LDPC codes from Singer cycles

Luca Giuzzi

Dipartimento di Matematica
Facoltà di Ingegneria
Università degli Studi di Brescia
Via Valotti 9 25133 Brescia, Italy
Email: giuzzi@ing.unibs.it

Angelo Sonnino

Dipartimento di Matematica e Informatica
Università della Basilicata
Campus Macchia Romana
Viale dell'Ateneo Lucano, 10
85100 Potenza, Italy
Email: angelo.sonnino@unibas.it

28th April 2009

Abstract

The main goal of coding theory is to devise efficient systems to exploit the full capacity of a communication channel, thus achieving an arbitrarily small error probability. Low Density Parity Check (LDPC) codes are a family of block codes—characterised by admitting a sparse parity check matrix—with good correction capabilities. In the present paper the orbits of subspaces of a finite projective space under the action of a Singer cycle are investigated. The incidence matrix associated to each of these structures yields an LDPC code in a natural manner.

Keywords: LDPC Codes; projective spaces; Singer cycles

1 Introduction

A $[n, k, d]$–linear code over $\mathrm{GF}(q)$ is a monomorphism θ from $M = \mathrm{GF}(q)^k$ into $R = \mathrm{GF}(q)^n$ such that the images of any two distinct vectors $\mathbf{m_1}, \mathbf{m_2} \in M$ differ in at least d positions in R. The elements of M are called messages, while the elements of the image $\mathcal{C} = \theta(M)$ are the codewords of θ. The function

$$\begin{array}{rcl} d : R \times R & \rightarrow & \mathbb{N} \\ (\mathbf{x}, \mathbf{y}) & \mapsto & |\{i : x_i - y_i \neq 0\}| \end{array}$$

is the *Hamming distance on R*. In the present paper we shall usually identify a code with the set of its codewords.

The problem of *minimum distance decoding* is to find, for any given vector $\mathbf{r} \in R$ the set $\mathcal{C}_{\mathbf{r}}$ of all the codewords $\mathbf{c} \in \mathcal{C}$ at minimum Hamming distance from $\mathbf{r}$. If $\mathcal{C}_{\mathbf{r}}$ contains just one element $\mathbf{c}$, then we can uniquely determine a message $\mathbf{m}$ such that $\theta(\mathbf{m}) = \mathbf{c}$ and we state that the decoding of $\mathbf{r}$ has succeeded; otherwise, we remark that it has not been possible to correctly determine the original message.

Minimum distance decoding is, in general, a hard problem; in fact, it is often convenient to sacrifice some of the correcting capabilities of a code in favour of ease of implementation and lower complexity, see [3]; this approach is followed in most of the currently deployed algorithms: notable examples are the syndrome decoding technique for general linear codes and the Welch–Berlekamp approach for BCH codes, see [18]. However, even these techniques might be prohibitively expensive when the length n of the code, that is the dimension of the vector space R, is large, see [2].

On the other hand, long codes present several advantages; indeed, it can be shown that almost all codes with large n have excellent correction capabilities, see [17]. It is thus important to determine and investigate special families of codes for which good encoding and decoding algorithms are known.

Low Density Parity Check (LDPC) codes have been originally introduced by Gallager in [10],[9] and, then, ignored for almost 30 years. Their rediscovery is quite recent; see [16]. It has been realised that they may be applied to high–speed, high–bandwidth digital channels since they support efficient decoding algorithms based upon message–passing strategies. It has also been seen that the performance of some of these codes is remarkably close to the Shannon limit for the AWGN channel; consequently, they result very competitive, even when compared with more elaborate constructions, like turbo codes, see [16]. The problem of providing efficient encoding for LDPC codes is, nevertheless, non–trivial in the general case, see [5]; although, it might still be often manageable, see [19]. This motivates the search for new ways of constructing suitable parity–check matrices for broad classes of LDPC codes.

Recall that a linear code is Low Density Parity Check if it admits at least one parity check matrix which is sparse. In particular, an LDPC code is *regular* if the set of its codewords is the null space of a parity check matrix $\mathbf{H}$ with the following structural properties:

(L1) each row of $\mathbf{H}$ contains $t + 1$ non–zero entries;

(L2) each column of $\mathbf{H}$ contains $r + 1$ non–zero entries;

(L3) the number of non–zero entries in common between any two distinct columns of $\mathbf{H}$ is at most 1;

(L4) both t and r are small compared with the length n of the code and the number of rows in $\mathbf{H}$.

It is immediate to see that any matrix satisfying conditions L1–L3 corresponds to the incidence matrix of a (t,r)–partial linear space; this suggests that a possible approach to constructing regular LDPC codes might be to investigate the geometry of finite projective spaces $\mathrm{PG}(n-1,q)$.

In the present paper we describe a procedure for constructing such parity–check matrices by determining suitable representatives of the orbits of subspaces of a finite projective space $\mathrm{PG}(n-1,q)$, with q even, under the action of a Singer cycle. This provides an efficient way for determining algorithmically this matrix without requiring to store any of its rows beforehand. Such an approach may be useful in memory constrained devices. In sections 2 and 3, preliminaries on incidence structures and projective spaces are recalled. The main tool for our construction is a $\mathrm{GF}(q)$–linear representation of a projective space $\mathrm{PG}(n-1,q^r)$, introduced in Section 4. The actual decompositions of $\mathrm{PG}(n-1,q^r)$ in orbits under the action of the Singer cycle are introduced respectively in Section 5. Finally, in Section 6, the 3–dimensional case with q even is studied in detail.

2 Preliminaries: incidence matrices

There is a well known correspondence between finite incidence structures and binary matrices. This topic has been widely investigated, also in the context of coding theory; see [1].

Given any binary matrix M, it is always possible to introduce an incidence structure $\mathcal{S}_M = (\mathcal{P},\mathcal{L},I)$ as follows: the points of $\mathcal{P}$ are the columns of M, the blocks of $\mathcal{L}$ are the rows of M and $P \in \mathcal{P}$ is incident with $L \in \mathcal{L}$ if and only if the intersection between the column P and the row L is 1. Conversely, given an incidence structure $\mathcal{S}$ with point–set $\mathcal{P} = \{p_1, p_2, \ldots, p_v\}$ and block–set $\mathcal{L} = \{l_1, l_2, \ldots, l_b\}$, an *incidence matrix* $M = (m_{ij})$ of $\mathcal{S}$ is any binary $b \times v$–matrix with

$$m_{ij} = \begin{cases} 1 & \text{if } p_j I l_i \\ 0 & \text{otherwise.} \end{cases}$$

An incidence structure $\mathcal{S} = (\mathcal{P},\mathcal{L},I)$ may be written simply as $(\mathcal{P},\mathcal{L})$ when any element $L \in \mathcal{L}$ is a subset of $\mathcal{P}$, and given $p \in \mathcal{P}$ and $L \in \mathcal{L}$, we have pIL if, and only if, $p \in L$.

A collineation of $\mathcal{S}$ is any map $\varphi : \mathcal{P} \cup \mathcal{L} \to \mathcal{P} \cup \mathcal{L}$ sending points into points, blocks into blocks and preserving all incidences. Clearly, the set of all collineations of an incidence structure together with functional composition is a group. In the present paper, we are interested in incidence structures endowed with a collineation group G acting regularly on the points. In this case, it turns out to be quite easy to write all the blocks in $\mathcal{L}$, and the associated incidence matrix $\mathbf{H}$ has a special form. We proceed as follows.

Given a point $P \in \mathcal{P}$, let $\mathcal{T} = \{\ell_1, \ell_2, \ldots, \ell_h\}$ be the set of the blocks of $\mathcal{S}$ incident with P such that:

- $\ell_i^g \neq \ell_j$ for any $g \in G$ and $1 \leq i < j \leq h$;
- for any block $\ell \in \mathcal{L}$ there is a block $\ell_i \in \mathcal{T}$ and a $g \in G$ such that $\ell = \ell_i^g$.

The set $\mathcal{T}$ is called a *starter set* for $\mathcal{S}$, see [6].

Observe that $\mathcal{L}$ is given by the disjoint union

$$\mathcal{L} = \bigcup_{j=1}^{h} \{ \ell_j^g \mid g \in G \};$$

therefore, the whole incidence matrix $\mathbf{H}$ of $\mathcal{S}$ can be reconstructed by just providing a suitable starter set $\mathcal{T}$ and generators for the group G.

Further, if we suppose that G is cyclic, and denote by τ one of its generators, the incidence structure

$$\mathcal{S} = (\mathcal{P}, \{ \ell_j^{\tau^i} \mid 1 \leq i \leq |G|, \ 1 \leq j \leq h \})$$

admits at least a circulant incidence matrix $\mathbf{H}$; that is, a block matrix $\mathbf{H}$ of type

$$\mathbf{H} = \begin{pmatrix} H_1 \\ \vdots \\ H_h \end{pmatrix}$$

wherein any row H_j, $j > 1$ is obtained from the preceding one H_{j-1} by applying a cyclic right shift. Clearly, for this to happen, the points and blocks of $\mathcal{S}$ have to be arranged is such a way that $P_i = P^{\tau^{i-1}}$ and $\ell_i = \ell_j^{\tau^{i-1}}$ with $j \in \{1, 2, \ldots, h\}$.

3 Preliminaries: projective spaces and spreads

Let $\mathrm{PG}(V, \mathbb{F})$ be the projective space whose elements are the vector subspaces of the vector space V over the field $\mathbb{F}$. We denote by the same symbol a 1–dimensional vector subspace of V and the corresponding element of $\mathrm{PG}(V, \mathbb{F})$. An element T of $\mathrm{PG}(V, \mathbb{F})$ has *rank* t and *dimension* $t-1$, whenever T has dimension t as a vector space over $\mathbb{F}$. When the dimension of V over $\mathbb{F} = \mathrm{GF}(q)$ is finite and equal to n, we shall usually write $\mathrm{PG}(n-1, q)$ instead of $\mathrm{PG}(V, \mathbb{F})$. The elements of rank 1, 2, 3 and $n-1$ in $\mathrm{PG}(n-1, q)$ are called respectively *points*, *lines*, *planes* and *hyperplanes.* Points contained in the same line are said to be *collinear.* Observe that, for any $i \geq 1$,

$$\mathrm{PG}_i(V) = (\mathcal{P}, \mathcal{L}),$$

where $\mathcal{P} = \{W \leq V : \dim W = 1\}$ and $\mathcal{L} = \{X \leq V : \dim X = i+1\}$, is an incidence structure.

Let now $\{E_0, E_1, \ldots, E_{n-1}\}$ be a fixed basis of V. Then, the point $\langle x_0 E_0 + x_1 E_1, + \cdots + x_{n-1} E_{n-1} \rangle$ of $\mathrm{PG}(V, \mathbb{F})$ has homogeneous projective coordinates $(x_0, x_1, \ldots, x_{n-1})$.

The points and the lines of a projective space $\mathrm{PG}(n-1, q)$ form a 2–design, whose incidence matrix M defines a regular LDPC code, called $\mathbb{PG}^{(1)}$ in [14]. The code defined by the transposed matrix M is also LDPC and it is called $\mathbb{PG}^{(2)}$ in the aforementioned paper.

The full collineation group of $\mathrm{PG}(n-1,q)$ is $\mathrm{P\Gamma L}(n,q)$; however, in the present paper we shall be mostly concerned with the group $\mathrm{PGL}(n,q)$ of the projectivities of $\mathrm{PG}(n-1,q)$, that is of all those collineations of $\mathrm{PG}(n-1,q)$ which might be represented by a non–singular $n \times n$–matrix; see [13, Section 2.1].

A cyclic subgroup S of $\mathrm{PGL}(n,q)$ acting regularly on the points of $\mathrm{PG}(n-1,q)$ is called a *Singer subgroup*. Any two Singer subgroups, say $\mathfrak{S}$ and $\mathfrak{S}'$, of $\mathrm{PGL}(n,q)$ are conjugated in $\mathrm{PGL}(n,q)$; for more details, see [13, Section 4.2].

We may identify the underlying n–dimensional vector space V of $\mathrm{PG}(n-1,q)$ with the field $\mathrm{GF}(q^n)$. Let now α be a generator of the multiplicative group of this field; then, the map σ of $\mathrm{GF}(q^n)$ into itself defined by $\sigma : x \mapsto \alpha x$ is a non–singular $\mathrm{GF}(q)$–linear map. Observe that σ, as a linear map, has order $q^n - 1$ and defines a collineation of $\mathrm{PG}(n-1,q)$ of order $q^{n-1} + \cdots + q + 1$, acting transitively on the points of $\mathrm{PG}(n-1,q)$; hence, the collineation group $\mathfrak{S}$ generated by σ is indeed a Singer cycle of $\mathrm{PG}(n-1,q)$.

The projective space $\mathrm{PG}(n-1,q) = \mathrm{PG}(V, \mathrm{GF}(q))$ may be regarded as a distinguished hyperplane of $\mathrm{PG}(n,q) = \mathrm{PG}(V', \mathrm{GF}(q))$, with $V' = \langle E\rangle \oplus V$. Let now σ be the generator of a Singer cycle of $\mathrm{PG}(n-1,q)$. The map

$$\sigma' : xE + v \mapsto xE + v^{\sigma}$$

gives a cyclic collineation group $\tilde{\mathfrak{S}}$ of order $q^n - 1$, which induces a Singer cycle on the hyperplane $\mathrm{PG}(n-1,q)$ and acts regularly on the points of $\mathrm{PG}(n,q) \setminus \mathrm{PG}(n-1,q)$ different from $\langle E\rangle$. Furthermore, this group $\tilde{\mathfrak{S}}$ acts transitively on the lines of $\mathrm{PG}(n,q)$ incident with $\langle E\rangle$. This is called the *affine Singer group* of $\mathrm{PG}(n,q)$.

A $(t-1)$*–spread* $\mathcal{S}$ of a projective space $\mathrm{PG}(n-1,q)$ is a family of mutually disjoint subspaces, each of rank t, such that each point of $\mathrm{PG}(n-1,q)$ belongs to exactly one element of $\mathcal{S}$. It has been proved by Segre [20] that a $(t-1)$–spread of $\mathrm{PG}(n-1,q)$ exists if and only if $n = rt$. A spread $\mathcal{S}$ with $t = 2$ is a *line–spread*. Suppose $\mathcal{S}$ to be a $(t-1)$–spread of $\mathrm{PG}(rt-1,q)$ and embed $\mathrm{PG}(rt-1,q)$ into $\mathrm{PG}(rt,q)$ as a hyperplane. It is now possible to introduce a new incidence structure $A(\mathcal{S}) = (\mathcal{P}, \mathcal{B})$ where

- the points in $\mathcal{P}$ are the points of $\mathrm{PG}(rt,q) \setminus \mathrm{PG}(rt-1,q)$;

- the blocks in $\mathcal{B}$ are the t–dimensional subspaces of $\mathrm{PG}(rt,q)$ which are not contained in $\mathrm{PG}(rt-1,q)$ but contain an element of $\mathcal{S}$;

- incidence is the natural one.

The structure $A(\mathcal{S})$ is a $2-(q^{rt}, q^t, 1)$ translation design with parallelism; see [4]. The $(t-1)$-spread $\mathcal{S}$ is called Desarguesian when $A(\mathcal{S})$ is isomorphic to the affine space $AG(r, q^t)$.

We need the following two characterisations of Desarguesian spreads, according as $r = 2$ or $r \neq 2$.

When $r = 2$, the underlying projective space has necessarily dimension $2t-1$.

Theorem 1 ([8])**.** *Assume $q > 2$. A $(t-1)$-spread $\mathcal{S}$ of $\mathrm{PG}(2t-1, q)$ is Desarguesian if and only if it is regular.*

Recall that a *regulus* $\mathcal{R}$ of $\mathrm{PG}(2t-1, q)$ is a set of $q+1$ mutually disjoint $(t-1)$-dimensional subspaces such that each line intersecting three elements of $\mathcal{R}$ has a point in common with all the subspaces of $\mathcal{R}$. If A, B, C are three mutually disjoint $(t-1)$-dimensional subspaces of $\mathrm{PG}(2t-1, q)$, then there is a unique regulus $\mathcal{R}(A, B, C)$ of $\mathrm{PG}(2t-1, q)$ containing A, B and C. A spread $\mathcal{S}$ is *regular* if the regulus $\mathcal{R}(A, B, C)$ is contained in $\mathcal{S}$ whenever A, B and C are three distinct element of $\mathcal{S}$.

A $(t-1)$-spread is *normal* when it induces a spread in any subspace generated by any two of its elements; see [15]. In particular, fix $T = \langle A, B\rangle$ with $A, B \in \mathcal{S}$. Then, for any $C \in \mathcal{S}$, either $C \subseteq T$ or $C \cap \mathcal{S} = \emptyset$. Such spreads are called *geometric* in [20].

Theorem 2 ([4])**.** *For $r > 2$, the $(t-1)$-spread $\mathcal{S}$ is Desarguesian if and only if it is normal.*

4 On the $\mathrm{GF}(q)$-linear representation of $\mathrm{PG}(r-1, q^t)$

Let V be the underlying r–dimensional vector space of $\mathrm{PG}(r-1, q^t)$. Clearly, V may also be regarded as an rt–dimensional vector space over the subfield $\mathrm{GF}(q)$. In particular, each point $\langle x\rangle$ of $\mathrm{PG}(r-1, q^t)$ determines a $(t-1)$-dimensional subspace $P(x)$ of the projective space $\mathrm{PG}(rt-1, q)$ and, likewise, each line l of $\mathrm{PG}(r-1, q^t)$ defines a $(2t-1)-$dimensional subspace $P(l)$ of $\mathrm{PG}(rt-1, q)$.

Write $\mathcal{L}$ for the set of all $(t-1)$-dimensional subspaces of $\mathrm{PG}(rt-1, \mathrm{GF}(q))$, each obtained as $P(x)$, as x varies in the set of points of $\mathrm{PG}(r-1, q^t)$; it turns out that $\mathcal{L}$ is a $(t-1)$-spread of $\mathrm{PG}(rt-1, q)$, which is called the $\mathrm{GF}(q)$-linear representation of $\mathrm{PG}(r-1, q^t)$. It has been shown that $\mathcal{L}$ is Desarguesian and any Desarguesian spread of $\mathrm{PG}(rt-1, q)$ is isomorphic to $\mathcal{L}$; see [8] for $r = 2$ and [20, 4] for $r > 2$.

There is a very strong link between Desarguesian spreads and cyclic collineation groups, as shown in the following general theorem.

Theorem 3. *A $(t-1)$-spread $\mathcal{S}$ of $\mathrm{PG}(rt-1, q)$ is Desarguesian if and only if there is a collineation group of $\mathrm{PG}(rt-1, q)$ of order $q^{t-1} + q^{t-2} + \cdots + q + 1$ fixing all elements of $\mathcal{S}$.*

Proof. Let T be the translation group of $A(\mathcal{S})$; that is, T is the group of all elations of $\mathrm{PG}(rt, q)$ with axis $\mathrm{PG}(rt-1, q)$. Fix a point O in $A(\mathcal{S})$ and write T_L for the stabiliser of any block L of $A(\mathcal{S})$ through O; denote by $\mathcal{K}$ the set of all the subgroups T_L thus obtained. Observe that the group T is elementary abelian, while each subgroup T_L is transitive on the points of the chosen block L. It is now possible to introduce a new incidence structure π, whose points are the elements of T and whose blocks are the lateral classes of the subgroups T_L in T. Given a point $P \in A(\mathcal{S})$, denote by $\tau_{O,P}$ the element of T which maps O into P. The map $P \mapsto \tau_{O,P}$ is an isomorphism between $A(\mathcal{S})$ and π.

The *kernel* K of $\mathcal{K}$ is the set of all the endomorphisms α of T such that $T_L^\alpha \subset T_L$ for any L. It has been shown in [7] that K is always a field. In particular, T is naturally a vector space over K and each element of $\mathcal{K}$ is a subspace. Given any central collineation ω of $\mathrm{PG}(rt, q)$ with axis $\mathrm{PG}(rt-1, q)$ and centre O, the map $\bar{\omega}$ of T into itself defined by $\bar{\omega} : \tau \mapsto \omega\tau\omega$ is an element of K. Hence, K contains a subfield isomorphic to $\mathbb{F} = \mathrm{GF}(q)$.

Consider now the projective space $\mathrm{PG}(T, \mathbb{F})$. Denote by $\mathcal{K}(\mathbb{F})$ the spread of $\mathrm{PG}(T, \mathbb{F})$ induced by $\mathcal{K}$. The designs π and $A(\mathcal{K}(\mathbb{F}))$ are isomorphic. Furthermore, the $(t-1)$-spreads $\mathcal{S}$ and $\mathcal{K}(\mathbb{F})$ are also isomorphic, that is, there is a collineation τ of $\mathrm{PG}(rt-1, q)$ such that $\mathcal{S}^\tau = \mathcal{K}(\mathbb{F})$, see [7].

It follows that $\mathcal{S}$ is Desarguesian if and only if T_L has dimension 1 over K; see [7]. This condition is equivalent to require that K has order $q^t - 1$; in this case it defines a collineation group of $\mathrm{PG}(rt-1, q)$ of order $q^{t-1} + q^{t-2} + \cdots + q + 1$ which fixes all the elements of $\mathcal{K}(\mathbb{F})$. □

Theorem 4. *Let* $\mathfrak{S}$ *be a Singer cycle of* $\mathrm{PG}(n-1, q)$*, with* $n = rt$ *and* q *even. Denote by* $\mathfrak{S}_1$ *and* $\mathfrak{S}_2$ *the subgroups of* $\mathfrak{S}$ *of order respectively* $\frac{q^t-1}{q-1}$ *and* $\frac{q^n-1}{q^t-1}$*, so that* $\mathfrak{S} = \mathfrak{S}_1 \times \mathfrak{S}_2$*. Then, there is a Desarguesian* $(t-1)$*-spread* $\mathcal{S}$ *of* $\mathrm{PG}(n-1, q)$ *such that* $\mathfrak{S}_2$ *acts regularly on* $\mathcal{S}$ *and* $\mathfrak{S}_1$ *fixes all its elements.*

Proof. Consider $\mathrm{PG}(n-1, q) = \mathrm{PG}(\mathrm{GF}(q^n), \mathrm{GF}(q))$ and assume $\mathfrak{S}$ to be the Singer cycle spanned by the collineation $\sigma : x \mapsto \alpha x$, where α is a generator of the multiplicative group of $\mathrm{GF}(q^n)$.

As t divides n, the element $\beta = \alpha^{\frac{q^n-1}{q^r-1}}$ is a generator of the multiplicative group of the subfield $\mathrm{GF}(q^t)$ of $\mathrm{GF}(q^n)$. Now let $\mathfrak{S}_1$ be the subgroup of $\mathfrak{S}$ generated by $\sigma_1 = \sigma^{\frac{q^n-1}{q^r-1}}$. Then, $\mathcal{S} = \{\, \mathrm{GF}(q^t)x \mid x \in \mathrm{GF}(q^n) \,\}$ is a $(t-1)$-spread of $\mathrm{PG}(n-1, q)$ which is preserved by $\mathfrak{S}_1$.

The incidence structure $A(\mathcal{S})$ is isomorphic to the affine space $\mathrm{AG}(r, GF(q^t))$; thus, $\mathcal{S}$ is Desarguesian.

If γ is a primitive element of $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q^t)$, then the collineation defined by the map $\sigma_2 : x \mapsto \gamma x$ defines a subgroup $\mathfrak{S}_2$ of $\mathfrak{S}$ of order $\frac{q^n-1}{q^t-1}$. By construction, $\mathfrak{S} = \mathfrak{S}_1 \times \mathfrak{S}_2$. As $\mathcal{S} = \{\, \mathrm{GF}(q^t)\gamma^j \mid (q^t)^{r-1} + \cdots + q^t + 1 \geq j \geq 0 \,\}$, the group $\mathfrak{S}_2$ preserves the $(t-1)$-spread $\mathcal{S}$ and acts regularly on its elements. □

5 Decompositions of $\mathrm{PG}(n-1, q)$

Let S be a Singer cycle of $\mathrm{PG}(n-1, q)$. We distinguish two cases, according as the rank n is odd or even.

If n is odd, any line of $\mathrm{PG}(n-1, q)$ has an orbit of length $\frac{q^n-1}{q-1}$ under the action of $\mathfrak{S}$; thus, the set of all lines of $\mathrm{PG}(n-1, q)$ consists of $\frac{q^{n-1}-1}{q^2-1}$ orbits. Each of these orbits, say i for $1 \leq i \leq \frac{q^{n-1}-1}{q^2-1}$, defines a cyclic structure whose incidence matrix M_i is circulant. Hence, the full incidence matrix M of $\mathbb{PG}^{(1)}$ has the following structure:

$$M = \begin{pmatrix} M_1 \\ M_2 \\ \vdots \\ M_{(q^{n-1}-1)/(q^2-1)} \end{pmatrix}.$$

A starter set may be constructed as follows. Let σ be a generator of $\mathfrak{S}$ and choose a point P. Fix a line l incident with P, suppose that $i_0 = 0, i_1, \ldots, i_q$ are integers, and $P = P^{\sigma^{i_0}}, P_1 = P^{\sigma^{i_1}}, \ldots, P_q = P^{\sigma^{i_q}}$ are the points of l. Then, $l_j = l^{\sigma^{i_j}}$, $0 \leq j \leq q$ are exactly the $q+1$ lines of the orbit of l under the action of $\mathfrak{S}$ which are incident with l. Hence, a starter set of $\mathrm{PG}(n-1,q)$ is given by $\mathbf{S} = \{s_1, s_2, \ldots, s_{\frac{q^{n-1}-1}{q^2-1}}\}$, consisting of $\frac{q^{n-1}-1}{q^2-1}$ lines incident with P such that, if P^{σ^h} belongs to s_i, then $s_i^{\sigma^h}$ does not belong to $\mathbf{S}$.

Suppose now $n = 2t$ with $t > 1$. As in Section 4, write $\mathfrak{S} = \mathfrak{S}_1 \times \mathfrak{S}_2$, where $\mathfrak{S}_1$ has order $\frac{q^2-1}{q-1}$ and $\mathfrak{S}_2$ has order $\frac{q^{2t}-1}{q^2+1}$. By Theorem 4, there is a Desarguesian line spread $\mathcal{S}$ of $\mathrm{PG}(2t-1,q)$ such that $\mathfrak{S}_1$ fixes all the lines of $\mathcal{S}$ while $\mathfrak{S}_2$ acts regularly on its elements.

Lemma 1. *The stabiliser in $\mathfrak{S}$ of a line m not in $\mathcal{S}$ is the identity.*

Proof. There are $\frac{q^n-1}{q^2-1}$ lines in $\mathrm{PG}(n-1,q)$ whose stabiliser in $\mathfrak{S}$ is different from the identity; see [21]. Since $\mathcal{S}$ contains exactly $\frac{q^n-1}{q^2-1}$ lines, each being fixed by $\mathfrak{S}_1$, we have that the stabiliser in $\mathfrak{S}$ of a line m not in $\mathcal{S}$ is the identity. □

The set of all the lines of $\mathrm{PG}(n-1,q)$ can be decomposed into $\mathcal{S}$ and $q(q^{2t-4} + q^{2t-6} + \cdots + q^2 + 1)$ orbits under the action of $\mathfrak{S}$, each of length $\frac{q^{2t}-1}{q-1}$. These orbits, say i, for $1 \leq i \leq q(q^{2t-4} + \cdots + q^2 + 1)$ define a cyclic structure whose incidence matrix M_i is circulant. Hence, the incidence matrix M of $\mathbb{PG}^{(1)}$ assumes in this case the following structure

$$M = \begin{pmatrix} M_0 \\ M_1 \\ \vdots \\ M_{q(q^{2t-2}-1)/(q^2-1)} \end{pmatrix},$$

where M_0 is the incidence matrix of the structure induced on $\mathcal{S}$. In particular, observe that the points of $\mathrm{PG}(n-1,q)$ may be indexed in such a way that

$$M_0 = \begin{pmatrix} B_1 & B_2 & \cdots & B_{q+1} \end{pmatrix},$$

where $B_1 = B_2 = \cdots = B_{q+1}$ is the identity matrix of order $q^{n-1} + q^{n-2} + \cdots + q + 1$.

6 Starters in $\mathrm{PG}(3, 2^e)$

In this section, a geometric description of a starter set in $\mathrm{PG}(3, 2^e)$ shall be presented. We first need to recall some properties of elliptic quadrics and regular spreads in this space. The interested reader might look at [12] for a proof of the results.

Denote by $Q^-(3, q)$ the set of all points of $\mathrm{PG}(3, q)$ whose homogeneous coordinates are solution of the equation

$$X_0X_1 + X_2^2 + bX_2X_3 + cX_3^2 = 0,$$

where b and c are such that as $\xi^2 + b\xi + c$ is an irreducible polynomial over $\mathrm{GF}(q)$. A set of points $\mathcal{O}$ is an *elliptic quadric* if there is a collineation τ of $\mathrm{PG}(3, q)$ such that $\mathcal{O}^\tau = Q^-(3, q)$. A line which intersects $\mathcal{O}$ in exactly one point is called a *tangent line,* while a plane which intersects $\mathcal{O}$ in just one point is called a *tangent plane.* The following properties are straightforward:

- $\mathcal{O}$ contains $q^2 + 1$ points;
- no three points of $\mathcal{O}$ are collinear;
- a plane meets $\mathcal{O}$ in either one or in $q + 1$ points;
- if P is a point of $\mathcal{O}$, then the lines tangent to $\mathcal{O}$ at P are contained in a plane, the tangent to $\mathcal{O}$ at P;
- there is a cyclic subgroup of order $q^2 + 1$ of $\mathrm{PGL}(4, q)$ which acts transitively on $\mathcal{O}$.

In particular there is always a regular spread $\mathcal{S}$ which consists of tangent lines to $\mathcal{O}$; see also [11]. This spread is Desarguesian; see Theorem 1. Thus $\mathcal{S}$ is a line orbit under the action of a Singer group $\mathfrak{S}$, see Theorem 3, and is stabilised by a subgroup $\mathfrak{S}_2 < \mathfrak{S}$ of order $q^2 + 1$. This subgroup acts regularly on $\mathcal{O}$.

Let $\mathfrak{S}_1 = \langle \tau \rangle$ be a subgroup of $\mathfrak{S}$ of order $q + 1$ fixing all the lines of $\mathcal{S}$ and acting transitively on the points of any line of the spread. Then, $\mathcal{O}_i = \mathcal{O}^{\tau^i}$, for $i = 0, 1, \ldots, q$ is an elliptic quadric and any line of $\mathcal{S}$ is tangent to $\mathcal{O}_i$; indeed, $\{\mathcal{O}_0, \mathcal{O}_1, \ldots, \mathcal{O}_q\}$ is a partition of the point-set of $\mathrm{PG}(3, q)$.

Lemma 2. *For any line ℓ of $\mathrm{PG}(3, q)$ not in $\mathcal{S}$ there is a unique quadric $\mathcal{O}_i$ such that ℓ is tangent to $\mathcal{O}_i$.*

Proof. As q is even, for any quadric $\mathcal{O}$ there is a symplectic polarity $\perp$ of $\mathrm{PG}(3, q)$ such that a line ℓ is tangent to $\mathcal{O}$ if and only if ℓ is totally isotropic with respect to π.

Let π_i be the symplectic polarity induced by $\mathcal{O}_i$ for $i \neq 0$ and write $\perp$ for the symplectic polarity induced by $\mathcal{O}$. The line ℓ of $\mathrm{PG}(3, q)$ is totally isotropic simultaneously respect to $\perp$ and to π_i if and only if ℓ belongs to $\mathcal{S}$; see [12]. Hence, ℓ may not be tangent to both $\mathcal{O}$ and $\mathcal{O}_i$; in particular, $\mathcal{O}_i$ and $\mathcal{O}_j$ for $i \neq j$ do not have any common tangent for $i \neq j$.

An elliptic quadric $\mathcal{O}_i$ has $(q^2+1)(q+1)$ tangent lines; as q^2+1 of these belong to $\mathcal{S}$, there are $(q^2+1)q(q+1)$ lines of $\mathrm{PG}(3,q)$ which are tangent to exactly one of the quadrics $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_q$. Since the number of the lines of $\mathrm{PG}(3,q)$ not in $\mathcal{S}$ is $(q^2+1)q(q+1)$, this yields the lemma. □

We are now in the position to state the main theorem of this section.

Theorem 5. *The lines tangent to the elliptic quadric $\mathcal{O}$ through a fixed point $P \in \mathcal{O}$ form a starter set of* $\mathrm{PG}(3,q)$.

Proof. Let α be the plane tangent to $\mathcal{O}$ at P and denote by $\{m_0, m_1, \ldots, m_q\}$ be the $q+1$ tangent lines through P. Assume that m_0 belongs to $\mathcal{S}$.

Suppose there is $\delta \in \mathfrak{S}$ such that $m_i^\delta = m_j$ with $i, j \neq 0$; clearly, $m_0^\delta \in \mathcal{S}$, since $\mathcal{S}$ is fixed by all the elements of $\mathfrak{S}$. Assume that $m_0^\delta \neq m_0$. If it were $\mathcal{O} = \mathcal{O}^\delta$, then the line m_j would be incident with both P and P^δ, both in $\mathcal{O}$; hence, m_j would not be tangent to $\mathcal{O}$. Thus, $\mathcal{O} \neq \mathcal{O}^\delta$. This implies that m_j is tangent to both $\mathcal{O}$ and $\mathcal{O}^\delta$ – a contradiction by Lemma 2. It follows that $m_0^\delta = m_0$. In particular, $\delta \in \mathfrak{S}_1$.

To conclude the proof, observe that if $P^\delta \neq P$, then m_j is tangent to $\mathcal{O}^\delta$ at P^δ and to $\mathcal{O}$ at P, against Lemma 2. Hence, $\mathcal{O} = \mathcal{O}^\delta$ and $\delta = \mathrm{id}$. □

Acknowledgements

The authors wish to express their gratitude to prof. G. Lunardon for several insightful discussions on the topics here-within investigated.

References

[1] E. F. Assmus, Jr. and J. D. Key, *Designs and their codes*, Cambridge Tracts in Mathematics, vol. 103, Cambridge University Press, Cambridge, 1992. MR MR1192126 (93j:51003)

[2] Alexander Barg, *Complexity issues in coding theory*, Electronic Colloquium on Computational Complexity (ECCC) **4** (1997), no. 046.

[3] Alexander Barg, Evgueni Krouk, and Henk C. A. van Tilborg, *On the complexity of minimum distance decoding of long linear codes*, IEEE Trans. Inform. Theory **45** (1999), no. 5, 1392–1405. MR MR1699066 (2000c:94016)

[4] A. Barlotti and J. Cofman, *Finite Sperner spaces constructed from projective and affine spaces*, Abh. Math. Sem. Univ. Hamburg **40** (1974), 231–241.

[5] L. M. J. Bazzi and S. K. Mitter, *Encoding complexity versus minimum distance*, IEEE Trans. Inform. Theory **51** (2005), no. 6, 2103–2112. MR MR1699066 (2000c:94016)

[6] T. Beth, D. Jungnickel, and H. Lenz, *Design theory. Vol. I*, second ed., Encyclopedia of Mathematics and its Applications, vol. 69, Cambridge University Press, Cambridge, 1999.

[7] F. Bonetti and G. Lunardon, *Sugli S-spazi di traslazione*, Boll. Un. Mat. Ital. A (5) **14** (1977), no. 2, 368–374.

[8] R. H. Bruck and R. C. Bose, *The construction of translation planes from projective spaces*, J. Algebra **1** (1964), 85–102.

[9] R. G. Gallager, *Low-density parity-check codes*, IRE Trans. **IT-8** (1962), 21–28. MR MR0136009 (24 #B2048)

[10] ———, *Low density parity–check codes*, M.I.T. Press, 1963.

[11] David G. Glynn, *On a set of lines of* $\mathrm{PG}(3, q)$ *corresponding to a maximal cap contained in the Klein quadric of* $\mathrm{PG}(5, q)$, Geom. Dedicata **26** (1988), no. 3, 273–280. MR MR950065 (89h:51015)

[12] J. W. P. Hirschfeld, *Finite projective spaces of three dimensions*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1985.

[13] ———, *Projective geometries over finite fields*, second ed., Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1998.

[14] Y. Kou, S. Lin, and M. P. C. Fossorier, *Low-density parity-check codes based on finite geometries: a rediscovery and new results*, IEEE Trans. Inform. Theory **47** (2001), no. 7, 2711–2736.

[15] G. Lunardon, *Normal spreads*, Geom. Dedicata **75** (1999), no. 3, 245–261.

[16] D. J. C. MacKay, *Good error–correcting codes based on very sparse matrices*, IEEE Trans. Inform. Theory **45** (1999), no. 2, 399–431.

[17] Samuel J. MacMullan and Oliver M. Collins, *A comparison of known codes, random codes, and the best codes*, IEEE Trans. Inform. Theory **44** (1998), no. 7, 3009–3022. MR MR1672071 (99j:94082)

[18] R. J. McEliece, *The theory of information and coding*, second ed., Encyclopedia of Mathematics and its Applications, vol. 86, Cambridge University Press, Cambridge, 2002. MR MR1899280 (2002k:94001)

[19] T. J. Richardson and R. L. Urbanke, *Efficient encoding of low-density parity-check codes*, IEEE Trans. Inform. Theory **47** (2001), no. 2, 638–656.

[20] B. Segre, *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane*, Ann. Mat. Pura Appl. (4) **64** (1964), 1–76.

[21] H. Tang, J. Xu, Y. Kou, S. Lin, and K. Abdel-Ghaffar, *On algebraic construction of Gallager and circulant low-density parity-check codes*, IEEE Trans. Inform. Theory **50** (2004), no. 6, 1269–1279.