-1} = \mathbb{P}(\mathcal{C}^*)$$
$$w_H(c) = n - \#(\mathcal{P} \cap H_c)$$
$$d(\mathcal{C}) = n - \max\{\#\mathcal{P} \cap H : H \text{ hyperplane of } \mathbb{P}^{k-1}\}$$

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

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

- Projective Reed-Muller code of order u:

$$\mathrm{PRM}(u,m) \leftrightsquigarrow \mathcal{P} = \mathbb{P}^m \hookrightarrow \mathbb{P}^{k-1} \quad \text{where} \quad k := \binom{m+u}{u}$$

and the embedding is the Veronese embedding of order u.

- (Generalized) Reed-Muller code of order u and length q^m:

$$\mathrm{RM}(u,m) \leftrightsquigarrow \mathcal{P} = \mathbb{A}^m \subset \mathbb{P}^m \hookrightarrow \mathbb{P}^{k-1}$$

- Grassmann code

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

and the embedding is the Plücker embedding.

- Affine Grassmann code

$$C^{\mathbb{A}}(\ell,m) \leftrightsquigarrow \mathcal{P} = \mathbb{A}^{\ell(m-\ell)} \subset G_\ell(\mathbb{F}_q^m) \hookrightarrow \mathbb{P}^{k-1}$$

Determinantal Codes

Fix a prime power q, positive integers t, ℓ, m, and define:

- $X = (X_{ij})$: a $\ell \times m$ matrix with variable entries
- $\mathbb{F}_q[X]$: polynomial ring over $\mathbb{F}_q$ in the ℓm variables X_{ij}
- $\mathbb{M}_{\ell \times m}(\mathbb{F}_q)$: set of all $\ell \times m$ matrices with entries in $\mathbb{F}_q$
- $\mathcal{I}_{t+1}$: ideal of $\mathbb{F}_q[X]$ generated by all $(t+1) \times (t+1)$ minors
- $\mathcal{D}_t$: affine variety $\{M \in \mathbb{M}_{\ell \times m}(\mathbb{F}_q) : \mathrm{rank}(M) \leq t\}$
- $\widehat{\mathcal{D}}_t$: corresponding projective variety $\mathbb{P}(\mathcal{D}_t) \subseteq \mathbb{P}^{\ell m - 1}$

The determinantal code $\widehat{C}_{\det}(t; \ell, m)$ is the nondegenerate linear code corresponding to the projective system $\widehat{\mathcal{D}}_t \hookrightarrow \mathbb{P}^{\ell m-1}(\mathbb{F}_q)$.
It is closely related to the code $C_{\det}(t; \ell, m) := \mathrm{im}(\mathrm{Ev})$, where

$$\mathrm{Ev} : \mathbb{F}_q[X]_1 \to \mathbb{F}_q^n \quad \text{defined by} \quad \mathrm{Ev}(f) = c_f := (f(M_1), \ldots, f(M_n)),$$

where $M_1, \ldots, M_n$ is an ordering of $\mathcal{D}_t$.

Relation between $C_{\det}(t;\ell,m)$ and $\widehat{C}_{\det}(t;\ell,m)$

Proposition

Write $C = C_{\det}(t;\ell,m)$ *and* $\widehat{C} = \widehat{C}_{\det}(t;\ell,m)$. *Let* n, k, d, *and* A_i *(resp.* $\hat{n}$, $\hat{k}$, $\hat{d}$, *and* $\hat{A}_i$*) denote, respectively, the length, dimension, minimum distance and the number of codewords of weight* i *of* C *(resp.* $\widehat{C}$*). Then*

$$n = 1 + \hat{n}(q-1), \quad k = \hat{k}, \quad d = \hat{d}(q-1), \quad \text{and} \quad A_{i(q-1)} = \hat{A}_i.$$

Moreover $A_n = 0$ *and more generally,* $A_j = 0$ *for* $0 \le j \le n$ *such that* $(q-1) \nmid j$. *Furthermore, if for* $1 \le r \le k$, *we denote by* d_r *and* $A_i^{(r)}$ *(resp:* $\hat{d}_r$ *and* $\hat{A}_i^{(r)}$*) the* r^{th} *higher weight and the number of* r*-dimensional subcodes of support weight* i *of* C *(resp.* $\widehat{C}$*), then*

$$d_r = (q-1)\hat{d}_r \quad \text{and} \quad A_{i(q-1)}^{(r)} = \hat{A}_i^{(r)} \text{ for } 0 \le i \le \hat{n}.$$

Length and Dimension

The code $C_{\mathrm{det}}(t;\ell,m)$ is degenerate, whereas $\widehat{C}_{\mathrm{det}}(t;\ell,m)$ is nondegenerate. The length and dimension of these two codes are easily obtained. The former goes back at least to Landsberg (1893) who obtained a formula for n, or rather for the number $\mu_t(\ell,m)$ of matrices in $\mathbb{M}_{\ell\times m}$ of a given rank t in case q is prime.

Proposition

$\widehat{C}_{\mathrm{det}}(t;\ell,m)$ is nondegenerate of dimension $\hat{k}=\ell m$ and length

$$\hat{n}=\sum_{j=1}^{t}\hat{\mu}_j(\ell,m) \quad \textit{where} \quad \hat{\mu}_j(\ell,m)=\frac{\mu_j(\ell,m)}{q-1}$$

and where

$$\mu_j(\ell,m)=q^{\binom{j}{2}}\prod_{i=0}^{j-1}\frac{\left(q^{\ell-i}-1\right)\left(q^{m-i}-1\right)}{q^{i+1}-1}.$$

Some Examples

(i) $t = \ell = \min\{\ell, m\}$: Here $\widehat{C}_{\det}(t; \ell, m)$ is a simplex code. So

$$\hat{n} = \frac{q^{\ell m} - 1}{q - 1}, \quad \hat{k} = \ell m \quad \text{and} \quad \hat{d} = q^{\ell m - 1}.$$

(ii) $\ell = m = t + 1$: Here $\mathcal{D}_t = \mathbb{M}_{\ell \times m} \setminus \mathrm{GL}_\ell(\mathbb{F}_q)$ while $\widehat{\mathcal{D}}_t$ is the hypersurface in $\mathbb{P}^{\ell^2 - 1}$ given by $\det(X) = 0$. Thus

$$\hat{d} = \hat{n} - \max_H |\widehat{\mathcal{D}}_t \cap H|, \quad \text{where} \quad \hat{n} = |\widehat{\mathcal{D}}_t| = \frac{q^{\ell^2} - 1}{q - 1} - q^{\binom{\ell}{2}} \prod_{i=2}^{\ell} (q^i - 1)$$

The irreducible polynomial $\det(X)$, when restricted to H gives rise to a (possibly reducible) hypersurface in $\mathbb{P}(H) \simeq \mathbb{P}^{\ell^2 - 2}$ of degree $\leq \ell$. Hence by Serre's inequality (1991)

$$|\widehat{\mathcal{D}}_t \cap H| \leq \ell q^{\ell^2 - 3} + \frac{q^{\ell^2 - 3} - 1}{q - 1}.$$

Example (ii) continued

Hence we get a bound on the minimum distance of $\widehat{C}_{\det}(t;\ell,\ell)$:

$$\hat{d} \geq q^{\ell^2-1} + q^{\ell^2-2} - (\ell-1)q^{\ell^2-3} - q^{\binom{\ell}{2}} \prod_{i=2}^{\ell}(q^i - 1).$$

In the special case when $\ell = m = 2$ and $t = 1$, we find

$$|\widehat{\mathcal{D}}_t \cap H| \leq 2q + 1 \quad \text{and} \quad \hat{d} \geq q^2.$$

The Serre bound $2q + 1$ is attained if we take H to be any of the coordinate hyperplanes. Hence $d\left(\widehat{C}_{\det}(1;2,2)\right) = q^2$.

Question: Determine, in general, the minimum distance and more generally, the weight distribution as well as all the higher weights of $\widehat{C}_{\det}(t;\ell,m)$.

Weight Distribution of Determinantal Codes

Lemma

Let $f(X) = \sum_{i=1}^{\ell}\sum_{j=1}^{m} f_{ij}X_{ij} \in \mathbb{F}_q[X]_1$ *and let* $F = (f_{ij})$ *be the coefficient matrix of* f*. Then the Hamming weights of the corresponding codewords* c_f *of* $C_{\det}(t;\ell,m)$ *and* $\hat{c}_f$ *of* $\widehat{C}_{\det}(t;\ell,m)$ *depend only on* $\operatorname{rank}(F)$*. In fact,* $\mathrm{w_H}(c_f) = \mathrm{w_H}(c_{\tau_r})$ *and* $\mathrm{w_H}(\hat{c}_f) = \mathrm{w_H}(\hat{c}_{\tau_r})$*, where* $r = \operatorname{rank}(F)$ *and* $\tau_r := X_{11} + \cdots + X_{rr}$ *.*

Weight Distribution of Determinantal Codes

Lemma

Let $f(X) = \sum_{i=1}^{\ell} \sum_{j=1}^{m} f_{ij} X_{ij} \in \mathbb{F}_q[X]_1$ *and let* $F = (f_{ij})$ *be the coefficient matrix of* f*. Then the Hamming weights of the corresponding codewords* c_f *of* $C_{\det}(t; \ell, m)$ *and* $\hat{c}_f$ *of* $\widehat{C}_{\det}(t; \ell, m)$ *depend only on* $\mathrm{rank}(F)$*. In fact,* $\mathrm{w_H}(c_f) = \mathrm{w_H}(c_{\tau_r})$ *and* $\mathrm{w_H}(\hat{c}_f) = \mathrm{w_H}(\hat{c}_{\tau_r})$*, where* $r = \mathrm{rank}(F)$ *and* $\tau_r := X_{11} + \cdots + X_{rr}$ *.*

Corollary

Each of the codes $C_{\det}(t; \ell, m)$ *and* $\widehat{C}_{\det}(t; \ell, m)$ *have at most* $\ell + 1$ *distinct weights,* $w_0, w_1, \ldots, w_\ell$ *and* $\hat{w}_0, \hat{w}_1, \ldots, \hat{w}_\ell$ *respectively, given by* $w_r = \mathrm{w_H}(c_{\tau_r})$ *and* $\hat{w}_r = \mathrm{w_H}(\hat{c}_{\tau_r}) = w_r/(q-1)$ *for* $r = 0, 1, \ldots, \ell$*. Moreover, the weight enumerator polynomials* $A(Z)$ *of* $C_{\det}(t; \ell, m)$ *and* $\hat{A}(Z)$ *of* $\widehat{C}_{\det}(t; \ell, m)$ *are given by*

$$A(Z) = \sum_{r=0}^{\ell} \mu_r(\ell, m) Z^{w_r} \quad \text{and} \quad \hat{A}(Z) = \sum_{r=0}^{\ell} \mu_r(\ell, m) Z^{\hat{w}_r},$$

Remark on a related work of Delsarte

The weight distribution or the spectrum is completely determined once we solve the combinatorial problem of counting the number of $\ell \times m$ matrices M over $\mathbb{F}_q$ of rank $\leq t$ for which $\tau_r(M) \neq 0$. Delsarte (1978), using an explicit determination of the characters of the Schur ring of an association scheme corresponding to bilinear forms, solved an essentially equivalent problem of determining the number $N_t(r)$ of $M \in \mathbb{M}_{\ell\times m}(\mathbb{F}_q)$ of rank t with $\tau_r(M) \neq 0$, and showed that $N_t(r)$ is equal to

$$\frac{(q-1)}{q}\left(\mu_t(\ell,m) - \sum_{i=0}^{\ell}(-1)^{t-i} q^{im+\binom{t-i}{2}} \begin{bmatrix} m-i \\ m-t \end{bmatrix}_q \begin{bmatrix} m-r \\ i \end{bmatrix}_q\right),.$$

Consequently, the nonzero weights of $C_{\det}(t;\ell,m)$ are given by $w_r = \sum_{s=1}^{t} N_s(r)$ for $r = 1,\ldots,\ell$. However, for a fixed t (even in the simple case $t=1$), it is not entirely obvious how $w_1,\ldots,w_\ell$ are ordered and which among them is the least.

Case of 2×2 minors

Using an elementary approach, we obtain rather easily the complete weight distribution of determinantal codes in the case $t = 1$:

Theorem

The nonzero weights of $\widehat{C}_{\det}(1; \ell, m)$ are $\hat{w}_1, \ldots, \hat{w}_\ell$, given by

$$\hat{w}_r = \mathrm{w_H}(\hat{c}_{\tau_r}) = q^{\ell+m-2} + q^{\ell+m-3} + \cdots + q^{\ell+m-r-1}$$

for $r = 1, \ldots, \ell$. In particular, $\hat{w}_1 < \hat{w}_2 < \cdots < \hat{w}_\ell$ and the minimum distance of $\widehat{C}_{\det}(1; \ell, m)$ is $q^{\ell+m-2}$.

Remark: The exponent $\ell + m - 2$ of q in the minimum distance $\widehat{C}_{\det}(1; \ell, m)$ is precisely the dimension of the determinantal variety $\widehat{\mathcal{D}}_t$ when $t = 1$. Also, the relative distance $\delta = d/n$ of $\widehat{C}_{\det}(1; \ell, m)$ is asymptotically equal to 1 as $q \to \infty$. On the other hand, the rate $R = k/n$ is quite small as $q \to \infty$, but it tends to 1 as $q \to 1$.

Determination of higher weights of Determinantal Codes

The first m of higher weights of $\widehat{C}_{\det}(1;\ell,m)$ can be found and these meet the Griesmer-Wei bound.

Theorem

For $r = 1, \ldots, m$, the r^{th} higher weight $\hat{d}_r$ of $\widehat{C}_{\det}(1;\ell,m)$ meets the Griesmer-Wei bound and is given by

$$\hat{d}_r = q^{\ell+m-2} + q^{\ell+m-3} + \cdots + q^{\ell+m-r-1} = q^{\ell+m-r-1}\frac{(q^r-1)}{q-1}.$$

In particular, if $r \le \ell$ and $\hat{w}_r$ is as in Theorem 3, then $\hat{d}_r = \hat{w}_r$.

Note that the phenonmenon $d_r = w_r$ for several values of r is rather special; it is observed in the (trivial) examples of :
(i) MDS codes, and (ii) simplex codes.

Continuing with the case $t = 1$, we can obtain lower and upper bounds for some of the subsequent weights.

Lemma

Assume that $\ell \geq 2$. *Then for* $s = 1, \ldots, \ell - 1$, *the* $(m+s)^{\mathrm{th}}$ *higher weight* $\hat{d}_{m+s}$ *of* $\widehat{C}_{\det}(1; \ell, m)$ *satisfies*

$$\hat{d}_{m+s} \geq q^{\ell-s-1} \frac{(q^{m+s} - 1)}{q-1} = \hat{d}_m + q^{\ell-s-1} \frac{(q^s - 1)}{q-1}$$

and

$$\hat{d}_{m+s} \leq \hat{d}_m + q^{\ell+m-s-2} \frac{(q^s - 1)}{q-1},$$

where $\hat{d}_m$ *is as in Theorem 4. In particular,*

$$\hat{d}_m + q^{\ell-2} \leq \hat{d}_{m+1} \leq \hat{d}_m + q^{\ell+m-3}.$$

Pushing things one step further

The Griesmer-Wei bound is not attained by $\hat{d}_r$ if $r > m$ and more work is needed to determine it.

Theorem

Assume that $\ell \geq 2$. For $1 \leq r \leq \ell m$, let $\hat{d}_r$ denote the r^{th} higher weight of $\widehat{C}_{\text{det}}(1; \ell, m)$. Then for $r = m+1, \ldots, \ell m$,

$$\begin{aligned} \hat{d}_r &\geq q^{\ell+m-r-1}\left(\frac{q^r - 1}{q-1} + q^{r-2} - 1\right) \\ &= \hat{d}_m + q^{\ell+m-r-1}\left(\frac{q^{r-m} - 1}{q-1} + q^{r-2} - 1\right), \end{aligned}$$

Moreover, equality holds when $r = m+1$ so that

$$\hat{d}_{m+1} = \hat{d}_m + q^{\ell+m-3}.$$

Idea of Proof

To optimize subspaces of with the least support weight, one has to construct subspaces of $\mathbb{F}_q[X]_1$ whose set of coefficient matrices contain as many rank 1 matrices in them as possible. In general, sums of rank 1 matrices doesn't have rank 1. Still we can ask:

Question: Can there be linear subspaces of $\mathbb{M}_{\ell \times m}$ all of whose nonzero members have rank 1? If so, what is the maximum possible dimension of such a subspace?

Idea of Proof

To optimize subspaces of with the least support weight, one has to construct subspaces of $\mathbb{F}_q[X]_1$ whose set of coefficient matrices contain as many rank 1 matrices in them as possible. In general, sums of rank 1 matrices doesn't have rank 1. Still we can ask:

Question: Can there be linear subspaces of $\mathbb{M}_{\ell\times m}$ all of whose nonzero members have rank 1? If so, what is the maximum possible dimension of such a subspace?

Theorem

Let $\mathbb{F}_q$ be a field and let $\mathcal{E}$ be a subspace of $\mathbb{M}_{\ell\times m}(\mathbb{F}_q)$ such that $\mathrm{rank}(M) = 1$ for all nonzero $M \in \mathcal{E}$. Then the structure of $\mathcal{E}$ can be explicitly described and in particular,

$$\dim \mathcal{E} \leq \max\{\ell, m\} = m.$$

Idea of Proof Contd.

Going forward we try to maximize the presence of rank 1 matrices in a subspace using the following:

Lemma

Let $\mathcal{D}$ be an r-dimensional subspace of $\mathbb{M}_{\ell\times m}(\mathbb{F}_q)$ with $r > m$. Then $\mathcal{D}$ contains at most $q^{r-1} + q^2 - q - 1$ matrices of rank 1. Consequently, $\mathcal{D}$ has at least $\left(q^{r-1} - q\right)(q-1)$ matrices of rank ≥ 2.

This will lead to one of the inequalities stated earlier for $\hat{d}_r$ of $\widehat{C}_{\det}(1;\ell,m)$. For the other inequality, one has to use an explicit construction of a "good" subspace.

Remark: In a continuation of this work, we (= Beelen and Ghorpade) have determined the minimum distance as well as the complete weight distribution of $\widehat{C}_{\det}(t;\ell,m)$ for an arbitrary t. The details will appear elsewhere.

Thank you!