Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles

Jon-Lark Kim[*], Keith E. Mellinger[†], and Leo Storme[‡]

October 12, 2006

Abstract

We find lower bounds on the minimum distance and characterize codewords of small weight in low-density parity check codes defined by (dual) classical generalized quadrangles. We analyze the geometry of the non-singular parabolic quadric in $PG(4, q)$ to find information about the low-density parity check codes defined by $Q(4, q)$, $\mathcal{W}(q)$ and $\mathcal{H}(3, q^2)$. For $\mathcal{W}(q)$ and $\mathcal{H}(3, q^2)$, we are able to describe small weight codewords geometrically. For $\mathcal{Q}(4, q)$, q odd, and for $\mathcal{H}(4, q^2)^D$, we improve the best known lower bounds on the minimum distance, again only using geometric arguments. Similar results are also presented for the LDPC codes $\mathrm{LU}(3, q)$ given in [10].

Keywords: LDPC code, generalized quadrangle, minimum distance
Classification: 51E12, 94B05

1 Introduction

The concept of low-density parity check (LDPC) codes was introduced by Gallager [4], and it was shown in [16] 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., H has many fewer 1s than 0s. When the columns of H have a constant weight ρ and the rows 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], [14].

Early known LDPC codes have been constructed randomly [4], [16]. There are several types of explicit constructions of LDPC codes. One is based on permutation matrices [3], [24]. Others are based on Ramanujan graphs [17], [19], expander graphs [21], and q-regular bipartite graphs [10].

[*]The first author acknowledges support by a Research Initiation Grant from University of Louisville

[†]The second author acknowledges support by a Faculty Development Grant from the University of Mary Washington

[‡]The third author thanks the Fund for Scientific Research Flanders-Belgium for a research grant

In 2001, Kou et al. [11] 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, [7], [8], [9], [15], [25], [26]). In particular, Vontobel and Tanner [25] 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 [16]. Later, Liu and Pados [13] 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 that several generalized polygon LDPC codes have powerful bit-error-rate performance when decoding is carried out via low-complexity variants of belief propagation [13].

In [6], the problem of determining the minimum distance of LDPC codes was addressed. Furthermore, Liu and Pados proved in [13] that the binary LDPC codes defined by generalized quadrangles only have codewords of even weight. We contribute in this article to the problem of finding the minimum distance of LDPC codes defined by the incidence structure of (dual) classical finite generalized quadrangles. We either find improved lower bounds on the minimum distances of these codes or characterize their low weight codewords using geometric techniques.

Furthermore we will obtain similar results for $\mathrm{LU}(3,q)$ [10] whose parity check matrix $H(3,q)$ or $H(3,q)^T$ is defined by the incidence structure which consists of part of the generalized quadrangle $\mathcal{W}(q)$ or $\mathcal{Q}(4,q)$, respectively.

This paper consists of six sections. Section 2 gives an introduction to generalized quadrangles and LDPC codes defined by them. Section 3 classifies geometrically the small weight codewords in the LDPC code defined by $\mathcal{W}(q)$ or $\mathcal{H}(3,q^2)$. In Sections 4 and 5, we improve the lower bounds on the minimum weight of codewords in $\mathcal{Q}(4,q)$, q odd, and $\mathcal{H}(4,q^2)^D$, respectively. In Section 6, we study codewords of small weight in $\mathrm{LU}(3,q)$ and improve a lower bound on the minimum distance of $\mathrm{LU}(3,q)$ defined by $H(3,q)^T$.

2 Generalized quadrangles

We provide a brief overview of generalized quadrangles and refer the reader to [5] or [18] for more details.

A *generalized quadrangle* Γ, also denoted by GQ, is defined axiomatically as a set of points and lines such that:

(a) any two distinct points are on at most one common line,

(b) all lines are incident with the same number of points, and all points are incident with the same number of lines, and,

(c) if the point P of Γ is not incident with the line ℓ of Γ, then there is precisely one line through P intersecting ℓ.

Note that the last axiom forces the non-existence of triangles in generalized quadrangles. The common number of points on a line is denoted by $s+1$, and the common number of lines through a point is denoted by $t+1$. The pair (s,t) is called the *order* of the generalized quadrangle Γ,

and Γ is also denoted by $\mathrm{GQ}(s,t)$. Interchanging the roles of points and lines in a generalized quadrangle Γ of order (s,t) gives the *dual* generalized quadrangle $\Gamma^D = \overline{\Gamma}$ of order (t,s). Counting techniques show that the number of points in a $\mathrm{GQ}(s,t)$ is $(s+1)(st+1)$ and the number of lines is $(t+1)(st+1)$.

All of the generalized quadrangles that we will discuss in this article arise, up to duality, naturally in a finite projective space $PG(n,q)$. The first family of generalized quadrangles is denoted by $\mathcal{Q}(n,q)$. Consider a non-singular quadric $\mathcal{Q}$ of projective index 1 in the projective space $PG(n,q)$, $n = 3, 4$, or 5. The points of $\mathcal{Q}$ together with the lines of $\mathcal{Q}$, which are the subspaces of maximal dimension contained in $\mathcal{Q}$, form the generalized quadrangle $\mathcal{Q}(n,q)$. We concentrate on the cases $n = 4, 5$. The GQ $\mathcal{Q}(4,q)$ is formed by a non-singular parabolic quadric of $PG(4,q)$. Without loss of generality, we can define this quadric by the quadratic form $X_0^2 + X_1X_2 + X_3X_4 = 0$, and in this case $s = t = q$. When $n = 5$, the GQ $\mathcal{Q}^-(5,q)$ is formed by the non-singular elliptic quadric in $PG(5,q)$. Without loss of generality, this quadric can be defined by a quadratic form $f(X_0, X_1) + X_2X_3 + X_4X_5 = 0$, where $f(X_0, X_1)$ is an irreducible homogeneous quadratic form over $GF(q)$. In this case, $s = q$ and $t = q^2$.

Now let $\mathcal{U}$ be a non-singular Hermitian variety in $PG(n,q^2)$, $n = 3$ or 4. Without loss of generality, we can use the equation $X_0^{q+1} + X_1^{q+1} + \cdots + X_n^{q+1} = 0$ to define $\mathcal{U}$. The points of $\mathcal{U}$, together with the lines of $\mathcal{U}$, define a generalized quadrangle, denoted by $\mathcal{H}(n,q^2)$. In this case, $s = q^2$ and $t = q$ when $n = 3$; and $s = q^2$ and $t = q^3$ when $n = 4$.

Finally, the points of $PG(3,q)$, together with the self-polar lines of a symplectic polarity η, form a generalized quadrangle $\mathcal{W}(q)$ with $s = t = q$. The geometry is quite interesting in this case. We obtain a set of $q^3 + q^2 + q + 1$ lines of $PG(3,q)$ with the property that through every point P of $PG(3,q)$, there are exactly $q+1$ coplanar lines of $\mathcal{W}(q)$ lying in the plane P^η, and in every plane Π, there are exactly $q+1$ concurrent lines of $\mathcal{W}(q)$ passing through the point Π^η.

The above described generalized quadrangles are called the *classical* generalized quadrangles, and their duals are called the *dual classical* generalized quadrangles.

In a generalized quadrangle, we denote the set of points collinear with a point P by $P^\perp$, and the set of lines intersecting a given line ℓ by $\ell^\perp$. For $\mathcal{W}(q)$, $P^\perp = P^\eta$.

The following relations between these (dual) classical generalized quadrangles are known [18].

Theorem 2.1. (1) *The generalized quadrangle $\mathcal{Q}(4,q)$ is isomorphic to the dual of $\mathcal{W}(q)$.*
(2) *The generalized quadrangles $\mathcal{W}(q)$ and $\mathcal{Q}(4,q)$ are self-dual if and only if q is even.*
(3) *The generalized quadrangle $\mathcal{Q}^-(5,q)$ is isomorphic to the dual of $\mathcal{H}(3,q^2)$.*

Recently, q-regular bipartite graphs $D(m,q)$ [12] were used to define the code $\mathrm{LU}(m,q)$ [10, 20] for the study of LDPC codes. We recall that $\mathrm{LU}(3,q)$ has parity check matrix either $H(3,q)$ or $H(3,q)^T$, where $H(3,q)$ is the incidence matrix with rows indexed by lines $[x,y,z] \in GF(q)^3$ and columns indexed by points $(a,b,c) \in GF(q)^3$. A point (a,b,c) is incident with a line $[x,y,z]$ if and only if $y = ax + b$ and $z = ay + c$.

In what follows, we give a geometric description of $H(3,q)$ in terms of $\mathcal{W}(q)$. Let $\Gamma(H(3,q))$ be the point-line geometry whose incidence matrix is $H(3,q)$.

Consider first of all the generalized quadrangle $\mathcal{W}(q)$ defined by the symplectic polarity η, and a point P and a line ℓ of $\mathcal{W}(q)$, where $P \in \ell$.

(1) The point set of $\Gamma(H(3,q))$ consists of the point set $PG(3,q) \setminus P^{\perp}$.

(2) The line set of $\Gamma(H(3,q))$ consists of the lines of $\mathcal{W}(q)$, not belonging to $\ell^{\perp}$.

(3) The incidences of the points and the lines of $\Gamma(H(3,q))$ coincide with the incidences in $PG(3,q)$.

Since we cancel $P^{\perp}$ and $\ell^{\perp}$ from $\mathcal{W}(q)$, we denote $\Gamma(H(3,q))$ also by $\mathcal{W}(q) \setminus (P^{\perp} \cup \ell^{\perp})$.

The incidence matrix H of a generalized quadrangle Γ, or of a subset Γ of a generalized quadrangle, is the matrix with rows labeled by the lines ℓ of Γ, columns labeled by the points P of Γ, and with a matrix entry, indexed by P and ℓ, equal to one when P is incident with ℓ, and zero when P is not incident with ℓ. The dual of the code generated by the incidence matrix of $\mathrm{GQ}(s,t)$ is a $(\rho := t+1, \gamma := s+1)$-LDPC code of length $(s+1)(st+1)$. Similarly if we consider $\mathrm{GQ}(s,t)^D$, we get a $(\rho := s+1, \gamma := t+1)$-LDPC code of length $(t+1)(st+1)$. Finally, $\mathrm{LU}(3,q)$ is a (q,q)-LDPC code of length q^3.

For many applications, we are interested in the *binary* linear code with this incidence matrix H as parity check matrix. Nevertheless, we can also address the codes defined by H over the finite field $GF(q)$ in the cases $\mathcal{Q}(n,q)$ and $\mathcal{W}(q)$, and over the finite field $GF(q^2)$ in the case $\mathcal{H}(n,q^2)$, or over the prime field $GF(p)$ of $GF(q = p^h)$ or $GF(q^2 = p^{2h})$. We will address the problem of finding the minimum distance of LDPC codes and of characterizing small weight codewords in LDPC codes. The methods applied here are valid both for binary LDPC codes, LDPC codes over $GF(q)$ or $GF(q^2)$, and for LDPC codes over $GF(p)$ [2].

Let $\mathcal{C}$ be a binary linear code defined by the parity check matrix H. For every binary LDPC code, there is an associated bipartite graph, called the "Tanner graph", which represents the code. In this setting, the Tanner graph is simply the bipartite incidence graph of the corresponding geometry. It is well regarded in the theory of low-density parity check codes that high girth in this graph increases the efficiency of the decoding. In general, girth 4 is considered to be poor. Note that using generalized quadrangles, or some subset thereof, implies a girth of at least 8 in the Tanner graph. This is one motivation for studying LDPC codes arising from generalized quadrangles, or from a subset of a generalized quadrangle.

Let $\mathcal{C}$ be an LDPC code defined by a generalized quadrangle Γ, or by a subset Γ of a generalized quadrangle. A codeword $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ in $\mathcal{C}$ satisfies $\mathbf{c}H^T = \bar{0}$. Hence, the codeword $\mathbf{c}$ defines through its non-zero positions which correspond to points of Γ,

(*) a set S of points of Γ such that every line of Γ contains 0 or at least 2 of the points of S.

Alternatively, we can work in the dual generalized quadrangle Γ^D. Here, this codeword $\mathbf{c}$ defines

(**) a set S of lines of Γ^D such that every point of Γ^D lies on 0 or on at least 2 of the lines of S.

We will refer to these as Property (*) and (**). These properties (*) and (**) can be used for binary LDPC codes, and for LDPC codes over $GF(q)$, $GF(q^2)$, or over $GF(p)$, p prime. We note

that (*) and (**) are necessary conditions that codewords must satisfy. More precisely, we use for instance (**) to get information on which lines belong to such a set S. Then we look for the coordinates in $\mathbf{c}$ corresponding to these lines of S.

Example 2.2. Consider $\mathcal{W}(q)$, the GQ formed by the points of $PG(3,q)$ together with the set of lines self-polar with respect to some symplectic polarity η. It is known that the classical generalized quadrangle $\mathcal{Q}(4,q)$ is the dual of $\mathcal{W}(q)$ (Theorem 2.1 (3)). We start the description of codewords in this dual generalized quadrangle $\mathcal{Q}(4,q)$.

Recall that a *regulus* of $PG(3,q)$ is a set of transversal lines to three pairwise skew lines. That is, a regulus $\mathcal{R}$ is a set of $q+1$ lines of $PG(3,q)$ with the property that any line meeting three lines of $\mathcal{R}$, meets in fact all $q+1$ lines of $\mathcal{R}$. Recall that the set of points covered by a regulus forms a quadratic surface of $PG(3,q)$, the so-called *hyperbolic quadric* $\mathcal{Q}^+(3,q)$.

Consider a hyperbolic quadric $\mathcal{Q}^+(3,q)$ contained in $\mathcal{Q}(4,q)$. This hyperbolic quadric consists of the $q+1$ lines of one regulus $\mathcal{R}$ and the $q+1$ lines of its *opposite* regulus $\mathcal{R}^{opp}$, which is the set of the transversal lines to $\mathcal{R}$.

Clearly this hyperbolic quadric $\mathcal{Q}^+(3,q)$ is a set of lines of $\mathcal{Q}(4,q)$ such that every point lies on 0 or on at least 2 of the lines (Property (**)). Label the lines of $\mathcal{R}$ by $\ell_0,\ldots,\ell_q$, and the lines of the opposite regulus by $m_0,\ldots,m_q$. In $\mathcal{W}(q)$, these lines correspond to two sets of points $\{p_0,\ldots,p_q\}$ and $\{r_0,\ldots,r_q\}$ lying on two non self-polar lines ℓ and ℓ^η under the symplectic polarity η.

Identify the positions in the codeword $\mathbf{c}$ with their corresponding points in Γ. Create the vector $\mathbf{c}$ with 1 in the coordinates corresponding to the points p_i, with -1 in the coordinates corresponding to the points r_j, and zero in its other positions. As every point of $\mathcal{Q}(4,q)$ lies on either 0 or 2 of the lines of $\mathcal{Q}^+(3,q)$, every line of $\mathcal{W}(q)$ contains either 0 or 2 of the points in $\{p_0,\ldots,p_q\}\cup\{r_0,\ldots,r_q\}$, one from each set. Moreover, $\mathbf{c}$ is orthogonal to every row of H and so it defines a codeword of weight $2(q+1)$ of the LDPC code arising from the generalized quadrangle $\mathcal{W}(q)$. This in fact is a codeword of minimal weight of this LDPC code [1, Lemma 2.4].

In Table 1, the lower bounds on the minimum distances d of the LDPC codes arising from the (dual) classical generalized quadrangles of [13] are given. These lower bounds arise from bounds called the *bit-oriented bound, parity-oriented bound*, and *tree bound* [22, 23, 25].

These lower bounds are in accordance with the results of Bagchi and Sastry [1] who showed that the minimum distance is at least $2(t+1)$, with equality if and only if the generalized quadrangle $\Gamma = \mathrm{GQ}(s,t)$ contains subquadrangles of order $(1,t)$. This is the case for $\mathcal{W}(q)$ and $\mathcal{H}(3,q^2)$. Example 2.2 shows this for $\mathcal{W}(q)$. For $\mathcal{H}(3,q^2)$, simply consider the $2(q+1)$ points of $\mathcal{H}(3,q^2)$ lying on two polar secant lines ℓ and ℓ^η to $\mathcal{H}(3,q^2)$, with η the unitary polarity defining $\mathcal{H}(3,q^2)$. By constructing the vector having 1 in the positions corresponding to the points of $\ell\cap\mathcal{H}(3,q^2)$, -1 in the positions corresponding to the points of $\ell^\eta\cap\mathcal{H}(3,q^2)$, and zero elsewhere, a codeword of weight $2(q+1)$ in the LDPC code arising from $\mathcal{H}(3,q^2)$ is obtained.

In the cases $\mathcal{W}(q)$ and $\mathcal{H}(3,q^2)$, we characterize small weight codewords in the corresponding LDPC codes, using geometric arguments. In the cases $\mathcal{Q}(4,q)$, q odd, and $\mathcal{H}(4,q^2)^D$, we improve the lower bound on d of Table 1 greatly by using geometric arguments.

We investigate in a similar way the LDPC codes arising from $H(3,q)$ and $H(3,q)^T$. For $H(3,q)$, we characterize the codewords of small weight, and for $H(3,q)^T$, we present an improved lower bound on the minimum distance.

LDPC code	Order (s,t)	d
$\mathcal{W}(q)$, $q=2^e$	(q,q)	$2(q+1)$
$\mathcal{W}(q)$, q odd	(q,q)	$2(q+1)$
$\mathcal{Q}(4,q)$, q odd	(q,q)	$\geq 2(q+2)$
$\mathcal{Q}^-(5,q)$	(q,q^2)	$\geq (q+1)(q^2-q+2)$
$\mathcal{H}(3,q^2)$	(q^2,q)	$2(q+1)$
$\mathcal{H}(4,q^2)$	(q^2,q^3)	$\geq (q^2+1)(q^3-q^2+2)$
$\mathcal{H}(4,q^2)^D$	(q^3,q^2)	$\geq 2(q^2+1)$

Table 1: Minimum distances of GQ LDPC codes

3 Small weight codewords in $\mathcal{W}(q)$

The goal in this section is to classify geometrically the small weight codewords in the LDPC code $\mathcal{C}$ defined by $\mathcal{W}(q)$. We remind the reader that, by Property (*), a codeword corresponds to a set S of points of $\mathcal{W}(q)$ with the property that every line of $\mathcal{W}(q)$ meets S in 0 or in at least 2 points. As $\mathcal{Q}(4,q)$ is isomorphic to the dual of $\mathcal{W}(q)$, we work in $PG(4,q)$ and look at sets of lines lying in a parabolic quadric of $PG(4,q)$ such that every point lies on 0 or on at least 2 of these lines (Property (**)). Since we are working in $\mathcal{W}(q)^D$, the columns of H correspond to the lines of $\mathcal{W}(q)^D = \mathcal{Q}(4,q)$ and the rows of H correspond to the points of $\mathcal{W}(q)^D = \mathcal{Q}(4,q)$. We will therefore describe the coordinate positions in a codeword by their corresponding lines in $\mathcal{Q}(4,q)$.

It is known that the minimum distance, and hence minimum weight, of the LDPC code defined by $\mathcal{W}(q)$ is $2(q+1)$ [1]. We have already mentioned that codewords of weight $2(q+1)$ are relatively easy to generate when we describe them on the dual generalized quadrangle $\mathcal{Q}(4,q)$.

Let $\mathcal{R} = \{\ell_1, \ldots, \ell_{q+1}\}$ and $\mathcal{R}^{opp} = \{m_1, \ldots, m_{q+1}\}$ be a regulus and its opposite regulus. The vector with 1 in the coordinates representing the lines in $\mathcal{R}$ and -1 in the coordinates representing the lines in $\mathcal{R}^{opp}$ is clearly a codeword of the LDPC code arising from $\mathcal{Q}(4,q)^D = \mathcal{W}(q)$.

Now consider two hyperbolic quadrics lying in $\mathcal{Q}(4,q)$ that intersect in a planar conic C. Let $\mathcal{R}_1, \mathcal{R}_1^{opp}, \mathcal{R}_2$, and $\mathcal{R}_2^{opp}$ be the reguli in these two quadrics. Moreover, let

$$\mathcal{R}_1 = \{\ell_1^{(1)}, \ldots, \ell_{q+1}^{(1)}\}, \;\; \mathcal{R}_1^{opp} = \{m_1^{(1)}, \ldots, m_{q+1}^{(1)}\},$$

$$\mathcal{R}_2 = \{\ell_1^{(2)}, \ldots, \ell_{q+1}^{(2)}\}, \;\; \mathcal{R}_2^{opp} = \{m_1^{(2)}, \ldots, m_{q+1}^{(2)}\}.$$

Then, the vector $\mathbf{v}$ with a 1 in the coordinates corresponding to the lines $\ell_i^{(1)}$ and $\ell_i^{(2)}$, and a -1 in the coordinates corresponding to the lines $m_j^{(1)}$ and $m_j^{(2)}$, forms a codeword of weight $4q+4$ of the LDPC code arising from $\mathcal{Q}(4,q)^D = \mathcal{W}(q)$.

In a similar fashion, consider two hyperbolic quadrics $\mathcal{H}_1$ and $\mathcal{H}_2$ of $\mathcal{Q}(4,q)$ intersecting in a pair of intersecting lines. Let $\mathbf{v}_1$ be the vector corresponding to $\mathcal{H}_1$. So, $\mathbf{v}_1$ has 1 in the coordinates

corresponding to the lines of one of the reguli ruling $\mathcal{H}_1$, -1 in the coordinates corresponding to the lines of the opposite regulus ruling $\mathcal{H}_1$, and zero elsewhere. Define $\mathbf{v}_2$ similarly for $\mathcal{H}_2$, where the two common lines of $\mathcal{H}_1$ and $\mathcal{H}_2$ have the same symbol in $\mathbf{v}_1$ and $\mathbf{v}_2$. Now, the difference $\mathbf{v}_1 - \mathbf{v}_2$ is a codeword of weight $4q$ of the LDPC code $\mathcal{C}$ arising from $\mathcal{Q}(4,q)^D = \mathcal{W}(q)$. The sum $\mathbf{v}_1 + \mathbf{v}_2$ gives a codeword of weight $4q$ if $\mathcal{C}$ is a binary code, and a codeword of weight $4q+2$ if $\mathcal{C}$ is not a binary code.

We will prove that the above described codewords are the smallest weight codewords of $\mathcal{C}$, different from those of minimal weight. Essentially, they can be described as being linear combinations of codewords of minimum weight $2(q+1)$.

For larger weights, this will also be true. We will characterize codewords in the LDPC code arising from $\mathcal{W}(q)$, up to weight $\sqrt{q}(q+1)/2$, as linear combinations of codewords of minimum weight $2(q+1)$. For weights larger than $4q+4$, we will not describe all the different weights of these linear combinations explicitly, since this becomes too tedious to describe.

So, from this point on, let $\mathbf{c}$ be a codeword of $\mathcal{C}$ of weight at most $2\delta(q+1) \leq \sqrt{q}(q+1)/2$. Such a codeword is easily obtained by, for instance, taking the lines of δ reguli and opposite reguli of hyperbolic quadrics $\mathcal{Q}^+(3,q)$ inside $\mathcal{Q}(4,q)$, or equivalently, by taking linear combinations of δ codewords of minimum weight in the LDPC code arising from $\mathcal{W}(q)$.

In the following proofs, we will use Property (**) and identify the codeword $\mathbf{c}$ with the set B of lines of $\mathcal{Q}(4,q)$ corresponding to the non-zero positions in the codeword $\mathbf{c}$, and characterize B by using the property that every point of $\mathcal{Q}(4,q)$ lies on 0 or on at least two lines of B.

Proposition 3.1. *If the line ℓ_1 is in B, then there is a hyperbolic quadric $\mathcal{Q} \cong \mathcal{Q}^+(3,q)$ of $\mathcal{Q}(4,q)$ containing ℓ_1 and such that each regulus of $\mathcal{Q}$ contains at least $q - 2\delta + 1$ lines of B.*

Proof. Let ℓ_1 and B be as defined above, and assume that B corresponds to a codeword of weight at most $2\delta(q+1)$. Then, every point of ℓ_1 lies on at least a second line of B. Denote these lines by $\ell_2, \ldots, \ell_{q+2}, \ldots$, where $\ell_2, \ldots, \ell_{q+2}$ pass through the distinct points of ℓ_1. There remain at most $2\delta(q+1) - q - 2$ lines in B. The $q(q+1)$ points of $\ell_2, \ldots, \ell_{q+2}$, not lying on ℓ_1, all lie on at least one other line of B. The average number of points of $\ell_2 \cup \cdots \cup \ell_{q+2}$ on one of these remaining lines in B is at least

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

Hence, there is a line ℓ_{q+3} in B intersecting at least y of the lines $\ell_2, \ldots, \ell_{q+2}$. Now, let Π be the projective 3-space determined by ℓ_1 and ℓ_{q+3}, and let $\mathcal{Q} = \mathcal{Q}(4,q) \cap \langle \ell_1, \ell_{q+3} \rangle$. Note that $\mathcal{Q}$ is a hyperbolic quadric of $\mathcal{Q}(4,q)$. Suppose now that x' lines of the first regulus of $\mathcal{Q}$ are in B and t' lines of the second regulus of $\mathcal{Q}$ are in B.

There are $(q+1-x')t' + (q+1-t')x'$ points on these $t'+x'$ lines of $\mathcal{Q}$ in B not yet lying on a second line in B. There are at most $2\delta(q+1) - t' - x'$ lines left in B. Note that any other line of B meeting the hyperbolic quadric in two points would necessarily be a line of the 3-space Π determined by ℓ_1 and ℓ_{q+3}. Therefore, any line of B not already considered meets at most one point of $\mathcal{Q}$. In order to avoid a contradiction, necessarily

$$(q+1-x')t' + (q+1-t')x' \leq 2\delta(q+1) - t' - x',$$

from which it follows that

$$x' + t' \leq \frac{2\delta(q+1)}{q+2} + \frac{2x't'}{q+2} \leq \frac{2\delta(q+1)}{q+2} + 2x'.$$

If we assume, without loss of generality, that $x' \leq t' \leq q+1$, we obtain

$$t' \leq 2\delta - 1 + x'.$$

We have shown that x' and t' cannot differ by more than $2\delta - 1$. Let $t' = x' + i$ where $0 \leq i \leq 2\delta - 1$. Since $\mathcal{Q}$ contains $y > 2\sqrt{q}$ lines of one of its reguli, $t' = x' + i$ where $0 \leq i \leq 2\delta - 1$, and $\delta \leq \sqrt{q}/4$, obviously $t', x' > \sqrt{q}$. From above, we have

$$(x' + t')(q+2) \leq 2\delta(q+1) + 2x't'.$$

Substituting $x' + i$ for t', we obtain the following condition on x':

$$0 \quad \leq \quad 2(x')^2 + x'(-2q - 4 + 2i) - iq - 2i + 2\delta q + 2\delta. \tag{1}$$

The quadratic polynomial on the right hand side in x' obtains its minimum when $x' = (q - i)/2 + 1$. So, this minimum is obtained for some value of $x' \leq q/2 + 1$. We know that $x' > \sqrt{q}$. For $x' = \sqrt{q}$, the right hand side of (1) is negative. Now, let $x' = q - 2\delta$. Plugging into (1) and simplifying gives

$$0 \leq (-2\delta - 4 + i)q + 8\delta^2 + 10\delta - 4i\delta - 2i,$$

where, again, $0 \leq i \leq 2\delta - 1$. Choosing $\delta \leq \sqrt{q}/4$ makes this inequality false. Hence, if we assume that $x' \leq q - 2\delta$, we obtain a contradiction. So, x' is at least $q - 2\delta + 1$. Therefore, we have shown that a line ℓ_1 of B lies in a hyperbolic quadric $\mathcal{Q}$ of $\mathcal{Q}(4, q)$ containing in each of its reguli at least $q - 2\delta + 1$ lines of B. □

Remark 3.2. Following the results of Bagchi and Sastry [1] which characterize the codewords of smallest weight $2(q+1)$ as being a regulus and its opposite regulus, we wish to characterize the codewords of weight in between $2q+3$ and $2\delta(q+1)$. So no single hyperbolic quadric $\mathcal{Q}$ can contain all the lines of B.

We also assume by induction on the weights of the codewords of $\mathcal{C}$ that all codewords of $\mathcal{C}$ of weight smaller than the weight of $\mathbf{c}$ have been characterized as being linear combinations of codewords of minimal weight $2(q+1)$.

Let $\mathcal{Q}_1 \cong \mathcal{Q}^+(3, q)$ be a first hyperbolic quadric containing at least $2(q - 2\delta + 1)$ lines of B. Let $\ell \in B$, $\ell \nsubseteq \mathcal{Q}_1$. Then, by Proposition 3.1, ℓ also lies in a second hyperbolic quadric $\mathcal{Q}_2$ containing at least $2(q - 2\delta + 1)$ lines of B, and the two distinct hyperbolic quadrics share at most two lines.

Now suppose that $\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_j$ are the distinct hyperbolic quadrics each containing at least $2(q - 2\delta + 1)$ lines of B. Then, since distinct hyperbolic quadrics share at most 2 lines,

$$|B| \geq \sum_{i=0}^{j-1} (2q - 4\delta + 2 - 2i),$$

which reduces to

$$2\delta(q+1) \quad \geq \quad 2jq - 4\delta j - j^2 + 3j. \tag{2}$$

The right hand side is maximized when $j = q - 2\delta + 3/2$. However, if $j = \delta + 2$, plugging into (2) and using $\delta^2 \leq q/16$ gives a contradiction. We have shown the following result.

Proposition 3.3. *Let B be any set of at most $2\delta(q+1) \leq \sqrt{q}(q+1)/2$ lines of $\mathcal{Q}(4,q)$ such that every point of $\mathcal{Q}(4,q)$ lies on either 0 or on at least 2 lines of B. Then all the lines of B lie in at most $\delta+1$ distinct hyperbolic quadrics of $\mathcal{Q}(4,q)$ having in every regulus at least $q-2\delta+1$ lines of B.*

Let $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$ be distinct hyperbolic quadrics of $\mathcal{Q}(4,q)$ having in every regulus at least $q-2\delta+1$ lines of B. Note that two distinct hyperbolic quadrics of $\mathcal{Q}(4,q)$ lie in two distinct solids. These solids necessarily intersect in a plane, and a plane intersects $\mathcal{Q}(4,q)$ in either a conic or in two lines. So two distinct hyperbolic quadrics of $\mathcal{Q}(4,q)$ share either a conic or two lines (one from each ruling class). Therefore, every regulus of $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$ contains at least $q-2\delta+1-\delta = q-3\delta+1$ lines of B not lying in any of the other hyperbolic quadrics. Let $\ell_1 \in B$, $\ell_1 \subseteq \mathcal{Q}_1$, and $\ell_1 \nsubseteq \mathcal{Q}_2, \ldots, \mathcal{Q}_{\delta+1}$. Then there are at least $q-\delta+1$ points R of ℓ_1 belonging to $\mathcal{Q}_1$, but not belonging to $\mathcal{Q}_2, \ldots, \mathcal{Q}_{\delta+1}$. All these points must lie on at least a second line of B. Since these lines all lie in $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$, but as the point $R \notin \mathcal{Q}_2 \cup \ldots \cup \mathcal{Q}_{\delta+1}$, necessarily, this second line of B through R is contained in $\mathcal{Q}_1$. So every regulus of $\mathcal{Q}_1$ contains at least $q-\delta+1$ lines of B, not lying in a second hyperbolic quadric $\mathcal{Q}_2, \ldots, \mathcal{Q}_{\delta+1}$.

We have obtained the following result.

Proposition 3.4. *Let B be any set of at most $2\delta(q+1) \leq \sqrt{q}(q+1)/2$ lines of $\mathcal{Q}(4,q)$, such that every point of $\mathcal{Q}(4,q)$ lies on either 0 or on at least 2 lines of B. Then all the lines of B lie in at most $\delta+1$ distinct hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$ of $\mathcal{Q}(4,q)$ having in every regulus at least $q-\delta+1$ lines of B that only lie in exactly one of those hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$.*

We can now deduce precise information on the coordinates in the codeword $\mathbf{c}$. Here, we identify every position in $\mathbf{c}$ with its corresponding line in $\mathcal{Q}(4,q)$ (see beginning of this section).

Let $\ell_1 \in B$, where $\mathcal{Q}_1$ is the only hyperbolic quadric of $\mathcal{Q}(4,q)$ through ℓ_1 and where $\mathcal{Q}(4,q)$ contains in every one of its reguli at least $q-\delta+1$ lines of B.

Then at least $q-\delta+1$ points R_i, $i = 1, \ldots, q-\delta+1$, of ℓ_1 belong to $\mathcal{Q}_1$, but not to $\mathcal{Q}_2, \ldots, \mathcal{Q}_{\delta+1}$. These points R_i only belong to the line ℓ_1 of B and to some line ℓ_{i+1} of the opposite regulus in $\mathcal{Q}_1$, also belonging to B since a point of $\mathcal{Q}(4,q)$ lies on zero or on at least two lines of B.

Such a point R_i, $1 \leq i \leq q-\delta+1$, defines a row of the parity check matrix H. The row corresponding to R_i is only non-zero (only considering the columns of H defined by the lines of B) in the columns defined by ℓ_1 and ℓ_{i+1}. So, since $\mathbf{c}$ is orthogonal to this row in H, up to a scalar multiple, the codeword $\mathbf{c}$ for B has 1 and -1 in the positions corresponding to ℓ_1 and ℓ_{i+1}. Hence, the codeword $\mathbf{c}$ has $(1, -1, \ldots, -1)$ in the positions of the lines $\ell_1, \ell_2, \ldots, \ell_{q-\delta+2}$, where 1 corresponds to the line ℓ_1, and the -1 correspond to the lines $\ell_2, \ldots, \ell_{q-\delta+2}$.

But now, we look at the other lines of B of the regulus of $\mathcal{Q}_1$, containing ℓ_1, and not lying in any of the other hyperbolic quadrics $\mathcal{Q}_2, \ldots, \mathcal{Q}_{\delta+1}$. In particular, there are $q-\delta+1$ lines

$\ell_1, \ell_{q-\delta+3}, \ldots, \ell_{2q-2\delta+2}$ lying in $\mathcal{Q}_1$, but not in the other hyperbolic quadrics $\mathcal{Q}_i$, $2 \leq i \leq \delta+1$. A line ℓ_k, $q-\delta+3 \leq k \leq 2q-2\delta+2$, could intersect a line ℓ_m, $2 \leq m \leq q-\delta+2$, in a point also lying in another hyperbolic quadric $\mathcal{Q}_i$, $2 \leq i \leq \delta+1$, but this happens at most δ times. Since $q-\delta+1 > \delta$, ℓ_k intersects some line ℓ_l, $2 \leq l \leq q-\delta+2$, in a point of $\mathcal{Q}_1$, not lying in $\mathcal{Q}_i$, $2 \leq i \leq \delta+1$. So, repeating the arguments for R_i, $\mathbf{c}$ has the values 1 and -1 in the positions corresponding to the lines ℓ_k and ℓ_l.

Hence, up to a scalar multiple, the codeword $\mathbf{c}$ equals

$$\mathbf{c} = (1, -1, \ldots, -1, 1, \ldots, 1, \ldots)$$

where the $q-\delta+1$ lines $\ell_1, \ell_{q-\delta+3}, \ldots, \ell_{2q-2\delta+2}$ of B have the scalar 1 in their corresponding positions and the $q-\delta+1$ lines ℓ_l, $2 \leq l \leq q-\delta+2$, of B have scalar -1 in their corresponding positions. Now let $\mathbf{c}'$ be the codeword of weight $2q+2$ defined by the hyperbolic quadric $\mathcal{Q}_1$. Up to a scalar multiple, this codeword can be made to agree with $\mathbf{c}$ in the $2q-2\delta+2$ positions corresponding to $\ell_1, \ldots, \ell_{2q-2\delta+2}$. So $w(\mathbf{c}-\mathbf{c}') \leq w(\mathbf{c}) + (2q+2) - 2(2q-2\delta+2) = w(\mathbf{c}) - 2q + 4\delta - 2 < w(\mathbf{c})$.

By induction on the weights of the codewords, we can assume that such codewords are already characterized as being a linear combination of codewords of weight $2(q+1)$, so as a linear combination of reguli and opposite reguli of hyperbolic quadrics contained in $\mathcal{Q}(4,q)$. Adding $\mathbf{c}'$ back, also $\mathbf{c}$ is a linear combination of codewords of weight $2(q+1)$ of the LDPC code defined by $\mathcal{W}(q)$.

Proposition 3.5. *In the LDPC code defined by $\mathcal{W}(q)$, every codeword of weight at most $\sqrt{q}(q+1)/2$ is a linear combination of codewords of minimal weight $2(q+1)$.*

Remark 3.6. The same result is valid for the LDPC code $\mathcal{C}$ arising from the generalized quadrangle $\mathcal{H}(3,q^2)$. We again describe the situation on the dual generalized quadrangle $\mathcal{Q}^-(5,q)$. A codeword $\mathbf{c}$ of $\mathcal{C}$ corresponds to a set B of lines of $\mathcal{Q}^-(5,q)$ such that every point of $\mathcal{Q}^-(5,q)$ lies on zero or on at least 2 lines of B. The smallest weight codewords correspond to the lines of a regulus $\mathcal{R}$ and its opposite regulus $\mathcal{R}^{opp}$, contained in $\mathcal{Q}^-(5,q)$. It can be checked that our valid results for $\mathcal{Q}(4,q)$ are also valid for $\mathcal{Q}^-(5,q)$. This shows that we can repeat the conclusions of Proposition 3.5, but now for $\mathcal{H}(3,q^2)$.

Proposition 3.7. *In the LDPC code defined by $\mathcal{H}(3,q^2)$, every codeword of weight at most $\sqrt{q}(q+1)/2$ is a linear combination of codewords of minimal weight $2(q+1)$.*

4 Minimum weight of the LDPC code of $\mathcal{Q}(4,q)$, q odd

For q even, $\mathcal{W}(q)$ is self-dual (Theorem 2.1 (2)), so the preceding results also give characterization results on the small weight codewords of the LDPC code defined by $\mathcal{W}(q)^D = \mathcal{Q}(4,q)$.

For q odd, $\mathcal{W}(q)$ is not self-dual. This can also be seen by the fact that the results for the LDPC code defined by $\mathcal{W}(q)^D = \mathcal{Q}(4,q)$ are different from those for the LDPC code defined by $\mathcal{W}(q)$.

We now improve greatly the lower bound $d \geq 2(q+2)$ on the minimum distance of the LDPC code arising from $\mathcal{Q}(4,q)$, q odd (Table 1).

From Property (*), codewords in the LDPC code arising from $\mathcal{Q}(4,q)$ define sets of points in the parabolic quadric $\mathcal{Q}(4,q)$ with the property that every line of $\mathcal{Q}(4,q)$ meets these point sets in 0 or in at least 2 points. Let S be a set of points of $\mathcal{Q}(4,q)$ with this property.

Lemma 4.1. *Let x be the maximal size of intersection of S with a conic C of $\mathcal{Q}(4,q)$. Then $|S| \geq x(q+1)/2$.*

Proof. Let C be a conic of $\mathcal{Q}(4,q)$ containing x points of S. The points of $S \cap C$ lie on $x(q+1)$ lines of $\mathcal{Q}(4,q)$. Using properties of the parabolic quadric $\mathcal{Q}(4,q)$, q odd, there are at most 2 points collinear with all points of C [18]. We subtract $2x$ to not consider the incidences of these points with the lines of $\mathcal{Q}(4,q)$ through the points of $S \cap C$. So, there are at least $x(q-1)$ other lines of $\mathcal{Q}(4,q)$ through the points of $S \cap C$. They all contain at least one point of S not in C.

A point of $\mathcal{Q}(4,q)$, not collinear with all points of C, is collinear with at most two points of $S \cap C$. So, there are at least $x(q-1)/2$ other points in S. Adding the x points of $S \cap C$, $|S| \geq x(q-1)/2 + x = x(q+1)/2$. □

Lemma 4.2. *Let x be the maximal size of intersection of S with a conic of $\mathcal{Q}(4,q)$, q odd. Then,*

$$|S| \geq \frac{q^2}{2x} + 3\frac{q}{2} + \frac{x}{8} + 2.$$

Proof. Select a point P of S and consider the $q+1$ lines of $\mathcal{Q}(4,q)$ through P. They all contain at least one other point P_i, $i = 0, \ldots, q$, of S. The points $P_0, \ldots, P_q$ are pairwise non-collinear.

Each point P_i, $i = 0, \ldots, q$, is collinear with at least $q+1$ other points of S, P included.

For $P_i \neq P_j$, $P_i^\perp \cap P_j^\perp$ is a conic of $\mathcal{Q}(4,q)$, containing at most x points of S. Then

$$|S| \geq |\cup_{j=0}^{i} (P_j^\perp \cap S) \setminus \{P, P_j\}| \geq \sum_{j=0}^{i} (q - jx) = q(i+1) - \frac{xi(i+1)}{2} = f(i).$$

The maximum for $f(i)$ is obtained for $i = (2q-x)/(2x)$. Plugging this value into f gives $f\left(\frac{2q-x}{2x}\right) = \frac{q^2}{2x} + \frac{q}{2} + \frac{x}{8}$. Adding the points $P, P_0, \ldots, P_q$ gives

$$|S| \geq \frac{q^2}{2x} + 3\frac{q}{2} + \frac{x}{8} + 2.$$

□

We do not know the exact value for x. But for varying x, one of the two expressions of the two preceding lemmas gives a better bound on $|S|$. Note that, as a function of x, the first expression is always increasing and the second expression is always decreasing for $1 \leq x \leq q+1$. Hence, if the two expressions in x are equal, then the corresponding value for x provides a lower bound on $|S|$ no matter what the actual value of x is. Hence, we consider when the two expressions are equal:

$$\frac{x(q+1)}{2} = \frac{q^2}{2x} + \frac{3q}{2} + \frac{x}{8} + 2.$$

This is valid for

$$x = \frac{8 + 6q + 4\sqrt{(q+1)^3 + 3q + 3}}{3 + 4q}.$$

So

$$|S| \geq \frac{(q+1)x}{2} = \frac{(q+1)(4 + 3q + 2\sqrt{(q+1)^3 + 3q + 3})}{3 + 4q}.$$

Theorem 4.3. *The LDPC code arising from $\mathcal{Q}(4,q)$, q odd, has minimum distance at least*

$$\frac{(q+1)(4+3q+2\sqrt{(q+1)^3+3q+3})}{3+4q} \approx \frac{(q+1)\sqrt{q}}{2}.$$

Computer searches gave the following exact values for the minimum distance of binary LDPC codes arising from $\mathcal{Q}(4,q)$, q odd, q small.

Theorem 4.4. *The minimum distances of the binary LDPC codes arising from $\mathcal{Q}(4,3)$ and $\mathcal{Q}(4,5)$ are 10 and 20, respectively.*

5 Minimum weight of codewords in $\mathcal{H}(4,q^2)^D$

We now consider the Hermitian variety $\mathcal{U}$ in $PG(4,q^2)$ defining the GQ $\mathcal{H}(4,q^2)$. In this setting, we will make use of the isomorphism between $\mathcal{H}(3,q^2)^D$ and $\mathcal{Q}^-(5,q)$ (Theorem 2.1 (3)).

Lemma 5.1. ([18]) *For three pairwise skew lines ℓ_1,ℓ_2 and ℓ_3 of $\mathcal{H}(3,q^2)$, $|\{\ell_1,\ell_2,\ell_3\}^\perp| = q+1$.*

Lemma 5.2. *Every non-zero codeword of the LDPC code defined by $\mathcal{H}(4,q^2)^D$ has weight at least $q\sqrt{(q^2+1)(q-1)}+q^2+2$.*

Proof. First note that such a codeword corresponds to a set B of lines of $\mathcal{H}(4,q^2)$ such that every point of $\mathcal{H}(4,q^2)$ lies on zero or on at least two lines of B (Property (**)). Let $\ell_1 \in B$ and let $m_1,\ldots,m_{q^2+1}$ be lines of B intersecting ℓ_1 in distinct points.

The lines $m_1,\ldots,m_{q^2+1}$ cover $(q^2+1)q^2$ points not belonging to ℓ_1. There are still $x = |B|-q^2-2$ lines in B. One of these lines $\ell_2 \in B$ intersects at least $\eta = \frac{(q^2+1)q^2}{x}$ of the lines $m_1,\ldots,m_{q^2+1}$. Let these lines be $m_1,\ldots,m_\eta$. The lines $m_1,\ldots,m_\eta$ cover $\frac{(q^2+1)q^2}{x}(q^2-1)$ points not belonging to $\ell_1 \cup \ell_2$.

For a line ℓ_3 skew to ℓ_1 and ℓ_2, we have that $|\{\ell_1,\ell_2,\ell_3\}^\perp| \leq q+1$. So, a third line of B intersects at most $q+1$ of the lines $m_1,\ldots,m_\eta$. So, necessarily

$$x(q+1) \geq \frac{(q^2+1)q^2(q^2-1)}{x}$$

or, equivalently,

$$x \geq q\sqrt{(q^2+1)(q-1)}.$$

So, $|B| \geq x+q^2+2 \geq q\sqrt{(q^2+1)(q-1)}+q^2+2$. □

Table 2 summarizes the new bounds on the minimum distances of LDPC codes defined by the (dual) classical generalized quadrangles. The new lower bounds on the minimum distance d for the LDPC codes arising from $\mathcal{Q}(4,q)$, q odd, and $\mathcal{H}(4,q^2)^D$ are written in boldface. In these two cases, we have improved greatly the bounds of Table 1 given in [13] or Table 1 of Section 2.

LDPC code	Order (s,t)	d
$\mathcal{W}(q)$, $q=2^e$	(q,q)	$2(q+1)$
$\mathcal{W}(q)$, q odd	(q,q)	$2(q+1)$
$\mathcal{Q}(4,q)$, q odd	(q,q)	$\gtrapprox \frac{(\mathbf{q+1})\sqrt{\mathbf{q}}}{\mathbf{2}}$
$\mathcal{Q}^-(5,q)$	(q,q^2)	$\geq (q+1)(q^2-q+2)$
$\mathcal{H}(3,q^2)$	(q^2,q)	$2(q+1)$
$\mathcal{H}(4,q^2)$	(q^2,q^3)	$\geq (q^2+1)(q^3-q^2+2)$
$\mathcal{H}(4,q^2)^D$	(q^3,q^2)	$\geq \mathbf{q\sqrt{(q^2+1)(q-1)}+q^2+2}$

Table 2: New minimum distances of GQ LDPC codes

6 The codes $\mathbf{LU}(3,q)$ from $H(3,q)$ and $H(3,q)^T$

We are again interested in the characterization of the small weight codewords of $\mathrm{LU}(3,q)$ from $H(3,q)$, and in a lower bound on the minimum weight of the code $\mathrm{LU}(3,q)$ from $H(3,q)^T$.

6.1 The incidence structures from $H(3,q)$ and $H(3,q)^T$

Recently, a lot of attention has been paid to the LDPC codes $\mathrm{LU}(3,q)$ arising from the incidence matrices $H(3,q)$ and $H(3,q)^T$ [10],[20]. To simplify the notations, we denote the code $\mathrm{LU}(3,q)$ from $H(3,q)$ by $\mathrm{LU}_H(3,q)$ and the code $\mathrm{LU}(3,q)$ from $H(3,q)^T$ by $\mathrm{LU}_{H^T}(3,q)$. We note that $\Gamma(H(3,q)^T)=\Gamma(H(3,q))^D$. As indicated in the introduction, the incidence structure $\Gamma(H(3,q))$ arises from the generalized quadrangle $\mathcal{W}(q)$, defined by a symplectic polarity η. Select a point P of $\mathcal{W}(q)$ and a line ℓ of $\mathcal{W}(q)$, where $P\in\ell$. Then the points of $\Gamma(H(3,q))$ are the points of $\mathcal{W}(q)\setminus P^\perp$, and the lines of $\Gamma(H(3,q))$ are the lines of $\mathcal{W}(q)\setminus \ell^\perp$. We will briefly denote this by $\Gamma(H(3,q))=\mathcal{W}(q)\setminus(P^\perp\cup\ell^\perp)$. In particular, this implies that the points of $\Gamma(H(3,q))$ coincide with the points of the affine 3-dimensional space $PG(3,q)\setminus P^\perp$.

Since $\mathcal{Q}(4,q)$ is dual to $\mathcal{W}(q)$, we can define the dual structure $\Gamma(H(3,q))^D$ directly on $\mathcal{Q}(4,q)$. Namely, the incidence structure $\Gamma(H(3,q))^D$ arises from the generalized quadrangle $\mathcal{Q}(4,q)$. Select again a point P of $\mathcal{Q}(4,q)$ and a line ℓ of $\mathcal{Q}(4,q)$, where $P\in\ell$. Omit the points R of $\mathcal{Q}(4,q)$ lying in $P^\perp$, and omit the lines m of $\mathcal{Q}(4,q)$ lying in $\ell^\perp$. We again denote this by $\Gamma(H(3,q))^D=\mathcal{Q}(4,q)\setminus(P^\perp\cup\ell^\perp)$.

In particular, this implies that the points of $\Gamma(H(3,q))^D$ coincide with the points of the set $\mathcal{Q}(4,q)\setminus P^\perp$, which is contained in an affine 4-space of $PG(4,q)$. This also implies that from every hyperbolic quadric $\mathcal{Q}^+(3,q)$ of $\mathcal{Q}(4,q)$, at most q lines of every regulus are lines of $\Gamma(H(3,q))^D$. More precisely, if P belongs to this hyperbolic quadric, but the hyperbolic quadric does not contain ℓ, then the two lines of this hyperbolic quadric through P are not lines of $\Gamma(H(3,q))^D$. If the hyperbolic quadric does not pass through P, then this hyperbolic quadric intersects $\mathcal{Q}(4,q)\cap P^\perp$ in a conic C. This conic C intersects ℓ in one point R, and the two lines of $\mathcal{Q}^+(3,q)$ passing through R are no longer lines of $\Gamma(H(3,q))^D$. If the hyperbolic quadric contains ℓ, only the q remaining lines of this hyperbolic quadric in the regulus of ℓ are lines of $\Gamma(H(3,q))^D$, and none of the lines of the opposite regulus are lines of $\Gamma(H(3,q))^D$.

6.2 Codewords of small weight in $\mathbf{LU}_H(3,q)$

In this section we characterize the small weight codewords of $\mathrm{LU}_H(3,q)$.

The codewords of $\mathrm{LU}_H(3,q)$ define point sets B of $\Gamma(H(3,q))$ such that every line of $\Gamma(H(3,q))$ contains zero or at least two points of B (Property (*)). We will describe this directly in the dual structure $\Gamma(H(3,q))^D$. So a codeword defines a set B of lines of $\Gamma(H(3,q))^D = \mathcal{Q}(4,q) \setminus (P^\perp \cup \ell^\perp)$ such that every point of $\Gamma(H(3,q))^D$ lies on zero or on at least two of the lines of B.

The columns of the parity check matrix $H(3,q)$ of $\mathrm{LU}_H(3,q)$ correspond to the points of $\Gamma(H(3,q))$, and the rows of $H(3,q)$ correspond to the lines of $\Gamma(H(3,q))$. Since we will consider everything in $\Gamma(H(3,q))^D$, the columns of the parity check matrix $H(3,q)$ of $\mathrm{LU}_H(3,q)$ correspond to the lines of $\Gamma(H(3,q))^D = \mathcal{Q}(4,q) \setminus (P^\perp \cup \ell^\perp)$, and the rows of $H(3,q)$ correspond to the points of $\Gamma(H(3,q))^D = \mathcal{Q}(4,q) \setminus (P^\perp \cup \ell^\perp)$.

We summarize these observations since we will rely on them greatly in the next proofs.

(1) A codeword $\mathbf{c}$ of the LDPC code $\mathrm{LU}_H(3,q)$ defines a set B of lines of $\Gamma(H(3,q))^D = \mathcal{Q}(4,q) \setminus (P^\perp \cup \ell^\perp)$ such that every point of $\Gamma(H(3,q))^D$ lies on zero or on at least two of the lines of B.

(2) The columns of the parity check matrix $H(3,q)$ of $\mathrm{LU}_H(3,q)$ correspond to the lines of $\Gamma(H(3,q))^D = \mathcal{Q}(4,q) \setminus (P^\perp \cup \ell^\perp)$, and the rows of $H(3,q)$ correspond to the points of $\Gamma(H(3,q))^D = \mathcal{Q}(4,q) \setminus (P^\perp \cup \ell^\perp)$.

The minimum weight of $\mathrm{LU}_H(3,q)$ is equal to $2q$ [10]. To find the codewords of weight $2q$ geometrically, we describe them in the dual structure $\Gamma(H(3,q))^D$. In $\Gamma(H(3,q))^D$, they define a set B of $2q$ lines such that every point of $\Gamma(H(3,q))^D$ belongs to zero or two lines of B.

The codewords of weight $2q$ in $\mathrm{LU}_H(3,q)$ correspond to the sets B consisting of the $2q$ lines of a hyperbolic quadric $\mathcal{Q}^+(3,q)$ contained in $\mathcal{Q}(4,q)$, and passing through P and not containing ℓ. Every point of $\mathcal{Q}^+(3,q)$, not lying in $P^\perp$, lies on two of these lines. The codeword of weight $2q$ corresponding to the $2q$ lines of B is defined by giving the positions corresponding to the q lines of B in a first regulus of $\mathcal{Q}^+(3,q)$ the coordinate 1, the positions corresponding to the q lines of B in the opposite regulus of $\mathcal{Q}^+(3,q)$ the coordinate -1, and all other positions the coordinate zero. In this way, a vector orthogonal to all rows of $H(3,q)$ is obtained.

Remark 6.1. Since $\mathrm{LU}(3,q)^D = \mathcal{Q}(4,q) \setminus (P^\perp \cup \ell^\perp)$, not all the hyperbolic quadrics $\mathcal{Q}^+(3,q)$ of $\mathcal{Q}(4,q)$ define codewords of weight $2q$ of $\mathrm{LU}_H(3,q)$.

Namely, consider a hyperbolic quadric $\mathcal{Q}^+(3,q)$ containing the line ℓ, then all the lines of the regulus of $\mathcal{Q}^+(3,q)$ containing the lines intersecting ℓ are no longer lines of $\Gamma(H(3,q))^D$. Only the q lines of the regulus containing ℓ are lines of $\Gamma(H(3,q))^D$, so this hyperbolic quadric does not define a set of lines such that every point of $\Gamma(H(3,q))^D$ lies on zero or on at least two lines of $\Gamma(H(3,q))^D$.

Similarly, consider a hyperbolic quadric $\mathcal{Q}^+(3,q)$ not passing through P and not containing ℓ. This intersects $P^\perp$ in a conic C. This conic shares one point R with ℓ. The two lines ℓ_1 and ℓ_2 of $\mathcal{Q}^+(3,q)$ passing through R are not lines of $\Gamma(H(3,q))^D$, so the points of $\ell_1 \setminus \{R\}$ and of $\ell_2 \setminus \{R\}$ are only lying on one line of $\Gamma(H(3,q))^D$ contained in $\mathcal{Q}^+(3,q)$. So, again this hyperbolic quadric

does not define a set of lines of $\Gamma(H(3,q))^D$ such that every point of $\Gamma(H(3,q))^D$ lies on zero or on at least two lines of $\mathcal{Q}^+(3,q)$.

Hence, the only hyperbolic quadrics $\mathcal{Q}^+(3,q)$ of $\mathcal{Q}(4,q)$ defining codewords of weight $2q$ in $\mathrm{LU}_H(3,q)$ are the hyperbolic quadrics passing through P, and not containing ℓ.

The next examples and our characterization results on the codewords of small weight of $\mathrm{LU}_H(3,q)$ however will show that it is possible to use linear combinations of hyperbolic quadrics of $\mathcal{Q}(4,q)$, not containing P and not containing ℓ, to define codewords of weight larger than $2q$ in $\mathrm{LU}_H(3,q)$.

We now present some codewords of $\mathrm{LU}_H(3,q)$ having a larger weight; we again describe them as sets of lines of $\Gamma(H(3,q))^D$.

Consider the tangent cone to $\mathcal{Q}(4,q)$ in the point P, and let R be a fixed point of $\mathcal{Q}(4,q)$ on the line ℓ, with $R \neq P$. Consider also two fixed lines ℓ_1 and ℓ_2 of $\mathcal{Q}(4,q)$, different from ℓ, passing through R. Let π be the plane defined by ℓ_1 and ℓ_2. The hyperplane $\langle \pi, P\rangle$ is the tangent hyperplane to $\mathcal{Q}(4,q)$ in the point R. All q other hyperplanes through the plane π intersect $\mathcal{Q}(4,q)$ in hyperbolic quadrics $\mathcal{Q}^+(3,q)_1,\ldots,\mathcal{Q}^+(3,q)_q$. We will now use the lines of $\Gamma(H(3,q))^D$ lying in these hyperbolic quadrics $\mathcal{Q}^+(3,q)_1,\ldots,\mathcal{Q}^+(3,q)_q$ to construct codewords in the LDPC code $\mathrm{LU}_H(3,q)$.

Let $\mathcal{R}_1^{(i)}$ be the regulus of $\mathcal{Q}^+(3,q)_i$ passing through the line ℓ_1, and let $\mathcal{R}_2^{(i)}$ be the regulus of $\mathcal{Q}^+(3,q)_i$ passing through the line ℓ_2.

We construct a codeword $\mathbf{c}_i$ in the LDPC code arising from $\mathcal{W}(q)$. Construct the vectors $\mathbf{c}_i$ having coordinate one in the positions corresponding to the lines of $\mathcal{R}_1^{(i)}$, coordinate -1 in the positions corresponding to the lines of $\mathcal{R}_2^{(i)}$, and zero elsewhere. These are codewords of the LDPC code arising from $\mathcal{Q}(4,q)^D = \mathcal{W}(q)$, but they are not codewords of $\mathrm{LU}_H(3,q)$ since the positions corresponding to the lines ℓ_1 and ℓ_2 are equal to 1 and -1.

But making the difference $\mathbf{c}_1 - \mathbf{c}_2$ of two of such codewords gives a new codeword of the LDPC code arising from $\mathcal{W}(q)$ which has zero in the positions corresponding to ℓ_1 and ℓ_2, and in all the other positions of lines of $\mathcal{Q}(4,q)$ in $\ell^\perp$. Shortening this codeword by cancelling all positions corresponding to lines of $\ell^\perp$, a codeword of $\mathrm{LU}_H(3,q)$ is obtained of weight $4q$.

Generalizing this to $2m$ hyperbolic quadrics $\mathcal{Q}^+(3,q)_1,\ldots,\mathcal{Q}^+(3,q)_{2m}$. By considering the codeword $\mathbf{c}_1+\cdots+\mathbf{c}_m-\mathbf{c}_{m+1}-\cdots-\mathbf{c}_{2m}$, a codeword of weight $4mq$ in the LDPC code defined by $\mathcal{W}(q)$ is obtained, which has zero in the positions of the lines ℓ_1 and ℓ_2, and in all the other positions of lines of $\mathcal{Q}(4,q)$ in $\ell^\perp$. Shortening this codeword by cancelling all positions corresponding to lines of $\ell^\perp$, a codeword of $\mathrm{LU}_H(3,q)$ is obtained of weight $4mq$.

Analogously, but just for non-binary LDPC codes, consider $2m+1$ hyperbolic quadrics $\mathcal{Q}^+(3,q)_1$, $\ldots$, $\mathcal{Q}^+(3,q)_{2m+1}$. By considering the codeword $\mathbf{c}_1+\mathbf{c}_2+\cdots+\mathbf{c}_{m+1}-2\mathbf{c}_{m+2}-\mathbf{c}_{m+3}-\cdots-\mathbf{c}_{2m+1}$, a codeword of weight $(4m+2)q$ in the LDPC code defined by $\mathcal{W}(q)$ is obtained, which has zero in the positions of the lines ℓ_1 and ℓ_2, and in all the other positions of lines in $\ell^\perp$. Shortening this codeword by cancelling all positions corresponding to lines of $\ell^\perp$, a codeword of $\mathrm{LU}_H(3,q)$ is obtained of weight $(4m+2)q$.

Adding linear combinations of codewords of $\mathrm{LU}_H(3,q)$ of minimal weight $2q$ to these codewords, new small weight codewords of $\mathrm{LU}_H(3,q)$ are obtained.

We will prove that the codewords of $\mathrm{LU}_H(3,q)$ of weight smaller than or equal to $\sqrt{q}q/2$ are, modulo linear combinations of codewords of minimal weight $2q$, obtained by shortening codewords of weight at most $\sqrt{q}q/2$, in the LDPC code defined by $\mathcal{W}(q)$, where these codewords have zero in the positions of the lines of $\ell^\perp$. By Proposition 3.5, these codewords of $\mathcal{W}(q)$ are linear combinations of codewords of minimal weight $2(q+1)$; in other words, they arise from the reguli and opposite reguli of hyperbolic quadrics contained in $\mathcal{Q}(4,q)$.

We summarize this since this will also be the induction hypothesis on which we will rely in the proofs that follow.

Remark 6.2. We will characterize the codewords of $\mathrm{LU}_H(3,q)$ of weight smaller than or equal to $\sqrt{q}q/2$ in the following way.

The codewords of $LU_H(3,q)$ of weight smaller than or equal to $\sqrt{q}q/2$ are, modulo linear combinations of codewords of minimal weight $2q$, obtained by shortening codewords of weight at most $\sqrt{q}q/2$, in the LDPC code defined by $\mathcal{W}(q)$, where these codewords have zero in the positions of the lines of $\ell^\perp$. By Proposition 3.5, these codewords in the LDPC code of $\mathcal{W}(q)$ are linear combinations of codewords of minimal weight $2(q+1)$; in other words, they arise from the reguli and opposite reguli of hyperbolic quadrics contained in $\mathcal{Q}(4,q)$.

Using geometric arguments, we first prove that the minimum weight of the code $\mathrm{LU}_H(3,q)$ is equal to $2q$, which was also given in [10], and that these codewords of minimum weight correspond to hyperbolic quadrics of $\mathcal{Q}(4,q)$ passing through P, and not containing ℓ.

Lemma 6.3. ([10]) *The minimum weight of the code $LU_H(3,q)$ is equal to $2q$, and the codewords of minimum weight correspond to hyperbolic quadrics of $\mathcal{Q}(4,q)$ passing through P, and not containing ℓ.*

Proof. Let $\mathbf{c}$ be a codeword of $\mathrm{LU}_H(3,q)$ of weight at most $2q$, and let B be the corresponding set of lines of $\mathcal{Q}(4,q)$. By Property (**), every point of $\mathrm{LU}(3,q)^D = \mathcal{Q}(4,q) \setminus (P^\perp \cup \ell^\perp)$ lies on zero or on at least two lines of B.

Let ℓ_1 be a first line of B. The q points of ℓ_1 each lie on at least a second line of B. Let $\ell_2, \ldots, \ell_{q+1}$ be lines of B intersecting ℓ_1 in distinct points of $\Gamma(H(3,q))^D$.

The $q-1$ points of $\Gamma(H(3,q))^D$ lying in $\ell_2 \setminus \ell_1$ all still need to lie on a second line of B. Let $\ell_{q+2}, \ldots, \ell_{2q}$ be the lines of B intersecting $\ell_2 \setminus \ell_1$ in the $q-1$ distinct points of $\Gamma(H(3,q))^D$.

Necessarily, $|B| = 2q$ and $B = \{\ell_1, \ldots, \ell_{2q}\}$. Since every point of $\ell_2, \ldots, \ell_{q+1}$ must lie on a second line of B, necessarily, the lines ℓ_i, $i = 2, \ldots, q+1$, intersect the lines ℓ_j, $j = q+2, \ldots, 2q$, in a point of $\Gamma(H(3,q))^D$.

This shows that B consists of $2q$ lines of a hyperbolic quadric $\mathcal{Q}^+(3,q)$. If this hyperbolic quadric does not pass through P or contains ℓ, then it cannot define a codeword of $\mathrm{LU}_H(3,q)$ (Remark 6.1), so this hyperbolic quadric passes through P, and does not contain ℓ.

We have characterized the codewords of minimum weight in $\mathrm{LU}_H(3,q)$. □

To characterize codewords of small weight in $\mathrm{LU}_H(3,q)$, a lot of the arguments of Section 3 can be repeated, but the final characterization of these small weight codewords is more complicated to

obtain, due to the fact that $\Gamma(H(3,q))^D$ only contains part of the points and lines of the generalized quadrangle $\mathcal{Q}(4,q)$.

In particular, $\Gamma(H(3,q))^D$ only contains the points of $\mathcal{Q}(4,q) \setminus P^\perp$, so this means that only the points of $\mathcal{Q}(4,q)$ lying in an affine 4-space are used. This implies that a line of $\Gamma(H(3,q))^D$ only contains q points of $LU(3,q)^D$. The $(q+1)$-th point in $PG(4,q)$ of this line belongs to $P^\perp$, so is not considered to be a point of $\Gamma(H(3,q))^D$.

This has as particular consequence that a lot of the arguments of Section 3 can be repeated, but the value $q+1$, which is the size of a line in $PG(4,q)$, must be replaced by the value q, which is the size of a line in $\Gamma(H(3,q))^D$.

We summarize the most important results.

Lemma 6.4. *Let $\mathbf{c}$ be a codeword of weight at most $2\delta q \leq \sqrt{q}q/2$ of the LDPC code $LU_H(3,q)$, then $\mathbf{c}$ defines a set B of at most $\sqrt{q}q/2$ lines of $\Gamma(H(3,q))^D$ such that every point of $\Gamma(H(3,q))^D$ lies on zero or on at least two lines of B. Moreover,*

(1) *If the line ℓ_1 is in B, then there is a hyperbolic quadric $\mathcal{Q} \cong \mathcal{Q}^+(3,q)$ of $\mathcal{Q}(4,q)$ containing ℓ_1 and such that each regulus of $\mathcal{Q}$ contains at least $q-2\delta$ lines of B.*

(2) *All the lines of B lie in at most $\delta+1$ distinct hyperbolic quadrics $\mathcal{Q}_1,\ldots,\mathcal{Q}_{\delta+1}$ of $\mathcal{Q}(4,q)$ having in both their reguli at least $q-2\delta$ lines of B.*

(3) *All the lines of B lie in at most $\delta+1$ distinct hyperbolic quadrics $\mathcal{Q}_1,\ldots,\mathcal{Q}_{\delta+1}$ of $\mathcal{Q}(4,q)$ having in both their reguli at least $q-\delta$ lines of B, only lying in one of those hyperbolic quadrics $\mathcal{Q}_1,\ldots,\mathcal{Q}_{\delta+1}$.*

(4) *Every hyperbolic quadric $\mathcal{Q}_i$, $i=1,\ldots,\delta+1$, contains, in both its reguli, at least $q-\delta$ lines of B lying in none of the other hyperbolic quadrics $\mathcal{Q}_j$, $j \neq i$.*

These $q-\delta$ lines $\ell_1,\ldots,\ell_{q-\delta}$ of B of one regulus of $\mathcal{Q}_i$ all have the same value α_i in their corresponding coordinate position of $\mathbf{c}$, and these $q-\delta$ lines $\ell_{q-\delta+1},\ldots,\ell_{2q-2\delta}$ of B of the opposite regulus of $\mathcal{Q}_i$ all have the value $-\alpha_i$ in their corresponding coordinate position of $\mathbf{c}$.

Proof. (1) Analogue to Proposition 3.1.
(2) Analogue to Proposition 3.3.
(3) Analogue to Proposition 3.4.
(4) Analogue to paragraphs following Proposition 3.4. □

Note that since the hyperbolic quadrics $\mathcal{Q}_i$ have at least $q-\delta$ lines of B, so of $\Gamma(H(3,q))^D$, these hyperbolic quadrics cannot contain the line ℓ (Remark 6.1).

Now the difference with the proofs of the LDPC code defined by $\mathcal{W}(q)$ arises. If one of these hyperbolic quadrics $\mathcal{Q}_i$ passes through P, then it defines a codeword $\mathbf{c}_i'$ of weight $2q$ in $\mathrm{LU}_H(3,q)$. Let $\ell_1,\ldots,\ell_{2q-2\delta}$ be the lines mentioned in Lemma 6.4 (4). We can make sure that the coordinates in $\mathbf{c}_i'$ in the positions corresponding to the lines $\ell_1,\ldots,\ell_{2q-2\delta}$ are equal to the coordinates in the corresponding positions in $\mathbf{c}$. Hence, $\mathbf{c}-\mathbf{c}_i'$ defines a codeword of weight at most $w(\mathbf{c})+2q-2(2q-2\delta) < w(\mathbf{c})$. By induction on the weight of the codewords, we can assume that

these codewords are described as in Remark 6.2, so also $\mathbf{c}$ is described as in Remark 6.2.

From now on, we will assume that none of the hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$ passes through P. Then the characterization of the codeword $\mathbf{c}$ needs to be done in a more elaborate way.

Let $\mathcal{Q}_i$ be one of the hyperbolic quadrics, containing in each of its reguli at least $q - \delta$ lines of B. Lemma 6.4 (4) shows that it is possible to associate to every regulus $\mathcal{R}_1^{(i)}$ of $\mathcal{Q}_i$ a value denoted by α_i, and to its opposite regulus $\mathcal{R}_2^{(i)}$ the value $-\alpha_i$. The meaning of this value is that every line of $\mathcal{R}_1^{(i)}$, not lying in a second hyperbolic quadric $\mathcal{Q}_j$, $j \neq i$, has this value α_i in its position in the codeword $\mathbf{c}$, and that every line of $\mathcal{R}_2^{(i)}$, not lying in a second hyperbolic quadric $\mathcal{Q}_j$, $j \neq i$, has this value $-\alpha_i$ in its position in the codeword $\mathbf{c}$.

Let m be a line of $\Gamma(H(3,q))^D$ lying in at least two of the hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$. Assume that m belongs to the hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$, and assume that m lies in the reguli $\mathcal{R}_1^{(1)}, \ldots, \mathcal{R}_1^{(r)}$. To these reguli correspond the values $\alpha_1, \ldots, \alpha_r$. We will show that the coordinate position of the line m in the codeword $\mathbf{c}$ has as value the sum $c_m = \alpha_1 + \cdots + \alpha_r$.

Consider again the line m. There are at least $q - \delta$ lines of $\Gamma(H(3,q))^D$ lying in the opposite reguli of $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$ lying in precisely one of the hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$. These latter lines all belong to B, and have values $-\alpha_1, \ldots, -\alpha_r$ in their coordinate positions in the codeword $\mathbf{c}$.

It is possible to find a point R on m, only lying in the hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$, and only lying on lines $m_1, \ldots, m_r$ of the opposite reguli of $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$ which lie in precisely one of those hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$. This is possible since $q - (\delta+2)\delta > 0$.

The codeword $\mathbf{c}$ is orthogonal to the row of $H = H(3,q)$ defined by R.

So, since the sum of all the values of $\mathbf{c}$ in the coordinate positions of the lines of B passing through R must be zero, necessarily m must have the value $\alpha_1 + \cdots + \alpha_r$ in its coordinate position. If $\alpha_1 + \cdots + \alpha_r \neq 0$, then $m \in B$, else $m \notin B$.

So, we have found the value in the coordinate positions of the codeword $\mathbf{c}$ in the lines of $\Gamma(H(3,q))^D$ lying in at least two of the hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$.

There is still one remaining possibility regarding the lines of the hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$. Each of these hyperbolic quadrics contains two lines intersecting the line ℓ in a point different from P. These are not lines of $\Gamma(H(3,q))^D$, but they are lines of $\mathcal{Q}(4,q)$.

Let m be such a line. Assume that it belongs to the hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$, and assume that m lies in the reguli $\mathcal{R}_1^{(1)}, \ldots, \mathcal{R}_1^{(r)}$ to which the values $\alpha_1, \ldots, \alpha_r$ correspond. The same arguments as above show that it is possible to associate the sum $c_m = \alpha_1 + \cdots + \alpha_r$ to the line m. The meaning of this value is as follows. If we consider the line m, then it is a line of $\mathcal{Q}(4,q)$ not considered to be a line of $\Gamma(H(3,q))^D$ since it intersects ℓ. But it contains q points R' of $\Gamma(H(3,q))^D$. It is possible to select a point R' similar to the point R of the preceding paragraphs, and to repeat the arguments for R, but now for R'. The codeword $\mathbf{c}$ must be orthogonal to the row defined by R'. So if R' is a point of m only lying in the hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$, then the scalar product of the codeword $\mathbf{c}$ with the row of H defined by R' is zero. But this scalar product is in fact the sum $\alpha_1 + \cdots + \alpha_r$. So $\alpha_1 + \cdots + \alpha_r = 0$.

These preceding results show that if we interpret $\mathbf{c}$ as a codeword of the LDPC code arising from

$\mathcal{W}(q)$ by again including the positions of the lines of $\mathcal{Q}(4,q)$ lying in $\ell^\perp$, by writing the values c_m in the positions corresponding to the lines m of $\ell^\perp$, then in fact we have a codeword of the LDPC code defined by $\mathcal{W}(q)$ which is a linear combination of the minimum weight codewords defined by the hyperbolic quadrics $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$. The lines of $\mathcal{Q}_1, \ldots, \mathcal{Q}_{\delta+1}$ intersecting ℓ have the value zero in their coordinate position. Hence, it is possible to shorten this codeword by cancelling the positions corresponding to the lines of $\ell^\perp$, and to obtain a codeword $\mathbf{c}'$ of the LDPC code $\mathrm{LU}_H(3,q)$. Now $\mathbf{c}$ is characterized as in Remark 6.2.

We have obtained the following result.

Theorem 6.5. *The codewords of $LU_H(3,q)$, of weight smaller than or equal to $\sqrt{q}q/2$ are, modulo linear combinations of codewords of minimal weight $2q$, obtained by shortening codewords of weight at most $\sqrt{q}q/2$, in the LDPC code defined by $\mathcal{W}(q)$, where these codewords have zero in the positions of the lines of $\ell^\perp$. By Proposition 3.5, these codewords in the LDPC code of $\mathcal{W}(q)$ are linear combinations of codewords of minimal weight $2(q+1)$; in other words, they arise from the reguli and opposite reguli of hyperbolic quadrics contained in $\mathcal{Q}(4,q)$.*

6.3 The minimum distance of $\mathbf{LU}_{H^T}(3,q)$

For q even, $\mathcal{W}(q)$ is self-dual (Theorem 2.1 (2)). Since omitting $P^\perp$ and $\ell^\perp$, with $P \in \ell$, also is a self-dual situation, $\mathrm{LU}_H(3,q)$, q even, is self-dual. So, for q even, the preceding results also characterize small weight codewords in $\mathrm{LU}_{H^T}(3,q)$.

For q odd, $\mathrm{LU}_H(3,q) \ncong \mathrm{LU}_{H^T}(3,q)$. This can be seen by looking for the minimum distance of the LDPC code defined by $\Gamma(H(3,q))^D$.

We now prove the lower bound on the minimum distance of the LDPC code $\mathrm{LU}_{H^T}(3,q)$, similar to that of Theorem 4.3. The proofs of Lemma 4.1 and of Lemma 4.2 are completely similar, but again, in the proofs, $q+1$ has to be replaced by q since a point of $\Gamma(H(3,q))^D$ lies on q lines of $\Gamma(H(3,q))^D$.

We summarize the two lemmas similar to Lemma 4.1 and Lemma 4.2. From Property (*), a codeword in the LDPC code arising from $\Gamma(H(3,q))^D$ defines a point set in $\mathcal{Q}(4,q) \setminus (P^\perp \cup \ell^\perp)$ with the property that every line of $\mathcal{Q}(4,q) \setminus (P^\perp \cup \ell^\perp)$ meets this point set in 0 or in at least 2 points. Let S be a set of points with this property. With a conic of $\Gamma(H(3,q))$, we denote the set of $q-1, q$, or $q+1$ points of a conic of $\mathcal{Q}(4,q)$, lying in $\Gamma(H(3,q))$.

Lemma 6.6. *Let x be the maximal size of intersection of S with a conic C of $\Gamma(H(3,q))$, q odd. Then $|S| \geq xq/2$.*

Lemma 6.7. *Let x be the maximal size of intersection of S with a conic of $\Gamma(H(3,q))$, q odd. Then,*

$$|S| \geq \frac{4q^2-8q+4}{8x} + 2q + \frac{x}{8} - \frac{1}{2}.$$

Putting the two bounds on $|S|$ equal to each other gives the value for x leading to the following lower bound on the minimum distance of $\mathrm{LU}_{H^T}(3,q)$.

Theorem 6.8. *The LDPC code $LU_{H^T}(3,q)$, q odd, $q \geq 5$, has minimum distance at least*

$$\frac{4q^2 - q + q\sqrt{4q^3 + 7q^2 - 2q}}{4q - 1} \approx \frac{q\sqrt{q}}{2}.$$

Acknowledgement: The authors thank the referees for their valuable comments. The first author also thanks the Department of Pure Mathematics and Computer Algebra at Ghent University where part of the work was completed.

References

[1] B. Bagchi and N.S. Narasimha Sastry, Codes associated with generalized polygons, Geom. Dedicata, Vol. 27 (1988) pp. 1–8.

[2] M.C. Davey and D.J.C. MacKay, Low density parity check codes over $GF(q)$, IEEE Communications Letters, Vol. 2, No. 6 (1998) pp. 165–167.

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

[5] J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries.* Oxford University Press (1991).

[6] 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.

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

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

[9] 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/

[10] 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.

[11] 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.

[12] F. Lazebnik and V.A. Ustimenko, Explicit construction of graphs with arbitrary large girth and of large size, Discrete Applied Math., Vol. 60 (1997) pp. 275–284.

[13] Z. Liu and D.A. Pados, LDPC codes from generalized polygons, IEEE Trans. Inform. Theory, Vol. 51, No. 11 (2005) pp. 3890–3898.

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

[15] 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.

[16] 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.

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

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

[19] 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.

[20] P. Sin and Q. Xiang, On the dimension of certain LDPC codes based on q-regular bipartite graphs, IEEE Trans. Inform. Theory, Vol. 52 (2006) pp. 3735–3737.

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

[22] R.M. Tanner, A recursive approach to low-complexity codes, IEEE Trans. Inform. Theory, Vol. 27 (1981) pp. 533–547.

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

[24] 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.

[25] 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.

[26] 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.

Addresses of the authors:

Jon-Lark Kim
University of Louisville
Department of Mathematics
328 Natural Sciences Building
Louisville, KY 40292, USA
(jl.kim@louisville.edu, http://www.math.louisville.edu/∼jlkim)

Keith E. Mellinger
Department of Mathematics
University of Mary Washington
1301 College Avenue, Trinkle Hall
Fredericksburg, VA 22401
(kmelling@umw.edu, http://people.umw.edu/∼kmelling)

Leo Storme
Ghent University
Department of Pure Mathematics and Computer Algebra
Krijgslaan 281-S22
9000 Ghent, Belgium
(ls@cage.ugent.be, http://cage.ugent.be/∼ls)