Des. Codes Cryptogr.
DOI 10.1007/s10623-012-9613-6

Families of twisted tensor product codes

Luca Giuzzi · Valentina Pepe

Received: 6 July 2011 / Revised: 14 December 2011 / Accepted: 14 January 2012

Abstract Using geometric properties of the variety $\mathcal{V}_{r,t}$, the image under the Grassmannian map of a Desarguesian $(t-1)$-spread of PG $(rt-1, q)$, we introduce error correcting codes related to the twisted tensor product construction, producing several families of constacyclic codes. We determine the precise parameters of these codes and characterise the words of minimum weight.

Keywords Segre product · Veronesean · Grassmannian · Desarguesian spread · Subgeometry · Twisted product · Constacyclic error correcting code · Minimum weight

Mathematics Subject Classification (2010) 94B05 · 94B27 · 15A69 · 51E20

1 Introduction

Linear codes provide a simple, yet powerful, method to add redundancy to a message in order to provide protection against transmission errors. For a general reference on coding theory, including standard notations, see [15]. As customary, we regard a q-ary linear code $\mathcal{C}$ with parameters $[n, k, d]$ as a subspace of dimension k of $\mathbb{F}_q^n$ whose non-zero vectors have Hamming weight at least d. Recall that the correction capacity of a code, at least on a first

Communicated by G. Lunardon.

L. Giuzzi—Part of this research has been performed while a guest of the Department of Mathematics of Ghent University.

L. Giuzzi
Department of Mathematics, Facoltà di Ingegneria, Università degli Studi di Brescia,
Via Valotti 9, Brescia 25133, Italy
e-mail: giuzzi@ing.unibs.it

V. Pepe (✉)
Department of Mathematics, Universiteit Gent, Building S22, Krijgslaan 281, Gent 9000, Belgium
e-mail: valepepe@cage.ugent.be

Published online: 08 February 2012

approximation, depends on its minimum distance d. Indeed, the most probable undetected errors are exactly those corresponding to words of minimum weight; thus, it is in practice quite important to be able to count and characterise such words. In general, the complexity of implementation of a code is tied to the size q of the field under consideration. This is one of the reasons why some of the most widely used codes are actually defined over the binary field $\mathbb{F}_2$, even if some of the actual computations involved in the correction procedure are performed over algebraic extensions, as in the case of the BCH construction. On the other hand, some recent applications warrant for the use of non-binary codes in a 'natural way', as, in order to increase the storage density of data, addressable units larger than a single bit are often selected.

A code $\mathcal{C}$ might be determined by either a *generator matrix* G, a matrix whose rows constitute a basis for the subspace $\mathcal{C}$ of $\mathbb{F}_q^n$, or, dually, a *parity check matrix* H, that is a matrix providing a basis for the annihilator of $\mathcal{C}$ in ${\mathbb{F}_q^n}^{\perp}$.

In this article we shall adopt the latter approach; in particular, the code $\mathcal{C}$ is the kernel of the linear application induced by H.

The link between incidence structures and coding theory has been very fruitful. Possibly, it has been first pointed out in [16]; for a reference on the development of the topic and some of the related problems we refer to the book [1]. Codes derived from geometries have proven themselves to be interesting for several reasons, not least the possibility of providing synthetic constructions and their usually large automorphism group.

In this article we shall study some codes related to the Segre embedding and twisted tensor products; see [2,6]. Our constructions generalise and strengthen some of the results of [2], albeit using different techniques. In Sect. 2 we shall recall some properties of the algebraic variety $\mathcal{V}_{r,t}$ and prove that any $t+1$ of its points are in general position. In Sect. 3, using these results, some new families of codes $\mathcal{C}_{r,t}$ will be introduced. We will determine their parameters and also characterise the words of minimum weight. All of these codes admit a large subgroup of monomial automorphisms, isomorphic to $\mathrm{P\Gamma L}(r, q^t)$ and they are always constacyclic in the sense of [3]. We shall also investigate some subcodes and show that by puncturing in a suitable way it is possible to obtain cyclic codes.

2 The variety $\mathcal{V}_{r,t}$ and twisted tensor products

Let $\mathrm{PG}(V, \mathbb{F})$ be the projective space defined by the lattice of subspaces of the vector space V over the field $\mathbb{F}$ and write $\mathrm{PG}(n-1, q) := \mathrm{PG}(V, \mathbb{F}_q)$, where $\dim_{\mathbb{F}_q} V = n$. Take $\mathrm{PG}(r_1-1, q), \mathrm{PG}(r_2-1, q), \ldots, \mathrm{PG}(r_t-1, q)$ to be t distinct projective spaces; the *Segre embedding*

$$\sigma : \mathrm{PG}(r_1-1, q) \times \mathrm{PG}(r_2-1, q) \times \cdots \times \mathrm{PG}(r_t-1, q) \longrightarrow \mathrm{PG}(r_1 r_2 \cdots r_t - 1, q)$$

is the map such that $\sigma(\mathbf{x}^1, \ldots, \mathbf{x}^t)$ is the vector of all the possible products $x_{j_1}^{(1)} x_{j_2}^{(2)} \cdots x_{j_t}^{(t)}$, as $\mathbf{x}^i = (x_0^{(i)}, x_1^{(i)}, \cdots, x_{r_i-1}^{(i)})$ varies in $\mathrm{PG}(r_i-1, q)$. The image of σ is the *Segre variety* $\Sigma_{r_1;r_2;\ldots;r_t}$: it can be regarded, in some way, as a product of projective spaces; see [11, Chap. 25], [9, Chap. 9] and [8, Chap. 2]. In the language of tensor products, σ is the natural *morphism* between the varieties

$$\mathrm{PG}(V_1, q) \times \mathrm{PG}(V_2, q) \times \cdots \times \mathrm{PG}(V_t, q) \longrightarrow \mathrm{PG}(V_1 \otimes V_2 \otimes \cdots \otimes V_t, q).$$

In this article, we are interested in the case $r_1 = r_2 = \ldots = r_t = r$; for brevity we shall write Σ_{r^t} instead of $\Sigma_{r_1;r_2;\ldots;r_t}$. Clearly, $\Sigma_{r^t} \subseteq \mathrm{PG}(r^t - 1, q)$.

The *Veronese variety* $\mathcal{V}(n,d)$ is an algebraic variety of PG $\left(\binom{n+d}{d}-1,q\right)$, image of the injective map

$$v_{n,d}:\mathrm{PG}\,(n,q)\longrightarrow\mathrm{PG}\left(\binom{n+d}{d}-1,q\right),$$

where $v_{n,d}(x_0,x_1,\ldots,x_n)$ is the vector of all the monomials of degree d in $x_0,\ldots,x_n$; for $d=2$, see [11, Chap. 25]; for general d, see [8, Chaps. 2,9] and also [5]. It is useful to remember that $\mathcal{V}(1,d)$ is a *normal rational curve* of PG (d,q) and any $d+1$ of its points happen to be in general position. The Veronese variety $\mathcal{V}(r,t)$ and Σ_{r^t} are closely related, in the sense that $\mathcal{V}(r,t)$ is the image under σ of the *diagonal* of PG $(r-1,q)\times\mathrm{PG}\,(r-1,q)\times\cdots\times\mathrm{PG}\,(r-1,q)$.

Consider now the projective space PG $(r-1,q^t)$ and let $v\longmapsto v^q$ be the $\mathbb{F}_q$–linear collineation of order t induced by the Frobenius automorphism of the extension $[\mathbb{F}_{q^t}:\mathbb{F}_q]$. For any $P\in\mathrm{PG}\,(r-1,q^t)$, write

$$P^\alpha=\sigma\left(\left[P,P^q,\ldots,P^{q^{t-1}}\right]\right).$$

The image of this correspondence is the variety $\mathcal{V}_{r,t}$. It is immediate to see that the $\mathbb{F}_q$–linear collineation of order t given by

$$(p_0\otimes p_1\otimes\cdots\otimes p_{t-1})\longmapsto\left(p_{t-1}^q\otimes p_0^q\otimes\cdots\otimes p_{t-2}^q\right)$$

fixes $\mathcal{V}_{r,t}$ point-wise; hence, $\mathcal{V}_{r,t}$ is contained in a subgeometry $\Omega=\mathrm{PG}\,(r^t-1,q)$ of PG (r^t-1,q^t). It turns out that $\mathcal{V}_{r,t}$ is, in fact, the complete intersection of the Segre product Σ_{r^t} with Ω.

As an algebraic variety $\mathcal{V}_{r,t}$ first appeared in [19]; it has then been described in [14] and therein extensively studied. Recently, in [17], an explicit parametrisation for $\mathcal{V}_{r,t}$ has been determined, leading to the discovery of some new properties. It is convenient to recall here this parametrisation. Take $\mathfrak{F}=\{f:\{0,\ldots,t-1\}\to\{0,\ldots,r-1\}\}$ and write $P=(x_0,\ldots,x_{r-1})\in\mathrm{PG}\,(r-1,q^t)$. Then, there is an injective map $\alpha:\mathrm{PG}\,(r-1,q^t)\to\mathcal{V}_{r,t}\subseteq\mathrm{PG}\,(r^t-1,q^t)$ sending any $P\in\mathrm{PG}\,(r-1,q^t)$ to the point $P^\alpha\in\mathrm{PG}\,(r^t-1,q^t)$ whose coordinates consist of all products of the form

$$\prod_{i=0}^{t-1}x_{f(i)}^{q^i}$$

as f varies in $\mathfrak{F}$.

There is a strong affinity between the Veronese variety and $\mathcal{V}_{r,t}$: take $\psi\in\mathrm{P\Gamma L}\,(r,q^t)$ so that $\psi^t=id$ and let $\mathcal{V}$ be the image under σ of the elements of type $(v,v^\psi,\ldots,v^{\psi^{t-1}})$; clearly $\mathcal{V}$ is a variety; furthermore, when $\psi=id$, then $\mathcal{V}=\Sigma_{r^t}\cap\mathrm{PG}\left(\binom{r-1+t}{t}-1,q^t\right)$ is a Veronese variety; if, on the contrary, ψ is a $\mathbb{F}_q$-linear collineation of order t, ultimately determining a subgeometry $\Omega=\mathrm{PG}\,(r^t-1,q)$, then $\mathcal{V}=\Sigma_{r^t}\cap\Omega$ and $\mathcal{V}=\mathcal{V}_{r,t}$.

We shall also make use of the alternative description of $\mathcal{V}_{r,t}$ from [14]. A *Desarguesian* (also called *normal*) *spread* of PG $(rt-1,q)$ is projectively equivalent to a linear representation of PG $(r-1,q^t)$ in PG $(rt-1,q)$; see [19]. As such, it consists of a collection $\mathcal{S}$ of $(t-1)$-dimensional subspaces of PG $(rt-1,q)$, each of them the linear representation of a point of PG $(r-1,q^t)$, partitioning the point set of PG $(rt-1,q)$. When regarded on the Grassmannian of all the $(t-1)$-dimensional subspaces of PG $(rt-1,q)$, the elements of $\mathcal{S}$ determine the algebraic variety $\mathcal{V}_{r,t}$. The best known example is for $r=t=2$: indeed,

the Grassmannian of the lines of a Desarguesian spread of PG$(3, q)$ is an elliptic quadric $\mathcal{V}_{2,2} = \mathcal{Q}^-(3, q)$; see, for instance, [10, Sect. 15.4].

More in general, if $\Pi_P \in \mathcal{S}$ is the linear representation of a point $P \in$ PG$(r-1, q^t)$, then the image under the Grassmann map of Π_P is P^α. Using this correspondence, it has been possible to investigate several properties of $\mathcal{V}_{r,t}$; see [13,14,17]. Here we will recall just some of them. As the group PΓL(r, q^t) preserves a Desarguesian $(t-1)$-spread $\mathcal{S}$ of PG$(rt-1, q)$, its lifting preserves $\mathcal{V}_{r,t}$ and its action on the points of $\mathcal{V}_{r,t}$ is isomorphic to the 2-transitive action of PΓL(r, q^t) on the elements of $\mathcal{S}$; see [14]. We remark that the aforementioned action is actually 3-transitive for $r = 2$.

The group $G =$ PGL(r, q^t) acts in a natural way on $M =$ PG$(r-1, q^t)$, which is both a G–module and an $\mathbb{F}_{q^t}$-vector space. The *twisted tensor product* has been introduced in [21] to realise a new G-module, say M', defined over the subfield $\mathbb{F}_q$ from M; this induces a straightforward embedding of PGL(r, q^t) in PGL(r^t, q).

We briefly recall the construction. Write the action of G on M as $g \cdot P \to gP$, where $g \in G$ and $P \in M$. For any automorphism ϕ of $\mathbb{F}_{q^t}$, we can define a new G-module M^ϕ with group action $g \cdot P \to g^\phi P$; when ϕ is the automorphism $g \to g^{q^i}$, we shall write $M^\phi = M^{q^i}$. Using this notation, the twisted tensor product of M over $\mathbb{F}_q$ is

$$M' = M \otimes M^q \otimes \cdots \otimes M^{q^{t-1}}.$$

If we restrict our attention to the points of $\mathcal{V}_{r,t}$, we see that for any $g \in G$ and $P \in$ PG$(r-1, q^t)$

$$(gP)^\alpha = \sigma\left(\left[gP, g^q P^q, \ldots, g^{q^{t-1}} P^{q^{t-1}}\right]\right) = g\sigma\left(\left[P, P^q, \ldots, P^{q^{t-1}}\right]\right) = gP^\alpha.$$

This is to say that PGL(r, q^t), as embedded in PGL(r^t, q), stabilises $\mathcal{V}_{r,t}$ and its action on the points of the variety is the same as on those of PG$(r-1, q^t)$. For this reason, we can consider $\mathcal{V}_{r,t}$ as a geometric realisation of PG$(r-1, q^t)$ in the twisted tensor product; in brief we shall call it the *twisted tensor embedding* over $\mathbb{F}_q$ of PG$(r-1, q^t)$. In close analogy, the image under α of a subgeometry PG$(r-1, q^s)$ of PG$(r-1, q^t)$, where $s|t$, is the twisted tensor embedding of the Veronese variety $\mathcal{V}(r-1, \frac{t}{s})$ defined on the field $\mathbb{F}_{q^s}$; this turns out to be the complete intersection of $\mathcal{V}_{r,t}$ with a suitable PG $\left(\binom{r-1+\frac{t}{s}}{\frac{t}{s}}^s - 1, q\right)$; in particular, for $s = 1$, we get a Veronese variety $\mathcal{V}(r-1, t)$ defined on $\mathbb{F}_q$; see [14] for $s = 1$ and $r = 2$ and [17] for the general case.

The set $\mathcal{R} = \{\Pi_P | P \in$ PG$(r-1, q)\}$ is a *regulus*. There are several equivalent descriptions for such a collection of spaces contained in a Desarguesian spread; for our purposes, the most useful is the following: suppose Σ to be a $(r-1)$-subspace of PG$(rt-1, q)$ such that Σ intersects every element of $\mathcal{S}$ in at most one point; then, the elements of $\mathcal{S}$ with non-empty intersection with Σ form a regulus $\mathcal{R}$.

As mentioned before, any $t+1$ points of the normal rational curve $\mathcal{V}(1, t)$ are in general position, that is they span a t-dimensional projective space; in [17] it is proved that also any $t+1$ points of $\mathcal{V}_{2,t}$ are in general position. Recently, Kantor [12] has announced a proof of the same property for the Veronesean $\mathcal{V}(r-1, t)$ with arbitrary r. Using a suitable adaptation of the arguments he proposed it is possible to generalise the result of [17] to $\mathcal{V}_{r,t}$ for any r. To this aim, first we prove a suitably adapted version of a result in [12].

Theorem 2.1 *Let* $\Pi_0, \Pi_1, \ldots, \Pi_{t-1}$ *be subspaces of* PG$(r-1, q^t)$ *and suppose that* $P \in$ PG$(r-1, q^t)$ *is not contained in any of them. Then,* P^α *is not contained in* $\langle \Pi_0^\alpha, \Pi_1^\alpha, \ldots, \Pi_{t-1}^\alpha \rangle$.

Proof For each $i = 0, \ldots, t-1$, consider a linear map ℓ_i vanishing on Π_i but not in P. That is to say that $\ell_i = 0$ is the equation of a hyperplane of PG $(r-1, q^t)$ containing the subspace Π_i but not the point P. Clearly, for $\ell_i = \sum_{j=0}^{r-1} a_{ij} x_j$, we have $\ell_i^q = \sum_{j=0}^{r-1} a_{ij}^q x_j^q$. Let

$$L = \prod_{i=0}^{t-1} \ell_i^{q^{i-1}}.$$

By construction, L vanishes on $\Pi_0, \Pi_1, \ldots, \Pi_{t-1}$ but not in P. By the parametrisation of $\mathcal{V}_{r,t}$ of [17], L evaluated on Π_i is the same as a $\mathbb{F}_{q^t}$-linear function evaluated on $\Pi_i^\alpha \subset \mathcal{V}_{r,t}$; hence, there exists a hyperplane Λ of PG $(r^t - 1, q^t)$ containing $\langle \Pi_i^\alpha : i = 0, 1, \ldots, t-1 \rangle$ but not P^α. It is well known that any hyperplane of PG $(r^t - 1, q^t)$ intersects a subgeometry PG $(r^t - 1, q)$ in a (possibly empty) subspace. This completes the proof. □

The case in which all of the subspaces reduce to a single projective point is of special interest for the geometry.

Corollary 2.2 *Any $t+1$ points of $\mathcal{V}_{r,t}$ are in general position.*

Corollary 2.3 *Suppose $q > t$. Any set of $t+2$ dependent points of $\mathcal{V}_{r,t}$ is contained in the image under α of a subline* PG $(1, q) \subset$ PG $(r-1, q^t)$.

Proof Take $t+2$ distinct points $P_0, P_1, \ldots, P_t, P$ forming a dependent system, and let

$$\Pi_i := P_i, \text{ for } i = 0, \ldots, t-2, \qquad \Pi_{t-1} = \langle P_{t-1}, P_t \rangle.$$

If it were $P \notin \Pi_{t-1}$, then, by Theorem 2.1, $P^\alpha \notin \langle P_0^\alpha, P_1^\alpha, \ldots, \Pi_{t-1}^\alpha \rangle$. However, by hypothesis, $P^\alpha \in \langle P_0^\alpha, P_1^\alpha, \ldots, P_{t-1}^\alpha, P_t^\alpha \rangle$ and $\langle P_0^\alpha, P_1^\alpha, \ldots, P_{t-2}^\alpha, P_{t-1}^\alpha, P_t^\alpha \rangle \subseteq \langle P_0^\alpha, P_1^\alpha, \ldots, \Pi_{t-1}^\alpha \rangle$—a contradiction. It follows that the $t+2$ points under consideration must all belong to the same line PG $(1, q^t) \subseteq$ PG $(r-1, q^t)$. In particular, their image is contained in a $\mathcal{V}_{2,t} \subseteq \mathcal{V}_{r,t}$. By [13, Lemma 2.5], for $t < q$, any $t+2$ linearly dependent points of $\mathcal{V}_{2,t}$ which are $t+1$ by $t+1$ independent are the image of elements of the same regulus in the Desarguesian $(t-1)$-spread of PG $(2t-1, q)$; it follows that they are contained in the image under α of the same subline PG $(1, q)$. □

3 The code $\mathcal{C}_{r,t}$ and its automorphisms

Definition 3.1 Let q be any prime power. For any two integers r, t with $t < q$, denote by $\mathcal{C}_{r,t}$ the code whose parity check matrix H has as columns the coordinate vectors of the points of the variety $\mathcal{V}_{r,t}$.

Remark 3.2 In Definition 3.1 we did not specify the field over which the code is defined. Clearly, $\mathcal{C}_{r,t}$ arises as a subspace of $\mathbb{F}_{q^t}^{r^t}$; however, by the considerations contained in the previous paragraph, it can be more conveniently regarded as defined over $\mathbb{F}_q$, up to a suitable collineation; this is what we shall do.

Remark 3.3 The order of the columns in H is arbitrary, but once chosen, it determines an order for the points of $\mathcal{V}_{r,t}$. In particular Definition 3.1 for $\mathcal{C}_{r,t}$ makes sense only up to code equivalence, as a permutation of the columns is not usually an automorphism of the code. It will be seen in the latter part of this section, however, that the most useful orders for the code $\mathcal{C}_{r,t}$ are those induced by the action of a cyclic collineation group of PG $(r-1, q^t)$—either

a Singer cycle or an affine Singer cycle. Both of these are cyclic linear collineation groups of PG $(r-1, q^t)$: a Singer cycle acts regularly on the points and the hyperplanes; an affine Singer cycle, however, has exactly 3 orbits in PG $(r-1, q^t)$: a hyperplane Σ, a single point O with $O \notin \Sigma$ and the points of $AG(r-1, q^t) = \text{PG}(r-1, q^t) \setminus \Sigma$ different from O. The action on the latter orbit is regular. For more details on this latter group, see [4,20]. This group has already turned out to be quite useful in a coding theory setting; see, for instance, [7].

In view of Remark 3.3, it is possible to give the following definition.

Definition 3.4 The *support* of a word $\mathbf{w} \in \mathcal{C}_{r,t}$ is the set of points of the variety $\mathcal{V}_{r,t}$ corresponding to the non-zero positions of $\mathbf{w}$.

In order to avoid degenerate cases, the condition $t < q$ shall always be silently assumed in the remainder of the article.

Theorem 3.5 *The code $\mathcal{C}_{r,t}$ has length $n = \frac{q^{rt}-1}{q^t-1}$ and parameters $[n, n-r^t, t+2]$.*

Proof By construction

$$n = |\mathcal{V}_{r,t}| = |\text{PG}(r-1, q^t)|.$$

As $\mathcal{V}_{r,t} \subseteq \text{PG}(r^t-1, q)$ is not contained in any hyperplane, the rank of the $r^t \times n$ matrix H is maximal and, consequently, the dimension of the code is $n - r^t$. Corollary 2.2 guarantees that any $t+1$ columns of H are linearly independent; thus, by [15, Theorem 10, p. 33], the minimum distance of $\mathcal{C}_{r,t}$ is always at least $d \geq t+2$.

The image under α of the canonical subline PG $(1, q)$ of PG $(r-1, q^t)$ determines a submatrix H' of H with many repeated rows; indeed, the points represented in H' constitute a normal rational curve contained in a subspace of dimension t; see [13, Theorem 2.16]. It follows that any $t+2$ such points are necessarily dependent. Hence, the minimum distance is exactly $t+2$. □

Remark 3.6 The code $\mathcal{C}_{2,3}$ is also constructed in [2, Theorem 2].

We now characterise the words of minimum weight in $\mathcal{C}_{r,t}$.

Theorem 3.7 *A word $\mathbf{w} \in \mathcal{C}_{r,t}$ has minimum weight if and only if its support consists of $t+2$ points contained in the image of a subline* PG $(1, q)$.

Proof By the proof of Theorem 3.5, the image of any $t+2$ points in a subline PG $(1, q)$ gives the support of a codeword of minimum weight.

Conversely, let $\mathbf{w} \in \mathcal{C}_{r,t}$ be of weight $t+2$; then, the support of $\mathbf{w}$ consists of $t+2$ dependent points of $\mathcal{V}_{r,t}$. By Corollary 2.3 these are contained in the image under α of a subline. The result follows. □

We shall now introduce a second class of codes, also a generalisation of a construction in [2].

Definition 3.8 Let q be any prime power. For any three integers r, t, s with $t < q$, $1 < s < t$ and $s|t$, denote by $\mathcal{C}^{(s)}_{r,t}$ the code whose parity check matrix K has as columns the coordinate vectors of the points of the subvariety of $\mathcal{V}_{r,t}$ image of the points of a subgeometry PG $(r-1, q^s)$, that is the twisted tensor embedding of a Veronese variety $\mathcal{V}(r-1, \frac{t}{s})$ defined over $\mathbb{F}_{q^s}$.

Remark 3.9 The matrix K is a submatrix of the matrix H.

Theorem 3.10 *Let* $m = \frac{q^{rs}-1}{q^s-1}$ *and suppose* $t < m - 1$. *Then, the code* $\mathcal{C}_{r,t}^{(s)}$ *has length* m *and parameters* $[m, m - \binom{r-1+\frac{t}{s}}{\frac{t}{s}}^s, t+2]$.

Proof By construction

$$m = |\mathrm{PG}\,(r-1, q^s)|.$$

By [17, Theorem 2], the subvariety under consideration spans a space of rank $\binom{r-1+\frac{t}{s}}{\frac{t}{s}}^s$; hence, the rank of K is $\binom{r-1+\frac{t}{s}}{\frac{t}{s}}^s$; consequently, the dimension of the code is $m - \binom{r-1+\frac{t}{s}}{\frac{t}{s}}^s$. The variety under consideration is a linear subvariety of $\mathcal{V}_{r,t}$, that is a section of $\mathcal{V}_{r,t}$ with a suitable subspace. Therefore, by Corollary 2.2, any $t+1$ of its columns are linearly independent—this shows that the minimum distance of the code is always at least $t+2$.

On the other hand, since $\mathrm{PG}\,(r-1, q^s)$ contains the points of a subline $\mathrm{PG}\,(1, q)$, there are also examples of $t+2$ columns which are linearly dependent; thus the minimum distance is exactly $t+2$. □

Remark 3.11 Both the codes $\mathcal{C}_{r,s}$ and $\mathcal{C}_{r,t}^{(s)}$ correspond to a $\mathbb{F}_q$-representation of $\mathrm{PG}\,(r-1, q^s)$; as such they have the same length. They clearly differ in their minimum distance d: $d(\mathcal{C}_{r,s}) = s+2$ and $d(\mathcal{C}_{r,t}^{(s)}) = t+2$, hence it is larger in the case of the latter code. Indeed, the construction of Theorem 3.10 might be used to produce codes over $\mathbb{F}_q$ with prescribed minimum distance and length. As a way to compare the two codes more in detail, consider the function

$$\eta(\mathcal{C}) = (d-1)/(n-k).$$

By the Singleton bound, $0 < \eta(\mathcal{C}) \leq 1$ for any code, and $\eta(\mathcal{C}) = 1$ if and only if the code is maximum distance separable (MDS). Thus, η provides an insight on the cost in redundancy per error (either detected or corrected). Under this criterion, in general, the codes $\mathcal{C}_{r,s}$ perform much better than $\mathcal{C}_{r,t}^{(s)}$. For example, consider the case $r = 3$, $s = 3$ and $t = 6$. Then, $\eta(\mathcal{C}_{3,3}) = 0.14$, while $\eta(\mathcal{C}_{3,6}^{(3)}) = 0.032$.

An automorphism of a linear code $\mathcal{C}$ is an isometric linear transformation of $\mathcal{C}$—in other words, a linear transformation of $\mathcal{C}$ preserving the weight of every word. The set of all the automorphisms of a code is a group, denoted as $\mathrm{Aut}\,\mathcal{C}$. We shall now focus on automorphisms of a restricted form.

Definition 3.12 An automorphism θ of $\mathcal{C}$ is called *monomial* if it is induced by a matrix which has exactly one non-zero entry in each row and in each column.

It is straightforward to see that any monomial transformation $\mathcal{C} \to \mathcal{C}$ is weight preserving and, thus, an automorphism; clearly, there might also be automorphisms which are not monomial.

Theorem 3.13 *Any collineation* $\gamma \in \mathrm{P\Gamma L}\,(r, q^t)$ *lifts to a monomial automorphism of* $\mathcal{C}_{r,t}$. *In particular, there is a group* $G \simeq \mathrm{P\Gamma L}\,(r, q^t)$ *such that*

$$G \leq \mathrm{Aut}\,\mathcal{C}_{r,t}.$$

Proof Let $H_0, H_1, \ldots, H_{n-1}$ be the columns of H, the parity check matrix of $\mathcal{C}_{r,t}$, and suppose $\gamma \in \mathrm{P\Gamma L}(r, q^t)$. Take $\mathbf{w} = (w_0, \ldots, w_{n-1}) \in \mathcal{C}$. As γ acts on the points of the variety $\mathcal{V}_{r,t}$ as a permutation group, there exists a permutation $\widetilde{\gamma}$ of $I = \{0, \ldots, n-1\}$ and elements $[\gamma, i] \in \mathbb{F}_q$ with $i \in I$ such that $\gamma(H_i) = [\gamma, i] H_{\widetilde{\gamma}(i)}$ as vectors; hence

$$H_i = [\gamma, \widetilde{\gamma}^{-1}(i)]^{-1} H_{\widetilde{\gamma}^{-1}(i)}.$$

In particular,

$$\mathbf{0} = \sum_i H_i w_i = \sum_i [\gamma, \widetilde{\gamma}^{-1}(i)]^{-1} H_{\widetilde{\gamma}^{-1}(i)} w_i = \sum_j H_j [\gamma, j]^{-1} w_{\widetilde{\gamma}(j)}.$$

Thus, γ induces a monomial transformation $\hat{\gamma} : \mathcal{C} \to \mathcal{C}$. □

We now focus our attention on the special case of cyclic automorphisms and constacyclic codes.

Definition 3.14 A q–ary code $\mathcal{C}$ is *constacyclic* if there exists $\beta \in \mathbb{F}_q$ such that for any $\mathbf{w} = (w_0\, w_1\, \ldots\, w_{n-1}) \in \mathcal{C}$,

$$\mathbf{w}^{\rho} := (\beta w_{n-1}\, w_0\, \ldots\, w_{n-2}) \in \mathcal{C}.$$

Constacyclic codes have been introduced in [3] as a generalisation of cyclic codes; for some of their properties see, for instance, [18]. In [2] it is shown that the codes $\mathcal{C}_{2,3}$ are constacyclic. Here, we extend the result to all $\mathcal{C}_{r,t}$.

Observe first that whenever there is a cyclic group acting regularly on the columns of the parity check matrix of a code, then the code is cyclic.

Corollary 3.15 *Let $\mathcal{C}$ be a code of length ℓ with parity check matrix H. Suppose that there is a cyclic group acting regularly on the columns of H. Then $\mathcal{C}$ is cyclic.*

Proof Let γ be the generator of the group. Under the assumptions, $[\gamma, j] = 1$ for any j. The result follows. □

Let now ω be a generator for a Singer cycle of $\mathrm{PG}(r-1, q^t)$ and order the columns $H_0, H_1, \ldots, H_{n-1}$ of the parity check matrix H so that

$$H_{i+1} = \omega(H_i), \qquad i = 0, \ldots, n-2.$$

By construction, $[\omega, i] = 1$ for $i < n-1$, while, in general, $\omega(H_{n-1}) = [\omega, n-1] H_0$ with $[\omega, n-1] \neq 1$. Thus, we have the following theorem.

Theorem 3.16 *The codes $\mathcal{C}_{r,t}$ are all constacyclic.*

Remark 3.17 The automorphism group $G = \mathrm{PGL}(r, q^s)$ of the subgeometry $\mathrm{PG}(r-1, q^s)$ acts as a permutation group on $\mathcal{V}(r-1, \frac{t}{s})$; furthermore it induces a linear collineation group of the ambient space; see [5, Theorem 2.10]. Thus, the arguments leading to Theorems 3.13 and 3.16 apply in an almost identical way to the codes $\mathcal{C}^{(s)}_{r,t}$. In particular, all of the codes $\mathcal{C}^{(s)}_{r,t}$ are equivalent to constacyclic codes and they admit a monomial automorphism group isomorphic to G.

As observed above, $\mathcal{C}_{r,t}$ is not, in general, cyclic; see also [2]. None the less, by considering the action of either the Singer cycle or the affine Singer cycle, we can always determine a smaller code which is cyclic and still related with our geometries.

We recall that *puncturing* a code $\mathcal{C}$ means deriving a new code $\mathcal{C}^*$ from $\mathcal{C}$ by deleting some of its coordinates; in general, this procedure decreases the minimum distance; see [15, p. 28].

Let $\xi_i : x_i = 0$ be a coordinate hyperplane in PG $(r-1, q^t)$; with this choice, the image under α of ξ_i is the full intersection of $\mathcal{V}_{r,t}$ with a suitable hyperplane Ξ_i of PG (r^t-1, q).

Definition 3.18 Take $O \in$ PG $(r-1, q^t)$ and suppose $O \notin \xi_i$. Write $\widetilde{\mathcal{C}}^O_{r,t,i}$ for the code obtained by puncturing $\mathcal{C}_{r,t}$ in the positions corresponding to O^α and Ξ_i.

The columns of $\widetilde{\mathcal{C}}^O_{r,t,i}$ correspond to the points of AG $(r^t-1, q)\setminus\{O\} \subseteq$ PG $(r^t-1, q)\setminus \Xi_i$.

Theorem 3.19 *The code $\widetilde{\mathcal{C}} = \widetilde{\mathcal{C}}^O_{r,t,i}$ is equivalent to a cyclic code.*

Proof Clearly, the length of $\widetilde{\mathcal{C}}$ is $m = q^{rt-t} - 1$. Write $\widetilde{H} = (\widetilde{H}_1, \ldots, \widetilde{H}_\ell)$ for its parity check matrix. Recall that the columns of $\widetilde{H}$ correspond to the points of an affine geometry $\mathfrak{A} =$ AG $(r-1, q^t)$ with a point removed. By construction, the image of $\mathfrak{A}$ under α is contained in an affine subspace AG $(r^t-1, q) =$ PG $(r^t-1, q) \setminus \Xi_i$. In particular, the affine cyclic Singer group with generator θ lifts to an affine group of AG (r^t-1, q) which acts cyclically on the columns of $\widetilde{H}$. We can assume, up to code equivalence, $\theta(\widetilde{H}_i) = H_{i+1}$ for $i < \ell$ and $\theta(\widetilde{H}_\ell) = H_0$. By Corollary 3.15, $\widetilde{\mathcal{C}}$ is cyclic. □

The matrix $\widetilde{H}$ contains the coordinates of affine points such that any $(t+1)$ of them are in general position. This is to say that any t columns of $\widetilde{H}$ are independent; thus the minimum distance of the new code is $t+1$. It is straightforward to see that $\widetilde{\mathcal{C}}$ admits a group of automorphisms isomorphic to $\Gamma\mathrm{L}\,(r-1, q^t)$.

As a special case, remark that as PGL $(2, q^t)$ acts 3-transitively on PG $(1, q^t)$, the code $\widetilde{\mathcal{C}}_{2,t}$ for $r = 2$ is the code $\mathcal{C}_{2,t}$ punctured in any two of its positions.

Acknowledgments The authors wish to thank W.M. Kantor, for having kindly shared an unpublished result which provided the insight necessary for obtaining the proof of Theorem 2.1 in the most general case. V. Pepe acknowledges the support of the project "Linear codes and cryptography" of the Fund for Scientific Research Flanders (FWO-Vlaanderen), Project No. G.0317.06, and is supported by the Interuniversitary Attraction Poles Programme, Belgian State, Belgian Science Policy: project P6/26- BCrypt.

References

1. Assmus E.F., Key J.D.: Designs and Their Codes. Cambridge University Press, Cambridge (1992).
2. Betten A.: Twisted tensor product codes. Des. Codes Cryptogr. **47**(1–3), 191–219 (2008).
3. Berlekamp E.R.: Algebraic Coding Theory. McGraw-Hill, New York (1968).
4. Bose R.C.: An affine analogue of Singer's theorem. J. Indian Math. Soc. **6**, 1–15 (1942).
5. Cossidente A., Labbate D., Siciliano A.: Veronese varieties over finite fields and their projections. Des. Codes Cryptogr. **22**, 19–32 (2001).
6. Couvreur A., Duursma I.: Evaluation codes from smooth Quadric surfaces and twisted segre varieties, arXiv 1101.4603v1.
7. Giuzzi L., Sonnino A.: LDPC codes from singer cycles. Discret. Appl. Math. **157**(8), 1723–1728 (2009).
8. Harris J.: Algebraic Geometry: a First Course. GTM 133, Springer, New York (1992)
9. Hassett B.: Introduction to Algebraic Geometry. Cambridge University Press, Cambridge (2007)
10. Hirschfeld J.W.P.: Finite Projective Spaces of Three Dimension. Oxford University Press, Oxford (1986).
11. Hirschfeld J.W.P., Thas J.A.: General Galois Geometries. Oxford University Press, Oxford (1991).
12. Kantor W.M., Shult E.E.: Veroneseans, power subspaces and independence. Adv. Geom. (in press).
13. Lunardon G.: Planar fibrations and algebraic subvarieties of the Grassmann variety. Geom. Dedicata **16**(3), 291–313 (1984).
14. Lunardon G.: Normal spreads. Geom. Dedicata **75**(3), 245–261 (1999).

15. MacWilliams F.J., Sloane N.J.A.: The Theory of Error Correcting Codes. North-Holland, Amsterdam (1977).
16. Paige L.J.: A note on the Mathieu groups. Can. J. Math. **9**, 15–18 (1957).
17. Pepe V.: On the algebraic variety $\mathcal{V}_{r,t}$. Finite Fields Appl., **17**(4), 343–349 (2011).
18. Radkova D., Van Zanten A.J.: Constacyclic codes as invariant subspaces. Linear Algebra Appl. **430**(2–3), 855–864 (2009).
19. Segre B.: Teoria di Galois, fibrazioni proiettive e geometrie non Desarguesiane. Ann. Mat. Pura Appl. **64**, 1–76 (1964).
20. Snapper E.: Periodic linear transformations of affine and projective geometries. Can. J. Math. **2**, 149–151 (1950).
21. Steinberg R.: Representations of algebraic groups. Nagoya Math. J. **22**, 33–56 (1963).