Discrete Mathematics 338 (2015) 1493–1500

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Linear codes associated to determinantal varieties☆

Peter Beelen [a], Sudhir R. Ghorpade [b,*], Sartaj Ul Hasan [c]

[a] Department of Applied Mathematics and Computer Science, Technical University of Denmark, DK 2800, Kgs. Lyngby, Denmark
[b] Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India
[c] Scientific Analysis Group, Defence Research and Development Organisation, Metcalfe House, Delhi 110054, India

ARTICLE INFO

Article history:
Received 14 September 2014
Received in revised form 19 January 2015
Accepted 5 March 2015
Available online 6 April 2015

Keywords:
Linear codes
Determinantal varieties
Generalized Hamming weight
Weight distribution

ABSTRACT

We consider a class of linear codes associated to projective algebraic varieties defined by the vanishing of minors of a fixed size of a generic matrix. It is seen that the resulting code has only a small number of distinct weights. The case of varieties defined by the vanishing of 2×2 minors is considered in some detail. Here we obtain the complete weight distribution. Moreover, several generalized Hamming weights are determined explicitly and it is shown that the first few of them coincide with the distinct nonzero weights. One of the tools used is to determine the maximum possible number of matrices of rank 1 in a linear space of matrices of a given dimension over a finite field. In particular, we determine the structure and the maximum possible dimension of linear spaces of matrices in which every nonzero matrix has rank 1.

1. Introduction

A useful and interesting way to construct a linear code is to consider a projective algebraic variety V defined over the finite field $\mathbb{F}_q$ with q elements together with a nondegenerate embedding in a projective space, and to look at the projective system (in the sense of Tsfasman and Vlăduţ [12]) associated to the $\mathbb{F}_q$-rational points of V. A good illustration is provided by the case of Grassmann codes and Schubert codes, which have been of much interest; see, for example, [10,5,6,14] or the survey [9]. In this paper we consider a class of linear codes that are associated to classical determinantal varieties. These will be referred to as determinantal codes. The length and dimension of these codes are easy to determine and also one can readily show that they are nondegenerate. We shall then focus on the question of determining the minimum distance and more generally, the complete weight distribution, and also the generalized Hamming weights of determinantal codes. From a geometric viewpoint, this corresponds to determining the number of $\mathbb{F}_q$-rational points in all possible hyperplane sections and also in maximal linear sections of determinantal varieties. We give a general description of all the weights of determinantal codes and then analyze in greater detail the codes associated to the variety defined by the vanishing of all 2×2 minors of a generic $\ell \times m$ matrix. It is seen in this case that the codes exhibit a curious phenomenon that there are exactly ℓ nonzero weights and these coincide with the first ℓ generalized Hamming weights which happen to meet the Griesmer–Wei bound. This phenomenon is exhibited by $[n, k]_q$-MDS codes (for instance, the Reed–Solomon codes), which have exactly k

☆ P. Beelen gratefully acknowledges the support from the Danish National Research Foundation and the National Science Foundation of China for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography (Grant No. 11061130539). S.R. Ghorpade gratefully acknowledges the support from the Indo-Russian project INT/RFBR/P-114 from the Department of Science & Technology, Govt. of India and the IRCC Award grant 12IRAWD009 from IIT Bombay.

* Corresponding author.
E-mail addresses: pabe@dtu.dk (P. Beelen), srg@math.iitb.ac.in (S.R. Ghorpade), sartajulhasan@gmail.com (S.U. Hasan).

http://dx.doi.org/10.1016/j.disc.2015.03.009
0012-365X/

nonzero weights and k generalized Hamming weights given by $n-k+1, n-k+2, \ldots, n$. Another trivial example is that of the simplex code (i.e., the dual of Hamming code) which has only one nonzero weight and it evidently coincides with the first generalized Hamming weight. However, we do not know any other nontrivial examples and determinantal codes appear to be interesting in this regard. Unlike simplex codes, determining *all* generalized Hamming weights of determinantal codes seems difficult but we make some partial progress here.

It turns out (although we were not initially aware of it) that codes analogous to determinantal codes were considered in a different context by Camion [1] and Delsarte [2] who consider codes derived from bilinear forms. In effect, Delsarte obtains the weight distribution of these codes using an explicit determination of the characters of the Schur ring of an association scheme corresponding to these bilinear forms (see end of Section 3 for more details). Our approach, however, is entirely different and may be of some interest. Further, results concerning generalized Hamming weights appear to be new. The auxiliary results used in finding the generalized Hamming weights were alluded to in the abstract, and these (namely, Corollary 2 and Lemma 4) may also be of some independent interest.

This work has been presented at the Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-XIV) held at Kaliningrad, Russia during September 2014, and an extended abstract containing statements of results appears in the informal proceedings of ACCT-XIV.

2. Preliminaries

Fix throughout this paper a prime power q, positive integers t, ℓ, m, and a $\ell \times m$ matrix $X = (X_{ij})$ whose entries are independent indeterminates over $\mathbb{F}_q$. We will denote by $\mathbb{F}_q[X]$ the polynomial ring in the ℓm variables X_{ij} ($1 \le i \le \ell$, $1 \le j \le m$) with coefficients in $\mathbb{F}_q$. As usual, by a *minor* of size t or a $t \times t$ minor of X we mean the determinant of a $t \times t$ submatrix of X, where t is a nonnegative integer $\le \min\{\ell, m\}$. As per standard conventions, the only 0×0 minor of X is 1. We will be mostly interested in the class of minors of a fixed size, and this class is unchanged if X is replaced by its transpose. With this in view, we shall always assume, without loss of generality, that $\ell \le m$. Given a field $\mathbb{F}$, we denote by $\mathbb{M}_{\ell\times m}(\mathbb{F})$ the set of all $\ell \times m$ matrices with entries in $\mathbb{F}$. Often $\mathbb{F} = \mathbb{F}_q$ and in this case we may simply write $\mathbb{M}_{\ell\times m}$ for $\mathbb{M}_{\ell\times m}(\mathbb{F}_q)$. Note that $\mathbb{M}_{\ell\times m}$ can be viewed as an affine space $\mathbb{A}^{\ell m}$ over $\mathbb{F}_q$ of dimension ℓm. For $0 \le t \le \ell$, the corresponding classical determinantal variety (over $\mathbb{F}_q$) is denoted by $\mathcal{D}_t$ and defined as the affine algebraic variety in $\mathbb{A}^{\ell m}$ given by the vanishing of all $(t+1) \times (t+1)$ minors of X; in other words

$$\mathcal{D}_t = \left\{ M \in \mathbb{M}_{\ell\times m}(\mathbb{F}_q) : \operatorname{rank}(M) \le t \right\}.$$

The affine variety $\mathcal{D}_t$ is, in fact, a cone; in other words, the vanishing ideal $\mathcal{I}_{t+1}$ (which is precisely the ideal of $\mathbb{F}_q[X]$ generated by all $(t+1) \times (t+1)$ minors of X) is a homogeneous ideal. Also it is a classical (and nontrivial) fact that $\mathcal{I}_{t+1}$ is a prime ideal (see, e.g., [3]). Thus $\mathcal{D}_t$ can also be viewed as a projective algebraic variety in $\mathbb{P}^{\ell m-1}$, and viewed this way, we will denote it by $\widehat{\mathcal{D}}_t$. We remark that the dimension of $\widehat{\mathcal{D}}_t$ (or rather of the corresponding projective variety over the algebraic closure of $\mathbb{F}_q$) is $t(\ell+m-t)-1$ (cf. [3]). Briefly put, the determinantal code $\widehat{C}_{\det}(t; \ell, m)$ is the linear code corresponding to the projective system $\widehat{\mathcal{D}}_t \hookrightarrow \mathbb{P}^{\ell m-1}(\mathbb{F}_q) = \mathbb{P}(\mathbb{M}_{\ell\times m})$. An essentially equivalent way to obtain this code is to consider the image $C_{\det}(t; \ell, m)$ of the evaluation map

$$\operatorname{Ev} : \mathbb{F}_q[X]_1 \to \mathbb{F}_q^n \quad \text{defined by } \operatorname{Ev}(f) = c_f := (f(M_1), \ldots, f(M_n)), \tag{1}$$

where $\mathbb{F}_q[X]_1$ denotes the space of homogeneous polynomials in $\mathbb{F}_q[X]$ of degree 1 together with the zero polynomial, and $M_1, \ldots, M_n$ is an ordering of $\mathcal{D}_t$.

Recall that in general for a linear code C of length n, i.e., for a linear subspace C of $\mathbb{F}_q^n$, the *Hamming weight* of a codeword $c = (c_1, \ldots, c_n)$, denoted $\mathrm{w_H}(c)$, and the *support weight* of any $D \subseteq C$, denoted $\|D\|$, are defined by

$$\mathrm{w_H}(c) := |\{i : c_i \ne 0\}| \quad \text{and} \quad \|D\| := |\{i : \text{there exists } c \in D \text{ with } c_i \ne 0\}|,$$

where for a finite set S, by $|S|$ we denote the cardinality of S. The minimum distance of C, denoted $d(C)$, and more generally, the rth *higher weight* or the rth *generalized Hamming weight* of C, denoted $d_r(C)$, are defined by

$$d(C) := \min\{\mathrm{w_H}(c) : c \in C,\ c \ne 0\} \text{ and for } r = 1, \ldots, k, \quad d_r(C) := \min\{\|D\| : D \text{ is a subcode of } C \text{ with } \dim D = r\}.$$

The parameters of $C_{\det}(t; \ell, m)$ determine those of $\widehat{C}_{\det}(t; \ell, m)$ and vice-versa. More precisely, we have the following.

Proposition 1. *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*

$$n = 1 + \hat{n}(q-1), \quad k = \hat{k}, \quad d = \hat{d}(q-1), \quad \text{and} \quad A_{i(q-1)} = \hat{A}_i \text{ for } 0 \le i \le \hat{n}.$$

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 rth higher weight and the number of r-dimensional subcodes of support weight i of C (resp. $\widehat{C}$), then $d_r = (q-1)\hat{d}_r$ and $A_{i(q-1)}^{(r)} = \hat{A}_i^{(r)}$ for $0 \le i \le \hat{n}$.