LDPC CODES FROM THE HERMITIAN CURVE

Valentina Pepe

Dipartimento di Matematica e Applicazioni "R. Caccioppoli"
Università degli Studi di Napoli Federico II
via Cintia, Monte S. Angelo
I-80126 Napoli, Italy
valepepe@unina.it

Abstract

Amongst the contributions to the theory of LDPC codes deriving from finite geometries ([13], [12], [9]), we present a study of the code **C** which has as parity-check matrix **H** the incidence matrix of the Hermitian curve of $PG(2, q^2)$ and the $q+1$-secant to it. The good performance of **C** with iterative decoding algorithm is showed by Johnson and Weller in [11]. In this paper we prove the "double" cyclic structure of **C**, we shorten **H** in a suitable way in order to obtain new codes and show how in some cases we have a gain in the code-rate; finally we present a geometric approach to easily construct the matrix **H**.

Keywords LDPC codes, quasi-cyclic codes, incidence matrix, Hermitian curve

1 Introduction

Let **H** be a parity-check matrix for the binary code **C**; if **H** is sparse, then the code **C** is said to be a Low Density Parity-Check (LDPC) code. Firstly introduced by Gallager [7], LDPC codes have been recently revitalized in [13, 9], where new results and applications are presented. The increasing interest in LDPC codes stems from their satisfying performance with iterative decoding, which turns out to be very close to the theoretical Shannon limit. Most of such codes have been computer generated, therefore a consequent incomplete knowledge about their structure is at the origin of a few unpleasant aspects in the applications, such as a certain decoding complexity, and a hard-to-determine minimum distance. More recent studies [13, 12, 9], are instead concerned with parity-check matrices being incidence matrices coming from finite geometries. Such a construction soon reveals its advantages: geometric properties -even

trivial ones, e.g. two lines have at most one common point, and so on- immediately translate into codes structural properties, in turn allowing for more efficient decoding algorithms - cyclic, quasi-cyclic ones arise; furthermore easier a priori descriptions of the code's characteristic become available, such as direct estimates on the minimum distance.

The aim of this paper is to give a rather satisfying description of some of the basic properties of the code $\mathbf{C}$ having as parity-check matrix $\mathbf{H}$ the incidence matrix of the *Hermitian curve* $\mathcal{H}(2, q^2)$ and the $q+1$ secants to $\mathcal{H}(2, q^2)$. Such a code has been already introduced and tested (see for example [11]) and it seems to perform well. We go further in the description of the code $\mathbf{C}$, in particular we give a precise determination of the C code-rate, we give a proof of the "double cyclic" structure of the code; eventually we describe a geometric approach allowing for an easy construction the matrix $\mathbf{H}$. Finally we present the codes $\mathbf{C}_{ext}$ and $\mathbf{C}_{sh}$, obtained in a standard way from $\mathbf{C}$, by extending and shortening $\mathbf{H}$ respectively, we compare their code-rate to the code-rate of $\mathbf{C}$ and study their Tanner graph.

2 Incidence structures, matrices and graphs

An incidence structure is a triple $\mathbb{P} = (\mathcal{P}, \mathcal{B}, I)$, where $\mathcal{P}$ is a set of *points*, $\mathcal{B}$ is a set of *blocks* and $I \subseteq (\mathcal{P} \times \mathcal{B} \cup \mathcal{B} \times \mathcal{P})$ is a symmetric *incidence relation*. We say that the point P and the block ℓ are incident (or P is on ℓ, or ℓ passes through P) if and only if $(P, \ell) \in I$. An incidence structure $\mathbb{P}$ with $|\mathcal{P}| = n$ and $|\mathcal{B}| = m$ can be represented by the incidence matrix, that is a $(m \times n)-$matrix, say $H = [h_{ij}]$, over $GF(2)$ whose rows (columns) are indexed by the blocks (points) and $h_{ij} = 1$ if and only if the ith block is incident with the jth point, $h_{ij} = 0$, otherwise.

If any two blocks of $\mathbb{P}$ are incident with at most one common point, $\mathbb{P}$ is called a *partial linear space* and the blocks are usually called *lines*. A *partial geometry* $pg(s, t, \alpha)$ is such that: each line is incident with a constant number $s+1$ of points, each point is incident with a constant number of $t+1$ lines and for any non-incident point-line pair (P, ℓ) the number of lines incident with P and intersecting ℓ is α. The incidence matrix of a partial geometry is regular, in the sense that any row has constant weight $s+1$ and any column has constant weight $t+1$. A map of $\mathcal{P} \cup \mathcal{B}$ into itself is called *collineation* if it maps points into points, lines into lines and preserves the incidence relation.

A matrix H is said to be *circulant* if every row is obtained by the preceding one by a right shift. Let $G = \langle g \rangle$ be a cyclic collineation group of a partial linear space $\mathbb{P} =(\mathcal{P}, \mathcal{B}, I)$, which acts regularly on the set $\mathcal{P}$, that is G is transitive on the points and the only element of G that fixes a point is the identity. Fix a point $P \in \mathcal{P}$ and label the elements of $\mathcal{P}$ so that $P_i = P^{g^{i-1}}$; let $G(\ell)$ be a line orbit under the action of G and label the lines of $G(\ell)$ so that $\ell_i = \ell^{g^{i-1}}$. In this

way, we have an incidence matrix $H = \begin{pmatrix} H_1 \\ \cdots \\ \cdots \\ H_t \end{pmatrix}$ of $\mathbb{P} = (\mathcal{P}, \mathcal{B}, I)$ where H_i (the incidence matrix of $\mathcal{P} \cup G(\ell)$) is a circulant matrix, $\forall\ i = 1, \ldots, t$. It is clear that in order to construct the matrix H, it is enough to know the first row of every H_i, that is, it is enough to know the incidence of t lines ℓ_i, $i = 1, \ldots, t$ such that $G(\ell_i) \neq G(\ell_j) \forall\ i \neq j$; we usually call such lines *starters*.

The *incidence graph* $\mathcal{G}$ of an incidence structure $\mathbb{P} = (\mathcal{P}, \mathcal{B}, I)$, is a graph which has as vertices set $\mathcal{P} \cup \mathcal{B}$ and two vertices x and y are connected if and only if $(x, y) \in I$. A *cycle* in $\mathcal{G}$ is a sequence of connected vertices which starts and ends at the same vertex and does not contain any other vertex more than once. The length of a cycle is the number of its vertices and the *girth* of $\mathcal{G}$ is the length of its shortest cycle. The graph of a partial geometry is free of cycles of length 4 and if α is greater than one, then $\mathcal{G}$ has $N_6 = \frac{1}{3} m(n - s - 1)\binom{\alpha}{2}$ cycles of length 6; if $\alpha = 1$, then the partial geometry is called generalized quadrangle, the graph $\mathcal{G}$ is free of cycles of length 4 and 6 and it contains $N_8 = \frac{1}{4} m(n - s - 1)ts$ cycles of length 8.

3 Finite-Geometry LDPC Codes

Let $\mathbf{H}$ be the incidence matrix of a partial geometry $pg(s, t, \alpha)$ and $\mathbf{C}$ be the binary LDPC code that has $\mathbf{H}$ (respect. the transpose of $\mathbf{H}$, say $\mathbf{H}^T$) as parity-check matrix. The code $\mathbf{C}$ turns out to be a $[n, n - rank_2(\mathbf{H})]$ (respect. $[m, m - rank_2(\mathbf{H})]$) code, where with $rank_2(\mathbf{H})$ we have denoted the rank of $\mathbf{H}$ over $GF(2)$; moreover, we have the minimum distance, $rank_2(\mathbf{H})$ and the girth of the Tanner graph of the code expressed in terms of the parameters of the partial geometry. In [12] the following lemma is proved:

Lemma 1 *Let* $\mathbf{H}$ *be the incidence matrix of a partial geometry* $pg(s, t, \alpha)$ *and* $\mathbf{C}$ *be the code which has* $\mathbf{H}^T$ *as parity-check matrix, then we have*

$$d_{\min} \geq \max \left\{ \frac{(t+1)(s+1-t+\alpha)}{\alpha}, \frac{2(s+\alpha)}{\alpha} \right\}. \tag{1}$$

Moreover, we have the following:

Lemma 2 *Let* $\mathbf{H}$ *be the incidence matrix of a partial geometry* $pg(s, t, \alpha)$ *and* $\mathbf{C}$ *be the code which has* $\mathbf{H}$ *as parity-check matrix, then we have*

$$d_{\min} \geq \max \left\{ \frac{(s+1)(t+1-s+\alpha)}{\alpha}, \frac{2(t+\alpha)}{\alpha} \right\}. \tag{2}$$

Proof. The matrix $\mathbf{H}^T$ is the incidence matrix of the dual geometry of the partial geometry $pg(s, t, \alpha)$, that is a partial geometry $pg(t, s, \alpha)$. ■

In [12], it is showed that

$$rank_2(H) \leq \frac{st(t+1)(s+1)}{\alpha(t+s+1-\alpha)} + 1 \tag{3}$$

and if $t+s+1-\alpha \equiv 1 \bmod 2$, then

$$rank_2(H) \geq \frac{st(t+1)(s+1)}{\alpha(t+s+1-\alpha)}. \tag{4}$$

The Tanner graph of a binary $[n,k]$ code $\mathbf{C}$ is a bipartite graph; the first level consists of the n vertices v_i which represent the code bits and the second level consists of the k vertices s_j which correspond to check sums; a code bit vertex v_i is connected with a check sum vertex s_j one if and only if the code bit v_i is contained in the check sum s_j. It is easy to see that the Tanner graph of a code from a partial geometry $pg(s,t,\alpha)$ is the incidence graph $\mathcal{G}$, hence if $\alpha > 1$, then the Tanner graph has girth 6, if $pg(s,t,\alpha)$ is a generalized quadrangle, then the Tanner graph has girth 8 .

In [13], [12] and [9] LDPC codes construction based on the incidence structure of finite geometries is presented and the properties of these codes are investigated. One of the most important proprieties observed in these codes is that they are cyclic or quasi-cyclic.

A $[n,k]$ code $\mathbf{C}$ is said to be *cyclic* if the right shift of a codeword $v = v_1 v_2 ... v_n$, i.e. $v' = v_n v_1 ... v_{n-1}$, is also a codeword. A cyclic code has a parity-check matrix in the form $\mathbf{H} = \begin{pmatrix} H_1 \\ \cdots \\ \cdots \\ H_t \end{pmatrix}$, where H_i is a circulant matrix, $\forall$ $i = 1, \ldots, t$. A linear code is said to be *quasi-cyclic* if it has a parity-check matrix in the form $\mathbf{H} = \begin{pmatrix} H_{1,1} & \ldots & H_{1,s} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ H_{t,1} & \ldots & H_{t,s} \end{pmatrix}$, where any $H_{i,j}$ is a circulant matrix.

Let V be a $d+1$ -dimensional vector space over the finite field $GF(q)$, with q a power of a prime number; the lattice of the subspaces of V is the d-dimensional *projective geometry* $\Sigma = PG(d,q)$. The Singer group $S = \langle \sigma \rangle$ is a cyclic group of collineations of Σ that acts regularly on the set of points and hyperplanes of Σ and hence has order $\frac{q^{d+1}-1}{q-1}$. Choose as $d+1$-dimensional vector space over $GF(q)$ the field $GF(q^{d+1})$ and let ξ be a primitive element of $GF(q^{d+1})$; the collineation σ is induced by the application

$$x \in GF(q^{d+1}) \rightarrow \xi x \in GF(q^{d+1}).$$

Labelling the points and the lines of Σ in a suitable way (see Section2 and [8]), the incidence matrix H of such incidence structure is a parity-check matrix of a cyclic code.

4 Hermitian LDPC Codes

We want to introduce a new class of codes arising from linear spaces.

A *correlation* π of $\Sigma = PG(d,q)$ is a permutation of the subspaces which inverts the inclusion, i.e. $S \subseteq T$ implies $S^\pi \supseteq T^\pi$, for any subspace S and T of Σ, and also if S is a $h-$dimensional subspace, then S^π is a $(d-h-1)-$dimensional subspace of Σ. A subspace S is called *totally isotropic*, *isotropic* or *non-isotropic* with respect the polarity π according as $S \cap S^\pi$ is S, nonempty and properly contained in S or empty, respectively. A point (or a hyperplane) is either non-isotropic or totally isotropic, in the latter case it is called *absolute*. A *polarity* is a correlation of order two. A polarity π is said to be a *unitary polarity* if it arises from a non-degenerate reflexive $\sigma-$*sesquilinear form* β of the underling vector space V in the following way

$$S \subseteq V \longmapsto S^\pi = \{u \in V / \beta(u,v) = 0 \ \forall \ v \in S\}$$

and the $\sigma-$sesquilinear form β is *Hermitian*, i.e. σ is the automorphism of $GF(q)$ of order two and $\beta(u,v) = \beta(v,u)^\sigma$, $\forall\, u, v \in V$. The projective space $\Sigma = PG(d,q)$ admits a unitary polarity if and only if q is a square. The set of non-singular linear application f of V into itself such that $\beta(u,v) = \beta(f(u), f(v))$, $\forall\, u, v \in V$, is called the *unitary group* $U(d+1, q^2)$; any element of $U(d+1,q^2)$ induces a collineation of Σ and the set of such collineations is called the *projective unitary group* $PGU(d+1,q^2)$. It is clear that a collineation of $PGU(d+1,q^2)$ maps totally isotropic (respect. isotropic, non-isotropic) subspaces in totally isotropic (respect. isotropic, non-isotropic) ones. From now on let π be a unitary polarity of the plane $PG(2,q^2)$ and denote by $\mathcal{H}(2,q^2)$ the set of absolute points, which is also called the *Hermitian curve*; the set of absolute lines is $\{P^\pi,\ P \in \mathcal{H}(2,q^2)\}$.

The incidence structure $\mathbb{P} = (\mathcal{P}, \mathcal{B}, I)$ that we consider is the following: $\mathcal{P}$ is the set of point of $\mathcal{H}(2,q^2)$, $\mathcal{B}$ is the set of the non isotropic lines and I is the natural incidence relation. The Hermitian curve $\mathcal{H}(2,q^2)$ consists of $n = q^3+1$ points and there are $m = q^2(q^2-q+1)$ non isotropic lines. This incidence structure is a linear space with parameters $s = q$, $t = q^2-1$ and $\alpha = q+1$.

Let $\mathbf{H}$ be the incidence matrix of $\mathbb{P}$: $\mathbf{H}$ is a $m \times n-$ matrix over $GF(2)$, such that any row has weight $q+1$, any column has weight q^2, hence the density is $\frac{1}{q^2-q+1}$. Finally, any two columns have exactly one non-zero component in common and any two rows have at most one non-zero component in common.

Hiss proves in [10] that if q is even, then $rank_2(\mathbf{H}) = q^3+1$, if q is odd, then $rank_2(\mathbf{H}) = q(q^2-q+1)$.

The code, say $\mathbf{C}$ which has $\mathbf{H}^T$ as parity-check matrix is a binary $[m, (q^2-q-1)(q^2-q+1)]$ LDPC code, if q is even, or a binary $[m, (q^2-q)(q^2-q+1)]$ LDPC code, if q is odd.

As the authors discuss in [9], since any two rows of $\mathbf{H}$ have at most one non zero entry in common, $\mathbf{C}$ is capable of correcting any error pattern with $[\frac{1}{2}(q+1)]$ or fewer errors using one step majority-logic decoding and so has minimum distance at least $q+2$ (see also [11]), that is a better lower bound

then the one found in (1).

The Tanner graph has girth 6 and it has $N_6 = \frac{1}{6}n(n-1)(n-q-1)$ cycles of length 6.

In order to prove next results, we need some preliminaries.

Let $\Pi = PG(2, q^2)$ be the projective plane over the finite field $GF(q^2)$. Choose as tree-dimensional vector space over $GF(q^2)$ the field $GF(q^6)$. A point $P = (x)$ of Π, with $x \in GF(q^6) \setminus \{0\}$, is $\{\lambda x, \lambda \in GF(q^2) \setminus \{0\}\}$. The Trace of $GF(q^6)$ over $GF(q^2)$

$$Tr : x \in GF(q^6) \to x + x^{q^2} + x^{q^4} \in GF(q^2)$$

is a non singular linear map and any non singular linear map of $GF(q^6)$ over $GF(q^2)$ is of the type:

$$Tr(u\cdot) : x \in GF(q^6) \to Tr(ux) \in GF(q^2)$$

hence a line $[u]$, with $u \neq 0$, is the set: $\{(x) \in \Pi / Tr(ux) = 0\}$.

As it is showed in [3], the sesquilinear form

$$(x, y) \in GF(q^6) \times GF(q^6) \to Tr(x^{q^3} y)$$

is a non degenerate Hermitian form, so it induces a unitary polarity of Π. The absolute points of such polarity , i.e. the points of the hermitian curve $\mathcal{H}\left(2, q^2\right)$, have equation $Tr(x^{q^3+1}) = 0$.

The Singer group $S = \langle \sigma \rangle$ of Π has order $q^4 + q^2 + 1$ and it is the direct sum of two subgroups: $S_1 = \langle \sigma_1 \rangle$ of order $q^2 + q + 1$ and σ_1 is induced by

$$x \in GF(q^6) \to \xi^{q^2-q+1} x \in GF(q^6)$$

and $S_2 = \langle \sigma_2 \rangle$ of order $q^2 - q + 1$ and σ_2 is induced by

$$x \in GF(q^6) \to \xi^{q^2+q+1} x \in GF(q^6).$$

In [1] it's showed that the point orbits of these two subgroups give arise to two different cyclic partitions of Π:

$$Baer(u) := \left\{ \xi^{u+i(q^2-q+1)} / \ i = 0, ..., q^2 + q \right\}$$

for $u = 0, ..., q^2 - q$ is a cyclic partition of Π into Baer subplanes, and

$$Arc(t) := \left\{ \xi^{t+i(q^2+q+1)} / \ i = 0, ..., q^2 - q \right\}$$

for $t = 0, ..., q^2 + q$ is a cyclic partition of Π into complete arcs. We recall that an arc A of Π is a set of points such that never three are collinear and A is said to be complete if there is no arc which properly contains it. A Baer subplane B is a subplane of Π such that every point (respect. line) of Π is incident with a line (respect. point) of B, and it's well known that if Π has order q^2 then B has order q. For every line ℓ of Π, ther exists one and only one $Baer(u)$ such

that $|\ell \cap Baer(u)| = q+1$ and in this case we say that ℓ contains a Baer subline of $Baer(u)$; for any other $Baer(v) \neq Baer(u)$, we have $|\ell \cap Baer(v)| = 1$ or $q+1$. Let $S_i(\ell)$ be the ℓ orbit under the action of S_i; we note that if ℓ contains a subline of $Baer(u)$, then any other line of $S_1(\ell)$ does and if ℓ is tangent (respect. secant, external) to $Arc(t)$, then any other line of $S_2(\ell)$ is.

In [3], it's showed that S_2 is a subgroup of the unitary group $PGU(3, q^2)$, hence there is a partition of $\mathcal{P}$ into $q+1$ complete arcs and a partition of $\mathcal{B}$ into q^2 orbits under the action of S_2.

Now it is easy to prove the following

Proposition 3 *The code* $\mathbf{C}$ *is quasi-cyclic.*

Proof.

Let $P_1, \ldots, P_{q+1}$ be points of $\mathcal{P}$ and $\ell_1, \ldots, \ell_{q^2}$ be lines of $\mathcal{B}$ that have distinct orbits under the action of S_2. Label the elements of $\mathcal{P}$ in the following way: $P^{((i-1)(q^2-q+1)+j+1)} := P_i^{\sigma_2^j}$, $i = 1, \ldots, q+1$, $j = 0, \ldots, q^2-q$; analogously for the elements of $\mathcal{B}$: $\ell^{((i-1)(q^2-q+1)+j+1)} := \ell_i^{\sigma_2^j}$, $i = 1, \ldots, q^2$, $j = 0, \ldots, q^2-q$. Hence the incidence matrix is $\mathbf{H} = \begin{pmatrix} H_{1,1} & \ldots & H_{1,q+1} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ H_{q^2,1} & \ldots & H_{q^2,q+1} \end{pmatrix}$ and $H_{i,j}$ is a circulant square matrix of order q^2-q+1, $\forall\ i = 1, \ldots, q^2$ and $j = 1, \ldots, q+1$.

■

Let now B_0 be $Baer(0)$ and $C = B_0 \cap \mathcal{H}(2, q^2)$. The following result shows how to find points of $\mathcal{P}$ and lines of $\mathcal{B}$ with distinct orbits under the action of S_2, i.e. *point-starters* and *line-starters* respectively.

Proposition 4 *The points of* C *are point-starters and the lines* $\{[u],\ (u) \in B_0 \setminus C\}$ *are line-starters, in particular, if* q *is even, then* $\{[u],\ (u) \in B_0 \setminus C\} = \{[u]$ *not passing through* (1) *and* $(u) \in B_0\}$.

Proof. In [1], it is proved that $|Arc(0) \cap Baer(u)| = 1\ \forall\ u = 0, ..., q^2-q$ but the same proof can be used to show that $|Arc(t) \cap Baer(u)| = 1\ \forall\ u = 0, ..., q^2-q$ and $t = 0, ..., q^2+q$, hence it is clear that the points of C are starters. For duality, we have that $S_1(\ell) \cap S_2(m)$ consists in one line, for every line ℓ and m of Π, hence the lines of $S_1(\ell) \cap \mathcal{B}$ are starters. The non isotropic lines are $\{\ell = P^\pi$, P non absolute point$\} = \{[u^{q^3}],\ (u) \notin \mathcal{P}\}$. If $\ell = [1]$, then $S_1(\ell) \cap \mathcal{B} = \{[u],\ (u) \in B_0\} \cap \{[u^{q^3}],\ (u) \notin \mathcal{P}\} = \{[u], (u) \in B_0 \setminus C\}$. If q is even, then $\{[u],\ (u) \in B_0 \setminus C\} = \{[u], (u) \in B_0$ and $Tr(u^{q^3+1}) \neq 0\} = \{[u], (u) \in B_0$ and $Tr(u^2) \neq 0\} = \{[u], (u) \in B_0$ and $Tr(u) \neq 0\} = \{[u], (u) \in B_0$ and $(1) \notin [u]\}$.

■

The incidence structure we are considering has $s = q$, i.e. any line passes through $q+1$ points; moreover we recall that the set $\mathcal{P}$ is partitioned into $q+1$ arcs. Next step is to describe how the $q+1$ points of a line are disposed in the $q+1$ arcs (hence we give a description of the submatrices H_{ij}). Fisher et. al. in [6] prove the following two lemmas:

Lemma 5 *If q is even, then $Baer(u) \cap \mathcal{H}(2, q^2)$ is a subline of $Baer(u)$; if q is odd, then $Baer(u) \cap \mathcal{H}(2, q^2)$ is a subconic of $Baer(u)$, $\forall\ u = 0, ..., q^2 - q$.*

Remark 6 *A conic of the plane $PG(2, q)$, q odd, is a set of points represented by the vectors v of a tree dimensional vector space over $GF(q)$, say $V(3, q)$, such that $Q(v) = 0$, for some non degenerate quadratic form Q of $V(3, q)$. All the conics of the plane are projectively equivalent (i.e. there exists a linear collineation that maps one onto the other) and the group of collineations that fix a conic is called the projective orthogonal group $PO(3, q)$. Finally we recall that $PO(3, q)$ is isomorphic to $PGL(2, q)$, the group of linear collineations of the line.*

Lemma 7 *If ℓ contains a subline of $Baer(u)$, then ℓ is tangent to the $q + 1$ arcs that contain the $q + 1$ points of $\ell \cap Baer(u)$.*

Now we prove the following:

Proposition 8 *If q is even, then there exists a unique orbit $S_2(\ell)$ such that any line of $S_2(\ell)$ is tangent to $Arc(t)$, $\forall\ Arc(t) \subset \mathcal{P}$; any other orbit $S_2(m) \neq S_2(\ell)$ is such that any line of $S_2(m)$ is tangent to the same unique arc of $\mathcal{P}$ and secant to the same $\frac{q}{2}$ arcs of $\mathcal{P}$. If q is odd, then there exist $\frac{1}{2}(q + 1)$ orbits $S_2(\ell)$ such that any line of $S_2(\ell)$ is tangent to the same two arcs of $\mathcal{P}$ and secant to the same $\frac{q-1}{2}$ arcs of $\mathcal{P}$; moreover there exist $\frac{1}{2}(q - 1)$ orbits $S_2(m)$ such that any line of $S_2(m)$ is secant to the same $\frac{q+1}{2}$ arcs of $\mathcal{P}$.*

Proof. For any $S_2(\ell)$ consider the unique line that contains a subline of B_0, namely just ℓ. If q is even, than C is a subline and two cases can occur: $\ell \cap C = C$, hence, by lemma7, ℓ is tangent to any arc of $\mathcal{P}$ and any other line of $S_2(\ell)$ is; or $|\ell \cap C| = 1$, hence ℓ is tangent to a unique arc of $\mathcal{P}$ and any other line of $S_2(\ell)$ is tangent to the same arc. If q is odd, then C is a subconic and we have two cases: $|\ell \cap C| = 2$, so ℓ is tangent to two arcs of $\mathcal{P}$ and any other line of $S_2(\ell)$ is tangent to the same arcs; otherwise $\ell \cap C = \emptyset$, hence ℓ is not tangent to any arc of $\mathcal{P}$ and any other line of $S_2(\ell)$ is not. ■

Finally, we prove the "double cyclic structure" of the code $\mathbf{C}$, i.e. we find a circulant display of submatrices H_{ij}.

Proposition 9 *If q is even, then*

$$\mathbf{H} = \begin{pmatrix} I_1 & I_2 & \dots & \dots & \dots & I_{q+1} \\ A_{1,1} & A_{1,2} & \dots & \dots & \dots & A_{1,q+1} \\ A_{1,q+1} & A_{1,1} & \dots & \dots & \dots & A_{1,q} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ A_{1,2} & A_{1,3} & \dots & \dots & \dots & A_{1,1} \\ A_{2,1} & A_{2,2} & \dots & \dots & \dots & A_{2,q+1} \\ A_{2,q+1} & A_{2,1} & \dots & \dots & \dots & A_{2,q} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ A_{2,2} & A_{2,3} & \dots & \dots & \dots & A_{2,1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ A_{q-1,1} & A_{q-1,2} & \dots & \dots & \dots & A_{q-1,q+1} \\ A_{q-1,q+1} & A_{q-1,1} & \dots & \dots & \dots & A_{q-1,q} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ A_{q-1,2} & A_{q-1,3} & \dots & \dots & \dots & A_{q-1,1} \end{pmatrix}$$

where I_i is the identity matrix of order q^2-q+1, $\forall\ i = 1, \dots, q+1$ and A_{ij} is a square circulant matrix of order q^2-q+1, $\forall\ i = 1, \dots, q-1$ and $j = 1, \dots, q+1$.

If q is odd and $r = q+1$, then

$$\mathbf{H} = \begin{pmatrix} A_1 & A_2 & \dots & \dots & \dots & \dots & \dots & A_r \\ B_{1,1} & B_{1,2} & \dots & B_{1,\frac{r}{2}} & B_{1,\frac{r}{2}+1} & B_{1,\frac{r}{2}+2} & \dots & B_{1,r} \\ B_{1,\frac{r}{2}} & B_{1,1} & \dots & B_{1,\frac{r}{2}-1} & B_{1,r} & B_{1,\frac{r}{2}+1} & \dots & B_{1,r-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ B_{1,2} & B_{1,3} & \dots & B_{1,1} & B_{1,\frac{r}{2}+2} & B_{1,\frac{r}{2}+3} & \dots & B_{1,\frac{r}{2}+1} \\ B_{2,1} & B_{2,2} & \dots & B_{2,\frac{r}{2}} & B_{2,\frac{r}{2}+1} & B_{2,\frac{r}{2}+2} & \dots & B_{2,r} \\ B_{2,\frac{r}{2}} & B_{2,1} & \dots & B_{2,\frac{r}{2}-1} & B_{2,r} & B_{2,\frac{r}{2}+1} & \dots & B_{2,r-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ B_{2,2} & B_{2,3} & \dots & B_{2,1} & B_{2,\frac{r}{2}+2} & B_{2,\frac{r}{2}+3} & \dots & B_{2,\frac{r}{2}+1} \\ C_{1,1} & C_{1,2} & \dots & \dots & \dots & \dots & \dots & C_{1,r} \\ C_{1,r} & C_{1,1} & \dots & \dots & \dots & \dots & \dots & C_{1,r-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ C_{1,2} & C_{1,3} & \dots & \dots & \dots & \dots & \dots & C_{1,1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ C_{q-2,1} & C_{q-2,2} & \dots & \dots & \dots & \dots & \dots & C_{q-2,r} \\ C_{q-2,r} & C_{q-2,1} & \dots & \dots & \dots & \dots & \dots & C_{q-2,r-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ C_{q-2,2} & C_{q-2,3} & \dots & \dots & \dots & \dots & \dots & C_{q-2,1} \end{pmatrix}$$

where A_i, $i = 1, \dots, r$, B_{ij}, $i = 1, 2$ and $j = 1, \dots, r$, C_{ij}, $i = 1, \dots, q-2$ and $j = 1, \dots, r$ are square circulant matrices of order $q^2 - q + 1$.

Proof. In the subplane B_0, $PO(3, q) \cong PGL(2, q) \Rightarrow$ in both cases C is a line or a conic, there exists a cyclic group $T = \langle \tau \rangle$ that fixes C and is isomorphic to the Singer group of the line (i.e. $|T| = q+1$ and T acts regularly on the points

of C). $C \hookrightarrow \mathcal{H}(2,q^2) \Rightarrow T$ is a subgroup of $PGU(3,q^2)$. If C is a line, then T fixes C and the point $C^\pi = (1) \in B_0$. In this case, the other line-orbits (in B_0) have all order $q+1$ (see, for example, [8]). If C is a conic of B_0, namely the conic of equation $y^2 = xz$ (see the Remark6), we consider the following isomorphism between $PO(3,q)$ and $PGL(2,q)$: $f \in PGL(2,q)$ represented by $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \phi(f) \in PO(3,q)$ represented by $\phi'(A) \begin{pmatrix} d^2 & 2cd & c^2 \\ bd & ad+bc & ac \\ b^2 & 2ab & a^2 \end{pmatrix}$. Let ξ be a primitive element of $GF(q^2)$ with minimal polynomial $x^2 - x + \eta$, where η is a primitive element of $GF(q)$ (it does exist, see [2]); the collineation that spans the Singer group of the line is represented by

$$S = \begin{pmatrix} 0 & -\eta \\ 1 & 1 \end{pmatrix}$$

hence τ is represented by

$$S' : \phi'(S) = \begin{pmatrix} 1 & 2 & 1 \\ -\eta & -\eta & 0 \\ \eta^2 & 0 & 0 \end{pmatrix}.$$

$\det(S' - \lambda I) = (\eta - \lambda)(\lambda^2 + (2\eta - 1)\lambda + \eta^2)$. The irreducibility of $x^2 - x + \eta$ over $GF(q)$ implies the irreducibility of the polynomial $x^2 + (2\eta - 1)x + \eta^2$ over $GF(q)$, then S' has one eigenvalue $\lambda = \eta$ and eigenspace $V(\eta) = \langle e \rangle = \langle (2, -1, 2\eta) \rangle$.

Hence T fixes the point $P = \langle e \rangle$ and $\ell = P^\pi$, i.e. the line of equation $\eta x + y + z = 0$. Let $Q = \langle v \rangle$, $v = (x, y, -\eta x - y)$, be a point on ℓ, then $S'v^T = ((1-\eta)x + y, -\eta(x+y), \eta^2 x)^T$; hence it is clear that, on ℓ, S' induces a collineation represented by the matrix

$$\begin{pmatrix} 1-\eta & 1 \\ -\eta & -\eta \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -\eta & 0 \end{pmatrix}^2$$

and

$$\begin{pmatrix} 1 & 1 \\ -\eta & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} S \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

This means that T induces on ℓ a group of collineation isomorphic to the subgroup of order $\frac{q+1}{2}$ of the Singer group of the line, hence on ℓ there are two point orbits of order $\frac{q+1}{2}$. Any point not on ℓ and distinct by P can be written in unique way as $\langle v + e \rangle$, with $\langle v \rangle \in \ell$; we have $\tau^k(\langle v + e \rangle) = \langle \xi^{2k} v + \eta^k e \rangle = \langle \xi^{2k} v + \xi^{k(q+1)} e \rangle = \langle v + e \rangle$ if k is at least $q+1$, hence such a point has orbit of order $q+1$. For duality, there are two line orbits of order $\frac{q+1}{2}$ and $q-1$ line orbits of order $q+1$, and one of these is the orbit of the tangent lines to the conic, which not occur in the incidence structure we are considering. Let now P be a fixed point of C and label the point starters in the following way: $P_{i+1} := P^{\tau^i}$, $i = 0, \ldots, q$. If q is even, then there is a line starter, say ℓ_0, that contains the subline C and there are $q-1$ line starters, say $\ell_1, \ldots, \ell_{q-1}$, that contain sublines with distinct orbits under the action of T, then label the line

starters as follows: $\ell^{(0)} := \ell_0$, and $\ell^{((i-1)(q+1)+j+1)} := \ell_i^{\tau^j},\ i = 1, \ldots, q-1$ and $j = 0, \ldots, q$. If q is odd, then there is a line starter, say ℓ_0, that contains the unique subline fixed by T, there are two line starters, say ℓ_1,ℓ_2, that contain sublines with distinct orbits of order $\frac{q+1}{2}$ under the action of T and finally, and there are $q-2$ line starters, say $\ell_3, \ldots, \ell_q$, that contain sublines with distinct orbits of order $q+1$ under the action of T; hence label the line starters as follows: $\ell^{(0)} := \ell_0$, $\ell^{((i-1)(\frac{q+1}{2})+j+1)} := \ell_i^{\tau^j},\ i = 1, 2$ and $j = 0, \ldots, \frac{q-1}{2}$, $\ell^{((i-1)(q+1)+j+1)} := \ell_i^{\tau^j},\ i = 3, \ldots, q$ and $j = 0, \ldots, q$. ■

Remark 10 *We explicitly observe that if q is even, then in order to construct the matrix $\mathbf{H}$ is enough to know the incidence of $q-1$ lines of $S_1([1]) \setminus \{[1]\}$ such that they pass trough a fixed point of C and do not pass trough* (1).

4.1 Extended and shortened codes

The *code-rate* of a $[n, k]$ linear code is $\frac{k}{n}$, hence $\mathbf{C}$ has code-rate $\frac{q^2-q-1}{q^2}$, if q is even, or $\frac{q-1}{q}$, if q is odd. We observe that the higher is q the higher is the code-rate, but considering high values of q implies a high complexity of calculus and longer codes.

Extended and shortening in a suitable way finite-geometry codes, we obtain new good LDPC codes with the same Tenner graph girth, as it is showed in [9]; essentially, we obtain new codes that lack in regularity and in quasi-cyclic structure, but that have higher code-rate.

The column (or row) splitting is a technique employed in [9] for codes deriving from finite geometries, in particular it has been applied on the incidence structure we have considered in [11]. If we split any row of $\mathbf{H}$ in s rows of less weight, then we obtain from $\mathbf{C}$ a new code, say $\mathbf{C}_{ext}$, with sn code-bits and the same number of linearly independent check-sums, hence $\mathbf{C}_{ext}$ has code-rate $\frac{sq^2-q-1}{sq^2}$, if q is even, or $\frac{sq-1}{sq}$, if q is odd.

Let $\mathbf{H}'$ be the matrix obtained by $\mathbf{H}$ deleting a column which corresponds to a point P of $\mathcal{H}(2, q^2)$. The Tanner graph of the code, say $\mathbf{C}_{sh}^1$, which has $(\mathbf{H}')^T$ as parity-check matrix, has $N_6' = \frac{1}{6}n(n-1)(n-q-1) - \frac{1}{2}n(n-q-1)$ cycles of length 6. Moreover, we can delete a row and $q+1$ columns of $\mathbf{H}$, i.e. a line of the incidence structure and the $q+1$ points on it: we obtain a code, say $\mathbf{C}_{sh}^2$, and its Tanner graph has $N_6'' = \frac{1}{3}(m-1)\binom{q}{2}(n-2q-1)$ cycles of length 6. Finally, deleting a column and q^2 rows of $\mathbf{H}$, i.e. a point of the incidence structure and the q^2 lines trough it, we obtain a code, say $\mathbf{C}_{sh}^3$, and its Tanner graph has $N_6''' = \frac{1}{3}(n-1)(m-2q^2+1)\binom{q}{2}$ cycles of length 6.

Actually, there is a gain in the code-rate just in the codes $\mathbf{C}_{ext}$ and $\mathbf{C}_{sh}^1$. In the following, we compare the code-rate of the code $\mathbf{C}$ and the code-rate of the codes obtained by $\mathbf{C}$ shortening or extending $\mathbf{H}$:

	$\mathbf{C}$	$\mathbf{C}_{ext}$	$\mathbf{C}_{sh}^1$	$\mathbf{C}_{sh}^2$	$\mathbf{C}_{sh}^3$
q even	$\frac{q^2-q-1}{q^2}$	$\frac{sq^2-q-1}{sq^2}$	$\frac{(q-1)^2}{q^2-q+1}$	$\geq \frac{q^4-2q^3-q^2-q-1}{(q-1)(q^3+q+1)}$	$\geq \frac{q-2}{q-1}$
q odd	$\frac{q-1}{q}$	$\frac{sq-1}{sq}$	$\geq \frac{q-1}{q}$	$\geq \frac{(q^2-q+1)(q^2-q-1)}{(q^3+q+1)(q-1)}$	$\geq \frac{q^3-2q^2+q-1}{q^2(q-1)}$

	$\mathbf{C}$	$\mathbf{C}_{ext}$	$\mathbf{C}^1_{sh}$	$\mathbf{C}^2_{sh}$	$\mathbf{C}^3_{sh}$
$q=4$,$s=2$	0.6875	0.84375	0.69231	≥ 0.51691	≥ 0.66667
$q=8$,$s=2$	0.85937	0.92969	0.85965	≥ 0.82232	≥ 0.85714
$q=5$,$s=2$	0.8	0.9	≥ 0.8	≥ 0.76140	≥ 0.79
$q=7$,$s=2$	0.85714	0.92857	≥ 0.85714	≥ 0.83713	≥ 0.85374

5 The construction of H

In this section we discuss geometric considerations that allow to construct the matrix $\mathbf{H}$ in a easy way in the particular case of q even (see Remark10).

EVEN CHARACTERISTIC

Let $f(t) = t^3 + \beta t + \alpha$ be a primitive polynomial over $GF(q^2)$ (it exists provided $q \neq 4$, see [2]) and let ξ be a root of $f(t)$ in $GF(q^6)$: ξ is a primitive element of $GF(q^6)$ and $Tr(\xi) := Tr_{GF(q^6)/GF(q^2)}(\xi) = 0$. Choose the set $\{1, \xi, \xi^2\}$ as a basis of the tree-dimensional vector space $GF(q^6)$ over $GF(q^2)$. Let $P = (x)$ and let $\ell = [u]$ be a point and a line respectively of $PG(2, q^2)$, with $x = x_0 + x_1\xi + x_2\xi^2$ and $u = u_0 + u_1\xi + u_2\xi^2 \in GF(q^6)$; from now on we put $P = \langle (x_0, x_1, x_2) \rangle$ and ℓ is the set of points (x_0, x_1, x_2) of equation $u_0x_0 + \alpha u_2x_1 + \alpha u_1x_2 = 0$. The Hermitian curve $\mathcal{H}(2, q^2)$ has equation $x_0^{q+1} + Tr(\xi^{q^3+1})x_1^{q+1} + Tr(\xi^{2q^3+1})x_1x_2^q + Tr(\xi^{q^3+2})x_1^qx_2 + Tr(\xi^{q^3+1})^2x_2^{q+1} = 0$; let ξ^{q^3} be $(0, \lambda, \mu)$, by straightforward calculation we get $Tr(\xi^{q^3+1}) = \mu\alpha$ and $Tr(\xi^{q^3+2}) = \lambda\alpha$, hence the equation of $\mathcal{H}(2, q^2)$ is

$$x_0^{q+1} + \mu\alpha x_1^{q+1} + (\lambda\alpha)^q x_1x_2^q + \lambda\alpha x_1^q x_2 + (\mu\alpha)^2 x_2^{q+1} = 0. \tag{5}$$

The collineation σ that spans the Singer group of $PG(2, q^2)$ is induced by the non singular linear application

$$x = x_0 + x_1\xi + x_2\xi^2 \in GF(q^6) \mapsto x\xi = \alpha x_2 + (x_0 + x_2\beta)\xi + x_1\xi^2 \in GF(q^6)$$

and it is represented by the matrix

$$S = \begin{pmatrix} 0 & 0 & \alpha \\ 1 & 0 & \beta \\ 0 & 1 & 0 \end{pmatrix}$$

Let $S_i = \langle \sigma_i \rangle$, i=1,2, be the two subgroups of the Singer group described in the Section4 ; then σ_1 is represented by S^{q^2-q+1} and σ_2 by S^{q^q+q+1}.

The set $C = \mathcal{H}(2, q^2) \cap Baer(0)$, is a Baer subline of the line [1], hence C has to satisfy the following conditions:

$$\begin{cases} x_0 = 0 \\ x_0^{q+1} + \mu\alpha x_1^{q+1} + (\lambda\alpha)^q x_1x_2^q + \lambda\alpha x_1^q x_2 + (\mu\alpha)^2 x_2^{q+1} = 0 \end{cases}. \tag{6}$$

We can assume that $x_2 = 1$, so x_1 must satisfy:
$\mu\alpha x_1^{q+1} + (\lambda\alpha)^q x_1 + \lambda\alpha x_1^q + (\mu\alpha)^2 = 0 \Leftrightarrow$

$(\mu\alpha x_1 + \lambda\alpha)^{q+1} + (\lambda\alpha)^{q+1} + (\mu\alpha)^3 = 0$.
Since $(\lambda\alpha)^{q+1}+(\mu\alpha)^3 = 0 \in GF(q)\backslash\{0\}$ (otherwise (5) derives from a degenerate Hermitian form) and α is a primitive element of $GF(q^2)$, we can assume that $(\lambda\alpha)^{q+1} + (\mu\alpha)^3 = \alpha^{k(q+1)}$, for a suitable $k \in 1, \ldots, q-1$, so we have

$$x_1 = \lambda\mu^{-1} + \mu^{-1}\alpha^{k-1+i(q-1)}, i = 1, \ldots, q-1.$$

If τ spans the group T (see Proposition9), then the action of τ on C is given by:

$$x_1 \mapsto \lambda\mu^{-1} + \alpha^{q-1}(\lambda\mu^{-1} + x_1)$$

and so τ is represented by the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha^{q-1} & \lambda\mu^{-1}(1+\alpha^{q-1}) \\ 0 & 0 & 1 \end{pmatrix}.$$

Finally, line starters which have distinct orbits under the action of T are the lines that satisfy the following condition:

- $\ell \in S_1([1]) \setminus \{[1]\}$;
- let $P = \langle(0, \overline{x}_1, 1)\rangle$ be a fixed point of C, then ℓ passes trough P and not trough $\langle(1,0,0)\rangle$; such a line ℓ has equation $x_0 + ux_1 + u\overline{x}_1 x_2 = 0$, with $u \neq 0$.

References

[1] E.Boros and T.Szönyi, On the sharpness of a theorem of B. Segre, *Combinatorica*, **6** (1986), 261-268

[2] S.D.Cohen, Primitive elements and polynomials with arbitrary trace, *Disc. Math.*, **83**(1990), No. 1, 1-7

[3] A.Cossidente, On Kestenband-Ebert partition, *J. Comb. Des.*, **5**(1997), No. 5, 367-375

[4] J.Coykendall and J.Dover, Sets with few intersection numbers from Singer subgroup orbits, *European J. Combin.*, **22** (2001), No. 4, 455-464

[5] K.Drudge, On the orbits of Singer groups and their subgroups, *Elec. J. Comb.*,**9** (2002), R15 (eletronic)

[6] J.C.Fisher, J.W.P.Hirschfeld, J.A.Thas, Complete arcs in planes of square order, *Ann. Discr. Math.*, **30** (1986), 243-250

[7] R.G.Gallager, Low-density parity check codes, *IRE Trans. Inform. Theory*, **IT-8**(1962), No.1, 21-28

[8] L.Giuzzi, G.Lunardon and A.Sonnino, LDPC Codes from projective spaces, to appear?

[9] H.Hang, J.Xu, S.Lin and Khaled A.S. Abdel Ghaffar, Codes on Finite Geometries, *IEE Trans. Inf. Theory*, **51** (2005), No. 2, 572-596

[10] G.Hiss, Hermitian function fields, classical unitals and representation of 3-dimensional unitary groups, *Indag. Math. (N.S.)*, **15** (2004), 223-243

[11] S.J.Johnson and S.R.Weller, High-rate LDPC codes from unital designs. In Proceedings of the IEEE Globecom Conference, San Francisco, CA, 1-5 December 2003.

[12] S.J.Johnson and S.R.Weller, Codes for iterative decoding from partial geometries, *IEE Trans. Comm.*, **52** (2004), No. 2, 236-243

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