Small weight codewords in the LDPC codes arising from linear representations of geometries

V. Pepe L. Storme G. Van de Voorde *

Abstract

In this paper, we investigate the minimum distance and small weight codewords of the LDPC codes of linear representations, using only geometrical methods. First we present a new lower bound on the minimum distance and we present a number of cases in which this lower bound is sharp. Then we take a closer look at the cases $T_2^*(\Theta)$ and $T_2^*(\Theta)^D$ with Θ a hyperoval, hence q even, and characterize codewords of small weight. When investigating the small weight codewords of $T_2^*(\Theta)^D$, we deal with the case of Θ a regular hyperoval, i.e. a conic and its nucleus, separately, since in this case, we have a larger upper bound on the weight for which the results are valid.

1 Introduction

The concept of low-density parity check (LDPC) codes was introduced by Gallager [5], and it was shown in [18] that these codes perform well under iterative probabilistic decoding. A binary $LDPC$ code C, in its broader sense, is a linear block code defined by a sparse parity check matrix H, i.e., the number of 1s in H is small compared to the number of 0s in H. When the rows of H have a constant weight ρ and the columns of H also have a constant weight γ, we call C a $(\rho, \gamma) - regular\ LDPC$ code. When LDPC codes are decoded using Gallager's decoding method, their empirical performance is known to be excellent [16], [18]. Early known LDPC codes have been constructed randomly [16],[18]. There are several types of explicit constructions of LDPC codes. One is based on permutation matrices [3], [27]. Others are based on Ramanujan graphs [19],[23], expander graphs [25], and q-regular bipartite graphs [12].

In 2001, Kou et al. [14] examined classes of LDPC codes defined by incidence structures in finite geometries. Since then, other LDPC codes have been produced based on various incidence structures in discrete mathematics and finite geometry (for example, [8],[9],[10],[17],[28],[29]). In particular, Vontobel and Tanner [28] considered the LDPC codes generated by generalized polygons, focusing on generalized quadrangles. They demonstrated that some generalized quadrangle LDPC codes perform well under the sum product algorithm [18]. Later, Liu and Pados [15] showed that all LDPC codes derived from finite classical generalized quadrangles are quasi-cyclic, and they gave the explicit size of the circulant blocks in the parity check matrix. Their simulation results show

*This author's research is supported by the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen).

that several generalized polygon LDPC codes have a powerful bit-error-rate performance when decoding is carried out via low-complexity variants of belief propagation [15]. In [7], the problem of determining the minimum distance of LDPC codes was addressed. Furthermore, Liu and Pados proved in [15] that the binary LDPC codes defined by generalized quadrangles only have codewords of even weight. In this article, we contribute to the problem of finding the minimum distance of LDPC codes defined by the incidence structures $T_2^*(\mathcal{K})$ which are the linear representations of the sets $\mathcal{K}$ in $PG(2,q)$, with $q = p^h$, p prime, $h \geq 1$. We rely on techniques developed by Kim, Mellinger and Storme who investigated the minimum distance of LDPC codes defined by the incidence structures of (dual) classical generalized quadrangles [11].

Acknowledgement: Part of this research was done when the first author was visiting the Incidence Geometry research group of the Department of Pure Mathematics and Computer Algebra at Ghent University. The first author wishes to thank the members of this research group for their hospitality and the financial support offered to her.

2 LDPC codes arising from the linear representation $T_2^*(\mathcal{K})$

Let $\mathcal{K}$ be a set of points in the Desarguesian projective plane $PG(2,q)$ and embed $\pi_\infty = PG(2,q)$ as a hyperplane in $PG(3,q)$. The linear representation $T_2^*(\mathcal{K})$ has as point set the set of points of $AG(3,q) = PG(3,q) \setminus \pi_\infty$, as line set the set of lines of $AG(3,q)$ intersecting π_∞ in a point of $\mathcal{K}$, and it has the natural incidence relation. Each point of $T_2^*(\mathcal{K})$ is incident with $|\mathcal{K}|$ lines and each line is incident with q points. The type of incidence structure we obtain changes according to the choice of $\mathcal{K}$. Let α and β be two strictly positive integers. In the following three cases, $T_2^*(\mathcal{K})$ is a well-known combinatorial structure. References [22],[1] and [2] give more details about the following geometries.

1. If $|l \cap \mathcal{K}| \in \{0, \alpha+1\}$ for all lines l of Π_∞, then $T_2^*(\mathcal{K})$ is a partial geometry $pg(q-1, |\mathcal{K}|-1, \alpha)$. For example, if $\mathcal{K}$ is a hyperoval, then $T_2^*(\mathcal{K})$ is a generalized quadrangle.

2. If $|l \cap \mathcal{K}| \in \{1, \alpha+1\}$ for all lines l of Π_∞, then $T_2^*(\mathcal{K})$ is a semipartial geometry $spg(q-1, |\mathcal{K}|-1, \alpha)$. For example, let $\mathcal{K}$ be the Hermitian curve in $PG(2,q^2)$, then we get a $spg(q^2-1, q^3, q)$.

3. If $|l \cap \mathcal{K}| \in \{\alpha+1, \beta+1\}$ for all lines l of Π_∞, then $T_2^*(\mathcal{K})$ is an (α,β)-geometry.

The incidence matrix of a linear representation $T_2^*(\mathcal{K})$ is a matrix H with rows labelled by the points of $T_2^*(\mathcal{K})$, columns labelled by the lines of $T_2^*(\mathcal{K})$ and $h_{ij} = 1$ if and only if the point P_i is incident with the line ℓ_j and $h_{ij} = 0$ otherwise. Let $s+1$ denote the number of points on a line, and $t+1$ the number of lines through a point of $T_2^*(\mathcal{K})$. For $q = p^h$, p prime, $h \geq 1$, the p-ary linear code with H as parity check matrix is a ($\rho = t+1$,$\gamma = s+1$)-LDPC code of length $q^2|\mathcal{K}|$. On the other hand, the code arising from the dual geometry $T_2^*(\mathcal{K})^D$ of $T_2^*(\mathcal{K})$ is a ($\rho = s+1$,$\gamma = t+1$)-LDPC code of length q^3. In Table 1,

we have denoted by Θ, $\mathcal{B}$, $\mathcal{U}$ and $\mathcal{L}$ a hyperoval, a Baer subplane, a Hermitian curve, and two intersecting lines, respectively, and we have presented the lower bounds on the minimum distance d_{min} of the LDPC codes arising from their linear representations due to the *bit-oriented bound*, the *parity oriented bound* and *Massey's bound* [26].

LDPC code	Order (ρ,γ)	$d_{\min}$
$T_2^*(\Theta)$	($q+2$,q)	$\geq 2q$
$T_2^*(\Theta)^D$	(q,$q+2$)	$\geq 4q$
$T_2^*(\mathcal{B})$	($q+\sqrt{q}+1$,q)	$\geq q+1$
$T_2^*(\mathcal{U})$	($q\sqrt{q}+1$,q)	$\geq q+1$
$T_2^*(\mathcal{L})$	($2q+1$,q)	$\geq q+1$

Table 1: Known results

The main goal of this section is to find the minimum distance of these LDPC codes and to characterize their small weight codewords. The techniques used here are taken from [11] and they are valid for binary LDPC codes, LDPC codes over $\mathbb{F}_q$, or over $\mathbb{F}_p$. The following geometrical property is used to find examples of codewords of small weight. In this way, we can prove that the bounds for $T_2^*(\Theta)$, $T_2^*(\Theta)^D$, Θ a translation hyperoval, and $T_2^*(\mathcal{L})$, for q even, presented in Table 1 are sharp. Moreover, in the cases $T_2^*(\mathcal{B})$ and $T_2^*(\mathcal{U})$, we find larger lower bounds and prove their sharpness.

Let C be the LDPC code defined by $T_2^*(\mathcal{K})$. A codeword $c = (c_1, \ldots, c_n)$ of C is such that cH^T equals 0 and $supp(c)$, which is the set of all non-zero positions of c, defines

($*$) a set S of lines of $T_2^*(\mathcal{K})$ such that every point of $T_2^*(\mathcal{K})$ lies on zero or on at least two lines of S.

If we are considering the dual setting of $T_2^*(\mathcal{K})$, $supp(c)$ defines

($**$) a set S of points of $T_2^*(\mathcal{K})$ such that every line of $T_2^*(\mathcal{K})$ contains zero or at least two points of S.

The conditions ($*$) and ($**$) are necessary conditions, hence we look for codewords of C among the subsets of lines (or points) of $T_2^*(\mathcal{K})$ that satisfy these conditions.

Example 1. *Let π be an affine plane of $PG(3,q)$ that intersects $\mathcal{K}$ in at least two points P and Q, and let S be the set of all the affine lines of π through P and all the affine lines of π through Q. Clearly, every affine point lies in 0 or exactly two lines of S, hence S satisfies condition ($*$). Take the vector c with 1 in the coordinate positions corresponding to the lines through P, with -1 in the coordinate positions corresponding to the lines through Q, and zero in the other positions. The vector c is orthogonal to every row of H, and hence, it is a codeword of weight $2q$ of the code arising from $T_2^*(\mathcal{K})$, with $\mathcal{K}$ arbitrary. Therefore, if q is even and $\mathcal{K}$ is a hyperoval, the lower bound in the first row of Table 1 is sharp.*

Example 2. *Let q be even and let Θ be a regular hyperoval of $PG(2,q)$, $q = 2^h$, $h \geq 1$. We construct a set S of points that satisfies the condition ($**$) using the construction introduced by Segre in [24]. Here we use the coordinate description*

by Pambianco and Storme [20] to construct complete caps. Suppose that the plane at infinity has equation $x_2 = x_3$ and let Θ be the set $\{(t^2, t, 1, 1)|t \in \mathbb{F}_q\} \cup \{(1, 0, 0, 0), (0, 1, 0, 0)\}$. Let S be the set $C_1 \cup C_2 \cup C_1' \cup C_2'$, where $C_1 = \{(t^2, t, 1, 0)|t \in \mathbb{F}_q\}$, $C_2 = \{(t^2, t, 0, 1)|t \in \mathbb{F}_q\}$, $C_1' = \{(t^2 + \mu, t + \mu, 1, 0)|t \in \mathbb{F}_q\}$ and $C_2' = \{(t^2 + \mu, t + \mu, 0, 1)|t \in \mathbb{F}_q\}$, with $\mu \neq 0, 1$. Then every affine line through Θ contains zero or two points of S. More precisely, there are four possibilities for a line that intersects S. A line can intersect C_1 and C_2, or C_1' and C_2', or C_1 and C_1', or C_2 and C_2'. The lines through a point of C_1 and a point of C_2', and the lines through a point of C_1' and a point of C_2 are not in the geometry $T_2^*(\Theta)$.

Let c be the vector with 1 in the coordinates corresponding to the points of $C_1 \cup C_2 \cup C_1' \cup C_2'$, and zero in the other positions. Clearly, the vector c is a vector of the code arising from $T_2^*(\Theta)^D$ of weight $4q$, hence the lower bound of the second row of Table 1 is sharp for Θ a regular hyperoval.

Remark 1. *If we replace t^2 in the descriptions of $\Theta, C_1, C_2, C_1', C_2'$ by t^{2^v}, $\gcd(v, h) = 1$, we obtain similar codewords of weight $4q$ by using translation hyperovals instead of regular hyperovals.*

Remark 2. *In Example 2, we use a set of three translation ovals C_1, C_2, C, through a same point at infinity, and having the same nucleus at infinity, with the property that any line that intersects two of them, intersects the third one. From now on, we denote $(q+1)$-arcs C_1, C_2 satisfying this condition with respect to $\Theta = C$, by* corresponding *$(q+1)$-arcs w.r.t. $T_2^*(\Theta)$.*

Example 3. *Suppose that $\mathcal{K}$ contains a conic C and let S be the set of lines of a hyperbolic quadric $\mathcal{Q}^+(3, q)$ intersecting the plane at infinity in C. Then the set S satisfies condition $(*)$. Let the quadric $\mathcal{Q}^+(3, q)$ be the union of the two reguli $\mathcal{R}_1$ and $\mathcal{R}_2$, and take the vector c with 1 in the coordinate positions corresponding to the lines of $\mathcal{R}_1$, -1 in the coordinate positions corresponding to the lines of $\mathcal{R}_2$, and zero in the other positions. Then the vector c is a codeword of weight $2(q + 1)$.*

In Example 1, we have shown that a set of lines lying in the same plane gives rise to a small weight codeword. The following result shows how most of the small weight codewords of the code derived from $T_2^*(\mathcal{K})$ are due to such a planar configuration.

Proposition 4. *Let $\mathcal{K}$ be an arbitrary set of points at infinity, let $\mathcal{C}$ be the LDPC code arising from $T_2^*(\mathcal{K})$, c a codeword of $\mathcal{C}$ and let S be the set of lines defined by supp(c). If $wt(c) < 2q$, then S is contained in a plane. If $wt(c) = 2q$, then either:*

1. *S consists of $2q$ lines of a hyperbolic quadric having two lines at infinity contained in $\mathcal{K}$,*

or

2. *$S = S_1 \cup S_2$, where S_i, $i = 1, 2$, is a dual q-arc contained in the affine plane π_i, extended by the line at infinity to a dual $(q + 1)$-arc. Let l be $\pi_1 \cap \pi_2$, then S_i, the line at infinity of π_i, and l form a dual hyperoval, $i = 1, 2$, and q is even. If l is not a line of $T_2^*(\mathcal{K})$, then S gives rise to a minimal codeword. On the other hand, if l is a line of $T_2^*(\mathcal{K})$, then*

$c = c' - c''$, *where* c' *is the codeword derived from the dual* $(q+1)$*-arc* $S_1 \cup \{l\}$, c'' *is the codeword derived from the dual* $(q+1)$*-arc* $S_2 \cup \{l\}$ *and* $wt(c') = wt(c'') = q+1$, *where* c' *and* c'' *have the same symbol in their support.*

3. S *consists of* $2q$ *lines in a plane.*

Proof. Let S be the set of lines defined by $supp(c)$, with c a codeword of weight $\leq 2q$ in the LDPC code defined by $T_2^*(\mathcal{K})$. Let π be an affine plane and let $X = \{l_1, \ldots, l_i\}$ be the set of lines of S contained in π. In order to satisfy condition $(*)$, every line of X has at least $q - i + 1$ affine points that lie on a line of $S \setminus X$, hence

$$i(q - i + 1) \leq 2q - i$$

from which we get: $i \geq q$ or $i \leq 2$.

If $i = q$, then the line l_k of X has at least one affine point contained in a line of $S \setminus X$, $\forall k = 1, \ldots, q$, and $|S \setminus X| \leq q$, hence, l_k has exactly one affine point contained in a line of $S \setminus X$ and intersects the lines l_j, $j \neq k$, in different affine points, $\forall j, k = 1, \ldots, q$. If l_∞ is the line at infinity of π, then the set $\{l_\infty, l_1, \ldots, l_q\}$ is a dual $(q+1)$-arc of π. The lines of $S \setminus X$, say $m_1, \ldots, m_q$, must intersect each other in an affine point, hence, they all lie in the same plane π_1 and, using the same arguments, $m_1, \ldots, m_q$, and the line at infinity of π_1, say m_∞, form a dual $(q+1)$-arc. Let l be $\pi \cap \pi_1$; if l is a line of $T_2^*(\mathcal{K})$, then $\{l_\infty, l_1, \ldots, l_q, l\}$ and $\{m_\infty, m_1, \ldots, m_q, l\}$ are two dual hyperovals and they give rise to two codewords of weight $q+1$, say c' and c'', such that $c = c' - c''$. Hence, c' has a scalar α in the coordinate positions of the lines $l_1, \ldots, l_q, l$, and c'' has the same scalar α in the coordinate positions of the lines $m_1, \ldots, m_q, l$. If l is not a line of $T_2^*(\mathcal{K})$ (this happens when $\mathcal{K}$ contains at most q points of a line, for example when $\mathcal{K}$ is a maximal arc of degree q), then the set $\{l_1, \ldots, l_q, m_1, \ldots, m_q\}$ gives rise to a minimal codeword of weight $2q$. Therefore, if $i = q$, then we obtain case 2 of the proposition.

Now suppose that in the case $i \geq q+1$, there exists a line of S, say l, that is not contained in π. This line l has at least $q - 1$ affine points that must lie on a second line of S not contained in π, hence $S \setminus X$ contains at least $q - 1$ lines different from l. This yields

$$|S| = |X| + |S \setminus X| \geq q + 1 + 1 + q - 1 \geq 2q + 1,$$

a contradiction. We conclude that all lines of S are contained in π.

Suppose now that $i = 2$ and let $X = \{l_1, m_1\}$. We also assume that every plane contains at most two lines of S, since otherwise we are forced to the previous case. On the lines l_1 and m_1, there are $2(q-1)$ points that must lie on a line of $S \setminus X$; let $\{l_2, \ldots, l_q\}$ be the lines intersecting m_1 and $\{m_2, \ldots, m_q\}$ be the lines intersecting l_1. Until now, we have already counted $2q$ lines. If there are two lines of $\{l_2, \ldots, l_q\}$, say l_2 and l_3, intersecting in a point, then there exists a plane, say π', that contains $\{m_1, l_2, l_3\}$, but we excluded this possibility.

Now suppose that both in the set $\{l_1, \ldots, l_q\}$ and $\{m_1, \ldots, m_q\}$, the lines are pairwise skew, hence, l_i intersects m_j, $\forall i, j = 1, \ldots, q$; in other words, the lines of the set $\{l_1, \ldots, l_q, m_1, \ldots, m_q\}$ form a hyperbolic quadric intersecting $\mathcal{K}$ in two lines, so we get the case 1 of the proposition.

Finally, if $X = \{l\}$ and P is a point on l, then P is contained in at least a second line of S, say m. It follows that the plane $\pi' = \langle l, m \rangle$ contains at least two lines of S and so we get again one of the previous cases. □

Using Proposition 4, we can derive a new lower bound on the minimum distance of the LDPC code arising from $T_2^*(\mathcal{K})$, with $\mathcal{K}$ arbitrary.

Proposition 5. *Let c be a codeword of weight smaller than or equal to $2q$ in the LDPC code arising from $T_2^*(\mathcal{K})$ and let S be the set of lines defined by supp(c). Suppose that the lines of S all lie in the same plane π and let x be the number of points of $\pi \cap \mathcal{K}$; then we have $wt(c) \geq q + q/(x-1)$.*

Proof. Let $wt(c) = q + k$, with $1 \leq k \leq q$, and let $\pi \cap \mathcal{K} = \{P_1, \ldots, P_x\}$; the average number of lines of S through a point of $\pi \cap \mathcal{K}$ is $(q+k)/x$, hence there exists a point of $\mathcal{K}$, say P_1, through which there pass at least $(q+k)/x$ lines of S. Let l be a line of S through P_1; every affine point of l is contained in at least another line of S, hence, there are at least q lines of S not through P_1. This implies that the following inequality must hold:

$$\frac{q+k}{x} + q \leq q + k,$$

from which we derive $k \geq q/(x-1)$. □

If x is the minimum integer, greater than one such that $x = |\pi \cap \mathcal{K}|$, then the lower bound of the previous proposition is sharp in a number of cases.

1. If $x = 2$, then $wt(c) \geq 2q$. The lower bound is sharp because of Example 1 which always occurs, whatever $\mathcal{K}$ is.

2. If $x = q+1$, then $wt(c) \geq q+1$. Let q be even and let S be a dual $(q+1)$-arc of the plane extended by the line at infinity to a dual $(q+2)$-arc. The codeword c having a constant symbol α in the positions of S has weight $q+1$.

3. If $x = \sqrt{q}+1$, then $wt(c) \geq q + \sqrt{q}$. If q is even, then let S be a dual $(q+\sqrt{q})$-arc of type $(0, 2, \sqrt{q})$ and let the line at infinity be the dual nucleus of the arc. The following example of a $(q+\sqrt{q})$-arc of type $(0, 2, \sqrt{q})$ is based on a construction due to Korchmáros and Mazzocca (see [13]). Then

$$\{(z^2 + z^{2\sqrt{q}}, z, 1) | z \in \mathbb{F}_q\} \cup \{(1, z', 0) | z' \in \mathbb{F}_{\sqrt{q}}\}$$

   is a $(q+\sqrt{q})$-arc of type $(0, 2, \sqrt{q})$ with $(0,1,0)$ as $\sqrt{q}$-nucleus. The points $(z^2 + z^{2\sqrt{q}} = \rho, z, 1)$, with $z \in \mathbb{F}_q$, belong to $X = \rho Z$, for some $\rho \in \mathbb{F}_{\sqrt{q}}$. The points $(1, z', 0)$, with $z' \in \mathbb{F}_{\sqrt{q}}$, are on $Z = 0$. So the $\sqrt{q}$-secants through $(0,1,0)$ are $X = \rho Z$, with $\rho \in \mathbb{F}_{\sqrt{q}}$, and $Z = 0$, and these $\sqrt{q}+1$ lines l_i form a dual Baer subline. When we dualize, this gives a line l_∞ with $P_1, \ldots, P_{\sqrt{q}+1}$ the $\sqrt{q}+1$ points of a Baer subline, where we denoted the dual of the line l_i by P_i.

   There are $\sqrt{q}$ lines of S through every point P_i intersecting all the lines with a different direction in an affine point. Take a vector c with in all these $q + \sqrt{q}$ lines the same symbol, then c is a codeword of $T_2^*(\mathcal{K})$ with weight $q + \sqrt{q}$.

4. In general, the lower bound $q + q/(x-1)$ is sharp if we find a set of lines S that is a dual $(0, 2, t)$-arc of size $q + t$ in $PG(2, q)$ such that the line at infinity is the dual t-nucleus and $t = q/(x-1)$. A result of Gács and Weiner [4] shows that a $(0, 2, t)$-arc of size $q + t$ always has a t-nucleus. If such an arc exists, then q is even, unless $x = 2$.

The following table summarizes the results obtained in the previous part.

LDPC code	Order (ρ,γ)	d_{min}
$T_2^*(\Theta)$	$(q+2,q)$	$2q$
$T_2^*(\Theta)^D$, Θ a translation hyperoval	$(q,q+2)$	$4q$
$T_2^*(\mathcal{B})$, q even	$(q+\sqrt{q}+1,q)$	$q+\sqrt{q}$
$T_2^*(\mathcal{U})$, q even	$(q\sqrt{q}+1,q)$	$q+\sqrt{q}$
$T_2^*(\mathcal{L})$, q even	$(2q+1,q)$	$q+1$

Table 2: New results

So far, we have results for even q. In the general case $T_2^*(\mathcal{K})$, with odd $q = p^h$, we have not been able to determine the minimum weight of the p-ary linear code of $T_2^*(\mathcal{K})$.

In the following proposition, we present a codeword of weight $2q-2$ in the LDPC code of $T_2^*(\mathcal{K})$, where $\mathcal{K}$ contains a Baer subline, which shows that most likely in general, the minimum weight of the p-ary linear LDPC code of $T_2^*(\mathcal{K})$ is smaller than $2q$. Note that the following construction is also valid for q an even square.

Proposition 6. *When $\mathcal{K}$ contains a Baer subline, there exists a codeword of weight $2q-2$ in the p-ary linear code of $T_2^*(\mathcal{K})$, with $q = p^h$ odd, q square.*

Proof. Let L be the Baer subline $PG(1, \sqrt{q})$ at infinity contained in $\mathcal{K}$. In $PG(2, q)$, there exist Baer subplanes B_1 and B_2 which share the Baer subline L and one extra point P_1 (not on the line $\bar{L}$ of $PG(2, q)$, extending L). Then B_1 and B_2 share $\sqrt{q}+2$ lines; namely the line L and the lines through a point of L and P_1. So B_1 has $q-1$ lines not lying in B_2, and B_2 has $q-1$ lines not lying in B_1.

Give all the lines of B_1, not in B_2, symbol 1, and all the lines of B_2, not in B_1, symbol -1. All other lines have symbol zero. We show that this vector gives a codeword of weight $2q-2$.

An affine point not lying in $B_1 \cup B_2$ lies on one line of B_1 and one line of B_2. If these lines are different, they have respectively symbols 1 and -1, so the sum is zero. If these lines coincide, they pass through P_1, so they have symbol zero.

The point P_1 only lies on lines with symbol zero.

A point R of $B_1 \setminus B_2$ lies on $\sqrt{q}$ lines of B_1 not in B_2. The only line through R lying in B_2 is the line RP_1 with symbol zero. So the sum of the symbols is $\sqrt{q} \equiv 0 \bmod p$. Similarly, a point R of $B_2 \setminus B_1$ lies on $\sqrt{q}$ lines of B_2 not in B_1. So the sum of the symbols is $-\sqrt{q} \equiv 0 \bmod p$.

This shows that for any point, the sum of the symbols of lines passing through it equals zero, hence, we have found a codeword. □

In general, if q is odd and if we are considering the binary code arising from $T_2^*(\mathcal{K})$, we know that every codeword has an even weight in virtue of the following result.

Proposition 7. *Let $\mathfrak{I} = (\mathcal{P}, \mathcal{B}, I)$ be a finite incidence structure such that every block contains $s+1$ points, let H be the incidence matrix of $\mathfrak{I}$ (labelling the columns by blocks) and let C be the binary linear code having H as parity check matrix. If $s+1$ is odd, then every codeword of C has an even weight.*

Proof. Let c be a codeword of C and let B be the set of blocks defined by $supp(c)$. Since the code is binary and regarding $(*)$, every point P_i of $\mathcal{P}$ is contained in zero or in an even number of elements of B, say x_i. A double counting argument yields that

$$|B|(s+1) = \sum_i x_i.$$

The right hand side is even, and $s+1$ is odd, so $|B| = wt(c)$ is even. □

3 Small weight codewords in $T_2^*(\Theta)$

In this section, let q be even and let $\mathcal{K}$ be a hyperoval Θ. The linear representation $T_2^*(\Theta)$ is known to be (see [22]) a generalized quadrangle of order $(s,t) = (q-1, q+1)$. The goal of this section is to characterize small weight codewords of the q-ary LDPC code C arising from $T_2^*(\Theta)$, with $q = 2^h$, by using geometrical arguments. The columns of the parity check matrix H correspond to the lines of $T_2^*(\Theta)$, hence a codeword c defines a set S of lines satisfying Property $(*)$, i.e. every affine point is contained in zero or in at least two lines of S. From now on, we denote by the LDPC code of $T_2^*(\Theta)$ (and $T_2^*(\Theta)^D$), the *q-ary* LDPC code of $T_2^*(\Theta)$ (and $T_2^*(\Theta)^D$), where $q = 2^h$.

Proposition 8. *Let C be the LDPC code defined by $T_2^*(\Theta)$, and let S be the set of lines defined by $supp(c)$. If $wt(c) \leq 2(q+1)$, then either:*

1. *S defines a set of $2q$ lines in a plane*

or

2. *S defines a set of $2(q+1)$ lines of a hyperbolic quadric $\mathcal{Q}$, intersecting Θ in a conic.*

Proof. We have already shown in the previous section that the minimum weight of the code C is $2q$ and we have given the geometrical description of a codeword of minimum weight. Moreover, if Θ contains a conic, we have a geometrical description of a codeword of weight $2(q+1)$ (see Example 3). Using the same arguments as in the proof of Proposition 4 yields that this is the only possibility for a codeword c with $2q < wt(c) \leq 2(q+1)$. □

For weights larger than $2(q+1)$, $q = 2^h$, $h \geq 7$, we will characterize the codewords of C, up to weight $2\sqrt[3]{q}(q+1)/3$, as linear combinations of codewords of weight $2q$ and $2(q+1)$ in a similar way as the authors do in [11].

From now on, let c be a codeword of the code C arising from $T_2^*(\Theta)$, $q = 2^h$, $h \geq 7$, let $wt(c) = 2\delta(q+1) \leq 2\sqrt[3]{q}(q+1)/3$ and let S be the set of lines defined by $supp(c)$.

Proposition 9. *For every line l of S, there exists an affine plane π containing l such that π contains at least $2(q-2\delta+1)$ lines of S, or there exists a hyperbolic quadric $\mathcal{Q} \cong \mathcal{Q}^+(3,q)$ containing l and intersecting Θ in a conic, such that each regulus of $\mathcal{Q}$ contains at least $q-4\delta+2$ lines of S.*

Proof. Let l_1 be a line of S. In order to fulfill condition $(*)$, every affine point of l_1 needs to lie on a second line of S; let these lines be $m_1, \ldots, m_q$. The lines m_i do not intersect each other affinely (since $T_2^*(\Theta)$ is a GQ), hence there are $q(q-1)$ affine points on them that must lie on a second line of S. The average number of points of $m_1 \cup \cdots \cup m_q$ on one of the remaining lines is

$$y = \frac{q(q-1)}{(2\delta-1)(q+1)} > \frac{q-2}{2\delta}.$$

Hence, there exists a line l_2 in S that intersects at least y of the lines m_i, say $m_1, \ldots, m_k$, with $k \geq y > (q-2)/(2\delta)$. The lines l_1 and l_2 can be either skew or can intersect at infinity.

Case 1: Assume that the lines l_1 and l_2 intersect at infinity.

Then, the lines $l_1, l_2, m_1, \ldots, m_k$ all lie in the same plane π. Let x and t be the number of the lines of S through the two points of Θ in π, with $x \leq t$. Then there are $t(q-x)+x(q-t)$ affine points on these $x+t$ lines that still must lie on a second line of S. A line not in π can contain at most one affine point of π, so, in order to avoid a contradiction, we must have that

$$t(q-x)+x(q-t) \leq 2\delta(q+1)-x-t, \tag{1}$$

which implies that

$$x+t \leq 2\delta + \frac{2xt}{q+1} < 2\delta + 2x.$$

Let i be $t-x$, then $i < 2\delta$. Replacing t by $x+i$ in (1) yields:

$$2x^2 - 2x(q+1-i) + (2\delta-i)(q+1) \geq 0.$$

Recall that $\delta \leq \sqrt[3]{q}/3$ and that $i < 2\delta$. This implies that $x < \delta + 1/2$ or $x > q - 2\delta + 1$. Since t is at least $k \geq (q-2)/(2\delta)$, $x = t - i$ must be at least $q-2\delta+1$. So there exists a plane π through l_1 containing at least $2(q-2\delta+1)$ lines of S.

Case 2: Assume that the lines l_1 and l_2 are skew.

Hence, there are $k(q-2)$ affine points on the lines $m_1, \ldots, m_k$ that must lie on a second line of S, and the average number of these points on the remaining lines of S is

$$z = \frac{k(q-2)}{(2\delta-1)(q+1)-1} > \frac{(q-2)^2}{4\delta^2(q+1)},$$

hence, there exists a line l_3 of S that intersects $h \geq z > (q-2)^2/(4\delta^2(q+1))$ lines m_i, say $m_1, \ldots, m_h$. The lines l_1, l_2 and l_3 are pairwise skew and they intersect $m_1, \ldots, m_h$ in different points, hence they define a hyperbolic quadric $\mathcal{Q} \cong \mathcal{Q}^+(3,q)$. Suppose that there are x lines of S in the first regulus of $\mathcal{Q}$ and t lines of S in the opposite regulus, with $x \leq t$. On these lines, there are $t(q-x)+x(q-t)$ affine points that must lie on a second line of S. A line not contained in $\mathcal{Q}$ can meet the quadric $\mathcal{Q}$ in at most two points, hence

$$t(q-x)+x(q-t) \leq 4\delta(q+1)-2(x+t) \tag{2}$$

which yields that

$$x + t < 4\delta + 2x. \tag{3}$$

Replacing t by $x + i$ in (2) gives the following inequality

$$2x^2 - 2x(q + 2 - i) + 4\delta(q + 1) - i(q + 2) \geq 0.$$

Recall that $i < 4\delta$ from (3), $\delta \leq \sqrt[3]{q}/3$ and t must be at least $h > (q - 2)^2/(4\delta^2(q + 1))$, so the inequality (2) is only satisfied if $x > q - 4\delta + 2$. This implies that there exists a hyperbolic quadric $\mathcal{Q}^+(3, q)$ that contains at least $q - 4\delta + 2$ lines of S in each of its reguli. □

Proposition 9 implies that the lines of S are contained in planes and hyperbolic quadrics with "many" lines of S in it. Let S be contained in h of those planes and k of those hyperbolic quadrics. Two planes have at most one line in common, and a plane and a hyperbolic quadric have at most two lines in common. Two such hyperbolic quadrics containing at least $2(q - 4\delta + 2)$ lines of S share the same conic contained in Θ; and therefore share at most two lines. So we obtain the following inequality:

$$2h(q - 2\delta + 1) - \frac{h(h-1)}{2} + 2k(q - 4\delta + 2) - (h + k - 1)(h + k) \leq 2\delta(q + 1),$$

which implies that

$$-2(h + k)^2 + (h + k)(4q - 8\delta + 7) - h^2 + 3k - 8\delta k \leq 4\delta(q + 1). \tag{4}$$

Substituting λ for $h + k$, the inequality (4) becomes

$$-2\lambda^2 + 2\lambda(2q - 8\delta + 5) - h^2 + h(8\delta - 3) \leq 4\delta(q + 1). \tag{5}$$

The inequality (5) is satisfied when λ is at most $\lceil \delta \rceil$, where $\lceil x \rceil$ denotes the smallest integer larger than or equal to x. Hence, we have proven the following proposition.

Proposition 10. *The set S is contained in at most $\lceil \delta \rceil$ planes or hyperbolic quadrics sharing at least $2(q-2\delta+1)$ or $2(q-4\delta+2)$ lines with S, respectively.*

We use Proposition 10 to prove the following result.

Proposition 11. *If $X = \{X_1, \ldots, X_k\}$, $k \leq \lceil \delta \rceil$, is the set of planes and hyperbolic quadrics containing S, then each X_i contains at least $2(q - 2k)$ lines of S which are not contained in any X_j, $j \neq i$.*

Proof. Let X_1 be a plane and let l be a line of S in X_1 not contained in $X_2 \cup \cdots \cup X_k$. Then any of the planes or hyperbolic quadrics $X_2, \ldots, X_k$ intersects l in at most two points, hence there are at least $q - 2k$ affine points of l that must be contained in a line of X_1 not contained in X_i, $i \neq 1$. If the line l goes through the point at infinity P of X_1, then these $q - 2k$ lines of X_1 intersecting l go through the other point at infinity of $\Theta \cap X_1$. So in X_1, there are at least $q - 2k$ lines of S not contained in $X_i, i \neq 1$, for any one of the two points at infinity of X_1 in Θ.

If X_1 is a hyperbolic quadric and l a line of S in X_1 not contained in X_i, $i \neq 1$, then, since any plane or hyperbolic quadric intersects l in at most two points, the same arguments show that for every regulus in X_1, there are at least $q - 2k$ lines of S not contained in $X_i, i \neq 1$. □

Remark 3. *It follows from the proof of Proposition 11 that a line l_1 in S, contained in X_i and not contained in X_j, $j \neq i$, contains at least $q-2\lceil\delta\rceil$ points that lie on exactly one other line l_2 of S, and that this line l_2 is contained in X_i, but not in X_j, $j \neq i$.*

Using the same techniques as in [11], we will characterize the codewords of small weight as being linear combinations of codewords of weight $2q$ and $2(q+1)$.

Proposition 12. *In the LDPC code defined by $T_2^*(\Theta)$, $q = 2^h$, $h \geq 7$, every codeword of weight at most $2\sqrt[3]{q}(q+1)/3$ is a linear combination of codewords of weight $2q$ or $2(q+1)$.*

Proof. We will prove this by induction on the weight of the codewords. Let c be a codeword of C of weight $2\delta(q+1)$, $\delta \leq \sqrt[3]{q}/3$, and assume that all the codewords of C of weight smaller than $wt(c)$ have already been characterized as being linear combinations of codewords of weight $2q$ and $2(q+1)$.

Let S be the set of lines defined by $supp(c)$ and let l_1 be a line of S contained in X_1 and not contained in X_j, $j \neq 1$. According to Remark 3, there exist h points $R_1, \ldots, R_h$, with $h = q - 2\lceil\delta\rceil$, on l_1 lying on exactly two lines of S, the line l_1 and another line of X_1. Denote the second line of S through R_i by l_{i+1}.

Every point R_i, $i \leq h$, defines a row of the parity check matrix H and since a codeword has to be orthogonal to every row of H, the codeword c has (up to a scalar multiple) 1 in the position corresponding to l_1 and 1 in the positions corresponding to the lines $l_{i+1}, i = 1, \ldots, h$. The lines l_{i+1} intersect l_1, hence, if X_1 is a plane, then they are lines through an other point at infinity with respect to l_1. If X_1 is a hyperbolic quadric, then the lines l_{i+1} belong to the opposite regulus of the one containing l_1. Therefore, there are m lines, $l_{q-2\lceil\delta\rceil+k}, k = 2, \ldots, m+1$, with $m = q - 2\lceil\delta\rceil - 1$, through the same point at infinity as l_1 or in the same regulus of l_1 that belong only to X_1. A line $l_{q-2\lceil\delta\rceil+k}$ can intersect the $X_j, j > 1$, in at most $2\lceil\delta\rceil$ points (see Remark 3), hence, there exists a line among $l_2, \ldots, l_{q-2\lceil\delta\rceil+1}$ that intersects $l_{q-2\lceil\delta\rceil+k}$ in a point not belonging to $X_i, i > 1$. Repeating the same arguments yields that the codeword c has 1 in the positions corresponding to $l_1, l_{q-2\lceil\delta\rceil+k}$, with $k = 2, \ldots, m+1$, and 1 in the positions corresponding to $l_{i+1}, i = 1, \ldots, q-2\lceil\delta\rceil$. If X_1 is a hyperbolic quadric, then Θ is a regular hyperoval since it contains already at least $q-4\delta+2$ points of a conic [6, Lemma 8.9]. Let now c' be the codeword defined by taking all symbols in the positions corresponding to lines of X_1 equal to 1, then c and c' share at least $2q-2\lceil\delta\rceil$ non-zero positions and symbols, so $wt(c-c') < wt(c)$. The induction hypothesis states that $c-c'$ is a linear combination of codewords of weight $2q$ and $2(q+1)$. Hence, $c = (c-c') + c'$ is a linear combination of such codewords too. □

4 $T_2^*(\Theta)^D$, with Θ a non-regular translation hyperoval

In Sections 4 and 5, we characterize codewords of small weight of the LDPC code of $T_2^*(\Theta)^D$ with Θ a translation hyperoval, hence, q is even. This is motivated by the fact that the dual of a GQ $T_2(\Theta)$, Θ a translation oval, is again a $T_2(\Theta')$, for Θ' a translation oval. This will lead to easy descriptions of $T_2^*(\Theta)^D$, Θ a translation hyperoval.

We investigate the small weight codewords of the dual generalized quadrangle $T_2^*(\Theta)^D$ using property $(*)$. Hence, we are able to use the methods developed in Section 3. But to use these results, a detailed description of $T_2^*(\Theta)^D$ is needed.

Here we distinguish between the cases Θ a non-regular translation hyperoval (Section 4) and Θ a regular hyperoval, i.e. a conic and its nucleus (Section 5).

4.1 Describing $T_2^*(\Theta)^D$, with Θ a translation hyperoval

In this section, we explicitly describe the dual generalized quadrangle $T_2^*(\Theta)^D$. This description relies on the results of Payne and Thas [22, p. 174].

Let Θ be the translation hyperoval

$$\left\{(1, x, x^\beta) | x \in \mathbb{F}_q\right\} \cup \{(0,0,1),(0,1,0)\},$$

with β a generator of $\mathrm{Aut}(\mathbb{F}_q)$, embedded in the plane $X_0 = 0$ of $PG(3,q)$.

Proposition 13. *$T_2^*(\Theta)^D$ can be described as an incidence structure $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ with*

$$\mathcal{P} = \begin{cases} \textit{Affine points of } T_2^*(\Theta). \\ \textit{Affine planes through } (0,0,1,0) \textit{ and } (0,1,a,a^\beta), a \in \mathbb{F}_q. \\ \textit{Affine planes through } (0,0,0,1) \textit{ and } (0,1,a,a^\beta), a \in \mathbb{F}_q. \end{cases}$$

$$\mathcal{L} = \quad \textit{Affine lines through the points } (0,1,a,a^\beta) \textit{ of } \Theta.$$

$$\mathcal{I} = \begin{cases} \textit{An affine point lies on an affine line if the point lies on that line.} \\ \textit{An affine plane } \Pi \textit{ through } (0,1,a,a^\beta), \textit{ and } (0,0,0,1) \textit{ or } (0,0,1,0), \\ \textit{ is incident with the affine lines of } \Pi \textit{ through } (0,1,a,a^\beta). \end{cases}$$

Proof. Consider the mapping ϕ with $\phi(1,a,b,c) = \langle (1,0,c,b^\beta), (0,1,a,a^\beta)\rangle$. Then ϕ is obviously a bijection that maps points onto objects that will be the lines of the geometry $T_2^*(\Theta)^D$. From this definition, we get that $\mathcal{L}$ consists of all affine lines through the points $(0,1,u,u^\beta), u \in \mathbb{F}_q$.

We determine the image of the lines of $T_2^*(\Theta)$ under ϕ, since this will be the points of $T_2^*(\Theta)^D$.

A line $\langle (0,0,0,1),(1,a,b,c)\rangle$ through $R = (0,0,0,1)$ corresponds to the set

$$\left\{\langle (1,0,c+\lambda,b^\beta),(0,1,a,a^\beta)\rangle | \lambda \in \mathbb{F}_q\right\}.$$

All lines of this set are contained in a plane π_1 through $(0,0,1,0)$ and $(0,1,a,a^\beta)$, so we can identify this set of lines with π_1.

A line $\langle (0,0,1,0),(1,a,b,c)\rangle$ through $N = (0,0,1,0)$ corresponds to the set

$$\{\langle (1,0,c,b^\beta+\lambda^\beta),(0,1,a,a^\beta)\rangle | \lambda \in \mathbb{F}_q\}.$$

All lines of this set are contained in a plane π_2 through $(0,0,0,1)$ and $(0,1,a,a^\beta)$, so we can identify this set of lines with π_2.

A line through $(1,a,b,c)$ and $(0,1,u,u^\beta)$ corresponds to the set

$$\left\{\langle (1,0,c+\lambda u^\beta, b^\beta+\lambda^\beta u^\beta),(0,1,a+\lambda,a^\beta+\lambda^\beta)\rangle | \lambda \in \mathbb{F}_q\right\}.$$

Note that the lines of this set all pass through the point P with coordinates $(1,u^\beta,c+au^\beta,b^\beta+u^\beta a^\beta)$. So we can identify this set of lines with the point P.

Using these relations, it is clear that ϕ maps collinear points to intersecting lines, and intersecting lines to collinear points. □

4.2 Codewords of small weight in $T_2^*(\Theta)^D$

Theorem 14. *The minimum weight of the LDPC code of $T_2^*(\Theta)^D$, with Θ a translation hyperoval, is equal to $4q$. The minimum weight vectors correspond to the scalar multiples of incidence vectors of a set of all lines of $T_2^*(\Theta)^D$ in two planes, where these two planes pass through the same line at infinity.*

We immediately present the proof for codewords of weight $\leq 2\delta q$, with $\delta \leq \sqrt[3]{q}/3$, to avoid a too detailed repetition of the techniques of Section 3, and to build up already to Theorem 15.

Throughout this proof, we use $R = (0, 0, 0, 1)$ and $N = (0, 0, 1, 0)$. Let S be the set of lines defined by $supp(c)$, with c a codeword of the LDPC code of $T_2^*(\Theta)^D$.

Proof. Codewords of the LDPC code of $T_2^*(\Theta)^D$ satisfy Property $(*)$, hence the codeword corresponds to a set S of lines such that every point lies on zero or on at least two of them. There is only one kind of lines in $T_2^*(\Theta)^D$, the affine lines through the points with coordinates $(0, 1, u, u^\beta)$, and there are three kinds of points of $T_2^*(\Theta)^D$ that have to lie on zero or on at least two lines of S.

A: The affine points.

When we only use the condition that every affine point has to lie on zero or on at least two lines, we can copy the proof for the LDPC code of $T_2^*(\Theta)$. In that case, the minimum weight of the code equals $2q$ and this weight occurs when taking all lines of $T_2^*(\Theta)$ in a fixed plane.

For every line l of S, there are two possibilities: either there exists a plane through l with at least $2(q - 2\delta + 1)$ lines of S, or there is a hyperbolic quadric through l with at least $2(q - 4\delta + 1)$ lines of S. But in this case, there are no codewords consisting of hyperbolic quadrics, since there is no conic lying at infinity in Θ. So the initial description of the codewords becomes: *Every possible codeword of weight $\leq 2\delta q$, with $\delta \leq \sqrt[3]{q}/3$, in $T_2^*(\Theta)^D$ is a linear combination of codewords of $T_2^*(\Theta)$ of weight $2q$, consisting of the $2q$ lines of $T_2^*(\Theta)$ in a plane containing two points $(0, 1, u, u^\beta)$ and $(0, 1, v, v^\beta)$.* All lines in such a plane have a fixed symbol in the corresponding codeword.

We still need to investigate which extra conditions the other two kinds of points of $T_2^*(\Theta)^D$ impose.

B: The points coming from tangent planes to Θ (planes through $(0, 0, 1, 0)$).

Each tangent plane through a point $(0, 1, u, u^\beta)$ has to contain zero or at least two lines. Case A implies that the possible codewords of $T_2^*(\Theta)^D$ of weight $\leq 2\delta q$ are linear combinations of codewords of weight $2q$ of $T_2^*(\Theta)$ in planes through two points $(0, 1, u, u^\beta)$ and $(0, 1, v, v^\beta)$. Take a codeword of weight $2q$, lying in the plane π, then the tangent planes at $\pi \cap \Theta$ contain only one line of S. So at least two codewords of $T_2^*(\Theta)$ (in planes π_1 and π_2) are needed to construct a codeword. Now there are three possibilities.

- The intersection of $\pi_1 \cap \Theta$ and $\pi_2 \cap \Theta$ is empty. In this case, in each of the points of $\pi_1 \cap \Theta$ and $\pi_2 \cap \Theta$, their tangent planes through N contain only one line, a contradiction.

- There is exactly one intersection point in common in $\pi_1 \cap \Theta$ and $\pi_2 \cap \Theta$. In this case, for the two non-common intersection points, a tangent plane through them contains only one line, a contradiction.
- The two intersection points of $\pi_1 \cap \Theta$ and $\pi_2 \cap \Theta$ coincide.

The only possibility for a codeword consisting of two codewords of $T_2(\Theta)$, hence a codeword of weight $4q$, is a codeword arising from two planes π_1 and π_2 through the same points at infinity of $\Theta \backslash \{R, N\}$.

C: The points coming from planes through $(0,0,0,1) = R$ and a point of $\Theta \backslash \{R, N\}$.

Take a possible codeword found in Case B. Then S has two lines in common with the planes through R and the intersection points of the planes π_1 and π_2 with Θ. Furthermore, S has zero lines in common with planes through R and a different point of Θ. So the possible codeword of weight $4q$ does occur if we take the same symbol for the lines in the two planes π_1 and π_2. □

Theorem 15. *The codewords of the LDPC code of $T_2^*(\Theta)^D$, $q = 2^h$, $h \geq 7$, of weight $2\delta q$, with $\delta \leq \sqrt[3]{q}/3$, are linear combinations of codewords of $T_2^*(\Theta)$, with weight $2q$, which are coming from $2q$ lines in planes through two points of $\Theta \backslash \{R, N\}$, where the sum of the symbols of the lines through a point of $\Theta \backslash \{R, N\}$ has to be zero.*

Proof. From Case A, we derive that every codeword of weight at most $2\delta q$, with $\delta \leq \sqrt[3]{q}/3$, is a linear combination of codewords of $T_2^*(\Theta)$ with weight $2q$. Cases B and C yield the second condition, so that the sum of the symbols in the coordinate positions corresponding to the lines in each tangent plane to the q-arc $\Theta \backslash \{R, N\}$ equals zero. □

Remark 4. *Even though we use linear combinations of codewords of weight $2q$ of $T_2^*(\Theta)$, there are no codewords of weight $2q$ in $T_2^*(\Theta)^D$ (see Theorem 14).*

Remark 5. *The condition that the sum of the symbols in the coordinate positions corresponding to the lines in each tangent plane has to be zero is necessary. A set of all lines of $T_2^*(\Theta)^D$ in two planes π_1 and π_2 through the same points at infinity of $\Theta \backslash \{R, N\}$, with all lines in π_1 symbol a and all lines in π_2 symbol $b \neq a$ satisfies the condition that every point of $T_2^*(\Theta)^D$ lies on zero or on at least two lines of this set, but it is not a codeword of the LDPC code of $T_2^*(\Theta)^D$.*

Remark 6. *It is sufficient to make the assumption that the sum of the symbols in the coordinate positions corresponding to the lines in one kind of tangent planes, i.e. either through R or through N, equals zero. In the proof, we use the planes through N.*

4.3 Codewords of small weight in the LDPC code of $T_2^*(\Theta)^D$, with Θ a non-regular translation hyperoval, described in terms of $T_2^*(\Theta)$

In this section, the codewords of small weight in the LDPC code of $T_2^*(\Theta)^D$ are characterized by dualizing the results about the codewords of $T_2^*(\Theta)^D$, so that they are described in the original setting of $T_2^*(\Theta)$. We first have a closer look

at the duality ϕ^{-1}, where ϕ is the bijection between $T_2^*(\Theta)^D$ and $T_2^*(\Theta)$ defined in the proof of Proposition 13. When $\phi(x) = y$, or $\phi(x) = y$, then x and y are called *corresponding*.

Proposition 16. *The duality ϕ^{-1} maps lines of $T_2^*(\Theta)^D$ through the same point at infinity to points in the same plane in $T_2^*(\Theta)$.*

Proof. The line passing through $(1, 0, x, y^\beta)$ and $(0, 1, a, a^\beta)$ is mapped by ϕ^{-1} to the point $(1, a, y, x)$. So all lines of $T_2^*(\Theta)^D$ through $(0, 1, a, a^\beta)$ are mapped to points lying in the plane $aX_0 + X_1 = 0$. □

Proposition 17. *All planes in $T_2^*(\Theta)$ with points corresponding to lines in $T_2^*(\Theta)^D$ contain the points $R = (0, 0, 0, 1)$ and $N = (0, 0, 1, 0)$.*

Proof. As seen in Proposition 16, all these planes have equation $\alpha X_0 + X_1 = 0$, hence contain the points R and N. □

Proposition 18. *The duality ϕ^{-1} maps q coplanar lines of $T_2^*(\Theta)^D$ through a point $(0, 1, u, u^\beta), u \in \mathbb{F}_q$, to a q-arc in a plane through R and N.*

Proof. All points of the plane Π through $(0, 1, u, u^\beta)$, $(0, 1, v, v^\beta)$ and $(1, 0, a, b^\beta)$ have coordinates $(1, \lambda + \mu, a + \lambda u + \mu v, b^\beta + \lambda u^\beta + \mu v^\beta)$.

It follows that the affine lines through $(0, 1, u, u^\beta)$ and the q points $(1, 0, a + \lambda(u + v), b^\beta + \lambda(u^\beta + v^\beta))$, $\lambda \in \mathbb{F}_q$, in Π are mapped to the q points $(1, u, b + \lambda^{\beta^{-1}}(u + v), a + \lambda(u + v))$, with $\lambda \in \mathbb{F}_q$. It is easy to see that this set forms a q-arc. From Proposition 17 and 18, we get that this q-arc lies in the plane $uX_0 + X_1 = 0$ through R and N. □

Proposition 19. *Under the duality ϕ^{-1}, $2q$ coplanar lines in $T_2^*(\Theta)^D$ correspond to two corresponding q-arcs in two planes through RN.*

Proof. Consider $2q$ lines of $T_2^*(\Theta)^D$ lying in the same plane, say π. The preceding propositions tell us that these $2q$ lines correspond to a set B which is the union of two sets of q points, each set lying in a plane through R and N. Proposition 18 states that these sets form q-arcs. The duality ϕ^{-1} gives us the following correspondences.

By Proposition 13, a line through R in $T_2^*(\Theta)$ corresponds to a tangent plane in $T_2^*(\Theta)^D$ (which is a point of $T_2^*(\Theta)^D$); a line through N in $T_2^*(\Theta)$ corresponds to a plane through R in $T_2^*(\Theta)^D$ (which is a point of $T_2^*(\Theta)^D$).

A tangent plane in $T_2^*(\Theta)^D$ through one of the intersection points of π with Θ, say P, contains only one line. So a line through R in the plane defined by P in $T_2^*(\Theta)$ contains only one point of B. The affine planes through R and P contain only one line of π of $T_2^*(\Theta)^D$, so, applying ϕ^{-1}, every line through N in $T_2^*(\Theta)$ in the plane defined by P contains only one point of B. The same holds for the plane defined by the other intersection point of π with Θ.

We are taking q points in the two planes through RN containing the set B that form q-arcs. The points R and N only lie on tangents to these q-arcs, so R and N extend these q-arcs to $(q + 2)$-arcs.

The two sets of coplanar concurrent lines in $T_2^*(\Theta)^D$ are such that a point lies on zero or exactly two lines of this set. So a line of $T_2^*(\Theta)$ not through R or N contains zero or exactly two points of B. Connecting a point of $\Theta \backslash \{R, N\}$ with the q points of one q-arc gives rise to the q-arc in the second plane through RN and vice versa. So the two q-arcs are corresponding ones (see Remark 2). □

Notation: If the points of a set X (e.g. a q-arc) all have the same symbol α in the corresponding codeword of the LDPC code of $T_2^*(\Theta)^D$, then we say briefly that this set X has symbol α.

Theorem 20. *The codewords of the LDPC code of $T_2^*(\Theta)^D$, $q = 2^h$, $h \geq 7$, described in terms of points and lines of $T_2^*(\Theta)$, with weight $\leq 2\sqrt[3]{q}q/3$, are linear combinations of incidence vectors of 2 corresponding q-arcs with the same symbol, each in a plane through RN, such that the sum of the symbols on a line of $T_2^*(\Theta)$ is zero. In particular, the sum of symbols of q-arcs in a fixed plane through RN, is zero. The minimum weight is equal to $4q$, corresponding to 2 sets of corresponding q-arcs, lying in 2 planes through RN.*

Proof. This is the dual of Theorems 14 and 15, using Propositions 16, 17, 19 to dualize. □

5 $T_2^*(\Theta)^D$, with Θ a regular hyperoval

5.1 Describing $T_2^*(\Theta)^D$, with Θ a regular hyperoval

In this section, we use the same strategy as in Section 4 to characterize codewords of small weight in the LDPC code of $T_2^*(\Theta)^D$, with Θ a regular hyperoval, i.e. the union of a conic and its nucleus. The fact that Θ is a regular hyperoval will enable us to discuss codewords up to weight $4q^{3/2}/5$. We find a description of $T_2^*(\Theta)^D$ by using the following construction by Payne and Thas [21],[22].

Let $S = GQ(s) = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ and let x be a regular point, i.e. a point for which $|\{x,y\}^{\perp\perp}| = s+1$, for all points $y \neq x$. Then the following incidence structure $(\mathcal{P}', \mathcal{B}', \mathcal{I}')$ is a $GQ(s-1, s+1)$.
$\mathcal{P}' = \mathcal{P} \backslash x^{\perp}$
$\mathcal{L}' = \begin{cases} \text{The lines of } \mathcal{L} \text{ not through } x. \\ \text{The hyperbolic lines } \{x,y\}^{\perp\perp}, x \nsim y. \end{cases}$
$\mathcal{I}' =$ Natural incidence.

Applying the preceding construction on $T_2(\Theta')$, Θ' a conic, gives $T_2^*(\Theta)$ for Θ the regular hyperoval containing Θ'. Note that $T_2(\Theta')$ is isomorphic to $Q(4,q)$, so we can describe $T_2^*(\Theta)$ on $Q(4,q)$. Then $T_2^*(\Theta)$ is the following incidence structure $(\mathcal{P}, \mathcal{L}, \mathcal{I})$. Let P be a fixed point of $Q(4,q)$.
$\mathcal{P} =$ The points of $Q(4,q)$ not on $P^{\perp}$.
$\mathcal{L} = \begin{cases} \text{The lines of } Q(4,q) \text{ not through } P. \\ \text{The conics } C = \pi \cap Q(4,q) \text{ where } \pi \text{ is a plane through } \langle N, P \rangle, \\ \text{ with } N \text{ the nucleus of } Q(4,q). \end{cases}$
$\mathcal{I} =$ Natural incidence.

We want to characterize small weight codewords of the LDPC code of $T_2^*(\Theta)^D$, so the problem is again to find sets S of lines such that every point of $T_2^*(\Theta)^D$ lies on zero or on at least two lines of S in $T_2^*(\Theta)^D$.

We dualize the incidence structure of $T_2^*(\Theta)$ described on $Q(4,q)$. Since $Q(4,q)$, with q even, is self-dual (see e.g. [22]), the point P becomes a line L, and conics become reguli. So $T_2^*(\Theta)^D$ described on $Q(4,q)$ is an incidence structure $(\bar{\mathcal{P}}, \bar{\mathcal{L}}, \bar{\mathcal{I}})$ with

$\bar{\mathcal{P}} = \begin{cases} \text{The points of } Q(4,q) \text{ not on } L. \\ \text{The reguli through } L. \end{cases}$
$\bar{\mathcal{L}} =$ The lines of $Q(4,q)$ not in $L^{\perp}$.
$\bar{\mathcal{I}} =$ Natural incidence.

5.2 Codewords of small weight in $T_2^*(\Theta)^D$, with Θ a regular hyperoval

From now on, let c be a codeword of the LDPC code C arising from $T_2^*(\Theta)^D$, let $wt(c) \leq 4\delta q$, with $\delta \leq \sqrt{q}/5$, and with $q = 2^h$, $h \geq 5$, and let S be the set of lines defined by $supp(c)$.

Proposition 21. *For every line l of S, there exists a hyperbolic quadric $\mathcal{Q} \cong \mathcal{Q}^+(3,q)$ of $Q(4,q)$, containing l and such that each regulus of $\mathcal{Q}$ contains at least $q - 4\delta + 5/2$ lines of S.*

Proof. The proof is similar to that of Proposition 9. □

Proposition 22. *The set S is contained in at most $2\delta + 1$ hyperbolic quadrics of $Q(4,q)$, each one containing at least $2(q - 4\delta + 5/2)$ lines of S.*

Proof. Two hyperbolic quadrics of $Q(4,q)$ share at most two lines and a hyperbolic quadric contains at most q lines of S in each regulus because the lines of S do not intersect L. In case there are J distinct hyperbolic quadrics, each one containing at least $2(q - 4\delta + 5/2)$ lines of S, we see that

$$|S| \geq \sum_{i=0}^{J-1} (2q - 8\delta + 5 - 2i).$$

Filling in $J = 2\delta + 2$ and using $\delta \leq \sqrt{q}/5$ yields a contradiction. So it follows that $J \leq 2\delta + 1$. □

Theorem 23. *The minimum weight of the LDPC code of $T_2^*(\Theta)^D$, Θ a regular hyperoval, is $4q$ and the codewords of weight $4q$ correspond to two hyperbolic quadrics of $Q(4,q)$, intersecting in two lines m_1, m_2, such that m_1, m_2 intersect L in the same point, where the hyperbolic quadrics have the same symbol in the corresponding codeword.*

Proof. We immediately present the proof for codewords of weight $\leq 4q^{3/2}/5$, to avoid a too detailed repetition of the techniques of Section 3, and to build up already to Theorem 24.

The lines of S lie in at most $2\delta + 1$ hyperbolic quadrics of $Q(4,q)$, with in each regulus at least $q - 4\delta + 5/2$ lines of S. If $X = \{\mathcal{Q}_1, \ldots, \mathcal{Q}_k\}$, $k \leq 2\delta + 1$, is the set of hyperbolic quadrics of $Q(4,q)$ containing S, then each $\mathcal{Q}_i$ contains at least $2q - 12\delta + 4$ lines of S which are not contained in any $\mathcal{Q}_j$, $j \neq i$. In particular, $\mathcal{Q}_1$ contains at least $2q - 8\delta + 4 - 4\delta$ lines of S not contained in $\mathcal{Q}_j$, $j \neq 1$. Each of these lines contains at least $q - 4\delta$ points of $Q(4,q) \cap \bar{\mathcal{P}}$ lying only in $\mathcal{Q}_1$. Take such a line l_1 and suppose that it has symbol 1 in the codeword c. Then there are at least $q - 4\delta$ lines of the opposite regulus of $\mathcal{Q}_1$ having symbol 1. Note that we are not using the secant to L of this opposite regulus.

The other $q - 6\delta + 1$ lines of S only lying in the regulus of $\mathcal{Q}_1$ through l_1 can intersect already chosen lines of S in the opposite regulus of $\mathcal{Q}_1$ with symbol

1 in a point not only lying on $\mathcal{Q}_1$, but this can happen at most 4δ times for a line. Since $q - 4\delta > 4\delta$, there is for each of these $q - 6\delta + 1$ lines a point only lying on this line, and on an already chosen line of S in the opposite regulus of $\mathcal{Q}_1$ with symbol 1. We can conclude that all these $q - 6\delta + 1$ lines of S only lying in the regulus of $\mathcal{Q}_1$ through l must have symbol 1 in the codeword. So we have in total already $2q - 10\delta + 2$ lines in $\mathcal{Q}_1$ with symbol 1.

The line L intersects $\mathcal{Q}_1$ in a point P, and the sum of the symbols of the lines of $T_2^*(\Theta)^D$ through the points on the two lines l_1 and l_2 of $\mathcal{Q}_1$ through P has to be zero. There are points on l_1 and l_2 that lie only on a line with symbol 1 of $\mathcal{Q}_1$, so these points lie on at least one other quadric $\mathcal{Q}_i$, $i > 1$.

This shows that to obtain a codeword of minimal weight, we have to take at least two hyperbolic quadrics in $Q(4, q)$. Then the second hyperbolic quadric has also symbol 1 in most of its lines and passes through l_1 and l_2, and since we are only using two quadrics, they both have symbol 1 in all of their lines not lying in $L^\perp$. Since in every point, the sum of the symbols of the lines of S through it is zero, it is possible that this set is a codeword of $T_2^*(\Theta)^D$. But to make sure this set is a codeword, we have to check the other kind of points, the reguli through L.

The reguli of $Q(4, q)$ through L have to contain zero or at least two lines of the set S. So suppose that a regulus of $Q(4, q)$ through L contains the line L' of S in $\mathcal{Q}_1$ belonging to the regulus of l_2. Then the 3-dimensional space $\langle L, L' \rangle$ intersects the 3-space spanned by $\mathcal{Q}_2$ in a plane through the line l_1, so there has to lie a second line of $S \cap \mathcal{Q}_2$ intersecting l_1 in $\langle L, L' \rangle$. In order to have a codeword, the sum of the symbols of the lines of each regulus through L has to be equal to zero. This is here the case since the two lines of S in this regulus of $\mathcal{Q}(4, q)$ through L have the symbol 1. □

Theorem 24. *In the LDPC code defined by $T_2^*(\Theta)^D$, with $q = 2^h$, $h \geq 5$, Θ a regular hyperoval, every codeword c with $wt(c) \leq 4q^{3/2}/5$ is a linear combination of incidence vectors of hyperbolic quadrics such that the symbols corresponding to the coordinate positions of the lines intersecting L are zero, and such that the sum of the symbols of the lines in each regulus through L equals zero.*

Proof. As seen in the proof of Proposition 23, we find a set of $2q - 10\delta + 2$ lines with constant symbol a lying in $\mathcal{Q}_i$, $i = 1, \ldots, k$.

Let l_1' be a line in $S \cap \mathcal{Q}_1$. The 'point' $\mathcal{R}(l_1', L)$ of $T_2^*(\Theta)^D$ which is the regulus through l_1' and L has to contain a second line l_2' of S. Then the line l_2' lies on a hyperbolic quadric $\mathcal{Q}'$ with $2q - 10\delta + 2$ lines of S only lying in $\mathcal{Q}'$. Suppose that one of these lines has the symbol b, then the preceding arguments lead to $2q - 10\delta + 2$ lines in $\mathcal{Q}'$ with symbol b.

We conclude that to every hyperbolic quadric $\mathcal{Q}_i$, there corresponds a value α_i which is the symbol of the lines of $\mathcal{Q}_i$, not intersecting L and not lying in an other quadric $\mathcal{Q}_j$, $j \neq i$, in the codeword.

Consider a point P lying in exactly one hyperbolic quadric $\mathcal{Q}_i$, where P does not lie on the lines of $\mathcal{Q}_i$ intersecting L. Then both lines of $\mathcal{Q}_i$ through P have symbol α_i, so the sum of the symbols of the lines of S through P is zero.

The same arguments prove that for a second point P lying in s hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_s$, but not lying on any of the lines of $\mathcal{Q}_i$ intersecting L, that the sum of the symbols of the lines of $\mathcal{Q}_1, \ldots, \mathcal{Q}_s$ through P is zero.

Consider a point P of $\mathcal{Q}_1$ lying on a line of $\mathcal{Q}_1$ intersecting L. Denote this line by l_1. Since l_1 is not a line of $T_2^*(\Theta)^D$, but the sum of the symbols of

the lines of S through P is zero, P lies in at least a second hyperbolic quadric $\mathcal{Q}_j$, $j > 1$. Since this must be valid for all q points of $l_1 \setminus \{P\}$, in fact, l_1 lies completely in at least a second hyperbolic quadric $\mathcal{Q}_j$, $j > 1$.

Suppose that l_1 lies in the hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$. Using the same arguments as in [11, Lemma 6.4], we can find a point P on l_1, lying on r distinct lines in the opposite reguli of l_1 in $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$. So their symbols are respectively $\alpha_1, \ldots, \alpha_r$. Since the sum of the symbols of the lines of S through P is zero, necessarily $\alpha_1 + \cdots + \alpha_r = 0$.

Consider a regulus $\mathcal{R}(l_1', L)$, where $l_1' \in S$. Suppose that l_1' lies in the hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_u$, having symbols $\alpha_1, \ldots, \alpha_u$. Each hyperbolic quadric $\mathcal{Q}_i, i = 1, \ldots, u$, has a unique line l_i'' intersecting l_1' and L. For each such l_i'', the sum of symbols α_i of the hyperbolic quadrics $\mathcal{Q}_i$ in which l_i'' lies is equal to zero.

Vice versa, consider such a line l_i'' of a hyperbolic quadric $\mathcal{Q}_i$ lying in the complementary regulus of $\mathcal{R}(l_1', L)$. This hyperbolic quadric $\mathcal{Q}_i$ shares already one line l_i'' with the hyperbolic quadric containing $\mathcal{R}(l_1', L)$, so contains also a line of $\mathcal{R}(l_1', L) \setminus \{L\}$.

Consider all lines of hyperbolic quadrics in $\mathcal{Q}_1, \ldots, \mathcal{Q}_k$ lying in the regulus $\mathcal{R}(l_1', L)$.

These hyperbolic quadrics contain one line l_i'' of the opposite regulus of $\mathcal{R}(l_1', L)$. Each such hyperbolic quadric has a corresponding symbol α_i, and again for such a line l_i'', the sum of symbols α_i of the hyperbolic quadrics $\mathcal{Q}_i$ in which l_i'' lies is equal to zero. This implies that if we add up all the symbols of the lines of S in $\mathcal{R}(l_1', L)$, then this sum is zero.

We have found a linear combination of hyperbolic quadrics of $Q(4, q)$ which defines a codeword of the LDPC code of $T_2^*(\Theta)^D$.

This codeword coincides with the original codeword in all positions corresponding to the lines of S lying on exactly one of the hyperbolic quadrics of $\mathcal{Q}_1, \ldots, \mathcal{Q}_k$.

Since two hyperbolic quadrics share at most two lines, they differ in at most $k(k-1) \leq (2\sqrt{q}/5)^2 = 4q/25$ positions. So the difference of the two codewords has at most weight $8q/25$. Since the minimum distance is $4q$, the two codewords coincide. □

5.3 Codewords of small weight in the LDPC code of $T_2^*(\Theta)^D$, with Θ a regular hyperoval, described in terms of $T_2^*(\Theta)$

We have found the codewords of small weight of the LDPC code of $T_2^*(\Theta)^D$. Now we want to dualize these results to find the codewords of the LDPC code of $T_2^*(\Theta)^D$, described in terms of points and lines of $T_2^*(\Theta)$.

In Section 5.1, it is proven that $T_2^*(\Theta)^D$ can be described on $Q(4, q)$ by taking all points not on a special line L of $Q(4, q)$, and all lines not in $L^\perp$, with as special points the reguli through L.

From $T_2^*(\Theta)^D$ on $Q(4, q)$, we dualize and get $T_2^*(\Theta)$ on $Q(4, q)$ since $Q(4, q)$, q even, is self-dual. We say that a set and its image under this duality are *corresponding*.

The minimum weight codewords of $T_2^*(\Theta)^D$ come from two hyperbolic quadrics of $Q(4, q)$, intersecting in two lines, which intersect L, so a minimum weight

codeword of the code of $T_2^*(\Theta)^D$ is in the original setting $(\mathcal{P}, \mathcal{L}, \mathcal{I}) = T_2^*(\Theta)$ (see beginning of Section 5.1) a set of $4q$ points such that every line of $Q(4,q)$ not through P contains zero or at least two of them.

The line L corresponds to the point P, the intersection lines s_1 and s_2 of $\mathcal{Q}_1$ and $\mathcal{Q}_2$, the two hyperbolic quadrics defining a codeword of minimum weight in $T_2^*(\Theta)^D$, correspond to two points S_1 and S_2. Since s_1 and s_2 are not an element of $T_2^*(\Theta)^D$, S_1 and S_2 have to be points of $T_P(Q(4,q)) \cap Q(4,q)$, which is the set of all points of $Q(4,q)$ collinear with P. Since s_1, s_2 and L are concurrent, S_1, S_2 and P are collinear. The first hyperbolic quadric $\mathcal{Q}_1$ consists of two reguli $\mathcal{R}_1$ and $\mathcal{R}_2$, one through s_1 and one through s_2. The reguli $\mathcal{R}_1$ and $\mathcal{R}_2$ correspond to conics C_1 and C_2, respectively, in $Q(4,q)$, with $S_1 \in C_1$ and $S_2 \in C_2$.

Each line of $\mathcal{R}_1$ intersects each line of $\mathcal{R}_2$. So dually, every point on C_1 is collinear with every point on C_2. Projecting $Q(4,q)$ from its nucleus N onto a 3-dimensional space $PG(3,q)$, gives $W(3,q)$, a symplectic generalized quadrangle defined by a symplectic polarity η. In this projection, C_1 and C_2 become two lines M and M^η, because then every point of M is collinear with every point on M^η. The only conics that are projected onto a line under this projection are the conics of $Q(4,q)$ in a plane through N, and all conics in such a plane have N as their nucleus. So C_1 and C_2 are conics each lying in a plane through N, with N as nucleus.

To go from $T_2^*(\Theta)$ described on $Q(4,q)$ to the original setting $T_2^*(\Theta)$ as a linear representation in $PG(3,q)$, we project from the point P onto a 3-dimensional space $PG(3,q)$. The points S_1 and S_2 project onto the same point $S_1' = S_2'$ on a conic at infinity with nucleus N', so the conics C_1' and C_2' which are the projected conics C_1 and C_2 go through the same point $S_1' = S_2'$ at infinity.

The regulus of $\mathcal{Q}_2$ containing s_1 corresponds to a conic C_3' lying in a plane through S_1' and N'. This has to be the same plane as the one containing C_1', otherwise the lines through N' containing points of C_1' cannot have a second point in that plane. The other regulus of $\mathcal{Q}_2$ corresponds to a conic C_4' lying in the same plane as C_2'.

In order to get a codeword of the LDPC code of $T_2^*(\Theta)^D$, the conics have to be corresponding, which means that a line connecting a point of $\Theta \setminus \{S_1' = S_2', N'\}$ with a point of C_1' (C_3' resp.) intersects in C_2' (C_4' resp.).

Using this and dualizing Theorem 24 gives the following theorem.

Theorem 25. *In the LDPC code defined by $T_2^*(\Theta)^D$, with $q = 2^h$, $h \geq 5$, Θ a regular hyperoval, described in terms of points and lines of the linear representation $T_2^*(\Theta)$, every codeword c, with $wt(c) \leq 4q^{3/2}/5$, is a linear combination of incidence vectors of two by two corresponding conics with the same symbol, lying in tangent planes to the conic in Θ, such that the sum of the symbols on a line of $T_2^*(\Theta)$ is zero. In particular, the sum of symbols of the conics in one tangent plane is equal to zero.*

Remark 7. *The preceding arguments are more complicated than in the case of the non-regular translation hyperoval. We believe that this comes from the fact that a non-regular translation hyperoval $\{(1,t,t^{2^v}) | t \in \mathbb{F}_q\} \cup \{(0,0,1),(0,1,0)\}$, with $q = 2^h$, $\gcd(v,h) = 1$, is stabilized by a group of order $2q(q-1)$ fixing $\{R = (0,0,1), N = (0,1,0)\}$ while the regular hyperoval is stabilized by a group of order $q^3 - q$ only fixing $N = (0,1,0)$. So for the non-regular hyperoval, there*

is one point $R = (0, 0, 1)$ playing a special role which we observe in Proposition 17, while we have no such point in the case of the regular hyperoval.

References

[1] F. Buekenhout, *Handbook of incidence geometry: buildings and foundations*, North-Holland, Amsterdam (1995).

[2] S. Cauchie, F. De Clerck, and N. Hamilton, Full Embeddings of (α, β) -Geometries in Projective Spaces. *Eur. J. Comb.* 23(6) (2002) pp. 635–646.

[3] M.P.C. Fossorier, Quasicyclic low-density parity check codes from circulant permutation matrices. *IEEE Trans. Inform. Theory*, Vol. 50 (2004) pp. 1788–1793.

[4] A. Gács and Zs. Weiner, On $(q + t)$-arcs of type $(0, 2, t)$. *Des. Codes Cryptogr.*, 29 (2003) pp. 131–139.

[5] R.G. Gallager, Low density parity check codes. *IRE Trans. Inform. Theory*, Vol. 8 (1962) pp. 21–28.

[6] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, Oxford, second edition (1998).

[7] X.Y. Hu, M.P.C. Fossorier, and E. Eleftheriou, On the computation of the minimum distance of low-density parity check codes, *2004 IEEE International Conference on Communications*, Vol. 2 (2004) pp. 767–771.

[8] S.J. Johnson and S.R. Weller, Construction of low-density parity check codes from Kirkman triple systems, *Proc. IEEE Globecom Conf., San Antonio, TX, Nov. 2001*, available at http://www.ee.newcastle.edu.au/users/sta/steve/

[9] S.J. Johnson and S.R. Weller, Regular low-density parity check codes from combinatorial designs, *Proc. IEEE Inform. Theory Workshop, Cairns, Australia, Sep. 2001*, pp. 90–92.

[10] S.J. Johnson and S.R. Weller, Codes for iterative decoding from partial geometries, *Proc. IEEE Int. Symp. Inform. Theory, Switzerland, June 30 - July 5*, (2002), 6 page, extended abstract, available at http://murray.newcastle.edu.au/users/staff/steve/

[11] J.-L. Kim, K. Mellinger, and L. Storme, Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles. *Des. Codes Cryptogr.*, 42(1) (2007) pp. 73–92.

[12] J.-L. Kim, U. Peled, I. Perepelitsa, V. Pless, and S. Friedland, Explicit construction of families of LDPC codes with no 4-cycles. *IEEE Trans. Inform. Theory*, Vol. 50 (2004) pp. 2378–2388.

[13] G. Korchmáros and F. Mazzocca, On $(q + t)$-arcs of type $(0, 2, t)$ in a desarguesian plane of order q. *Math. Proc. Camb. Phil. Soc.*, 108 (1990) pp. 445–459.

[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*, Vol. 47, No. 7 (2001) pp. 2711–2736.

[15] Z. Liu and D.A. Pados, LDPC codes from generalized polygons. *IEEE Trans. Inform. Theory,* Vol. 51(11) (2005) pp. 3890–3898.

[16] D.J.C. MacKay, Good error correcting codes based on very sparse matrices. *IEEE Trans. Inform. Theory*, Vol. 45 (1999) pp. 399–431.

[17] D.J.C. MacKay and M.C. Davey, Evaluation of Gallager codes for short block length and high rate applications. *Codes, Systems and Graphical Models, B. Marcus and J. Rosenthal, editors,* Vol. 123, IMA in Math. and its Appl., Springer-Verlag, New York, (2000) pp. 113–130.

[18] D.J.C. MacKay and R.M. Neal, Near Shannon limit performance of low density parity check codes. *Electron. Lett.*, Vol. 32, No. 18 (1996) pp. 1645–1646.

[19] G.A. Margulis, Explicit constructions of graphs without short cycles and low density codes. *Combinatorica*, Vol. 2 (1982) pp. 71–78.

[20] F. Pambianco and L. Storme, Small Complete Caps in Spaces of Even Characteristic. *J. Comb. Theory, Ser. A* 75(1) (1996) pp. 70–84.

[21] S.E. Payne, Quadrangles of order $(s-1,\, s+1)$. *J. Algebra* 22 (1972) pp. 97–119.

[22] S.E. Payne and J.A. Thas, *Finite Generalized Quadrangles*. Pitman Advanced Publishing Program (1984).

[23] J. Rosenthal and P.O. Vontobel, Construction of LDPC codes using Ramanujan graphs and ideas from Margulis. *Proc. 38th Allerton Conf. on Communications, Control, and Computing, Monticello, IL, Coordinated Science Lab., P.G. Voulgaris and R. Srikant, Eds., Oct. 4-6*, (2000) pp. 248–257.

[24] B. Segre, On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two. *Acta Arith.* 5 (1959) pp. 315–332.

[25] M. Sipser and D.A. Spielman, Expander codes. *IEEE Trans. Inform. Theory*, Vol. 42 (1996) pp. 1710–1722.

[26] R.M. Tanner, Minimum distance bounds by graph analysis. *IEEE Trans. Inform. Theory*, Vol. 47(2) (2001) pp. 808–821.

[27] R.M. Tanner, D. Sridhara, A. Sridharan, T.E. Fuja, and D.J. Costello, Jr., LDPC block and convolutional codes based on circulant matrices. *IEEE Trans. Inform. Theory*, Vol. 50 (2004) pp. 2966–2984.

[28] P.O. Vontobel and R.M. Tanner, Construction of codes based on finite generalized quadrangles for iterative decoding. *Proceedings of 2001 IEEE Intern. Symp. Inform. Theory, Washington, DC*, (2001) p. 223.

[29] S.R. Weller and S.J. Johnson, Regular low-density parity check codes from oval designs. *European Transactions on Telecommunications*, Vol. 14, No. 5 (2003) pp. 399–409.

Address of the authors:

Valentina Pepe:
Dipartimento di Matematica e Applicazioni "R. Caccioppoli"
Università degli Studi di Napoli Federico II
Via Cintia - Monte S. Angelo
80126 Napoli (Italia)
valepepe@unina.it

Leo Storme:
Department of pure mathematics and computer algebra,
Ghent University
Krijgslaan 281-S22
9000 Ghent (Belgium)
ls@cage.ugent.be
http://cage.ugent.be/∼ls

Geertrui Van de Voorde:
Department of pure mathematics and computer algebra,
Ghent University
Krijgslaan 281-S22
9000 Ghent (Belgium)
gvdvoorde@cage.ugent.be