LDPC codes arising from partial and semipartial geometries

Peter Vandendriessche

LDPC codes arising from partial and semipartial geometries

Peter Vandendriessche[⋆]

Ghent University, Department of Mathematics,
Krijgslaan 281 - Building S22, 9000 Ghent, Belgium
Peter.Vandendriessche@UGent.be

Abstract. We study several high-rate LDPC codes derived from partial and semipartial geometries. We study in particular the minimum distance of several known infinite classes of these partial and semipartial and we improve the known bounds on this minimum distance in the binary and non-binary case. In some cases, we can determine the exact minimum distance.

Keywords: LDPC codes, bounds, finite geometry codes, minimum distance, partial and semipartial geometries

1 Introduction

Definition 1. *Let* $\mathbb{F}$ *be a finite field and let* H *be an* $m \times n$ *matrix of rank* $n-k$ *over* $\mathbb{F}$*. The* linear $[n,k]$-code C *defined by* H *is the* k*-dimensional subspace of* $\mathbb{F}^n$ *consisting of all vectors which have a zero inproduct (in* $\mathbb{F}$*) with all rows of* H*. The matrix* H *is called the* parity check matrix *of* C*. The parameters* n *and* k *are respectively called the* length *and* dimension *of the code* C *and are denoted by* $\mathrm{len}(C)$ *and* $\dim(C)$ *respectively.*

Definition 2. *Let* C *be a linear code. If* d *is the maximum integer for which every two different vectors in* C *differ in at least* d *positions, then* d *is called the* minimum distance *of the code* C*.*

Definition 3. *An LDPC code* C *is a code defined by a sparse parity check matrix, i.e. a parity check matrix with much more zeros than nonzero elements.*

In particular, we will focus on LDPC codes defined by $\{0,1\}$-matrices, i.e. matrices only containing entries 0 and 1. Since 0 and 1 are elements of every field, such matrices yield valid codes over any finite field $\mathbb{F}$.

[⋆] The author is supported by a PhD fellowship of the Research Foundation - Flanders (FWO).

Originally introduced by Gallager [9], LDPC ('low density parity check') codes are used frequently these days due to their excellent empirical performance under belief-propagation/sum-product decoding. In some cases, their performance is even near to the Shannon limit [18].

To exploit structural properties, one usually wants an explicit construction rather than random matrices. Lately, many constructions related to finite geometries have been studied because of their low complexity decoding features [15, 20], such as generalized quadrangles [13, 17], linear representations [21, 23, 24] and partial and semipartial geometries [12, 16]. Geometrical LDPC codes have been used in several high-end modern data transmission systems [6, 7] and in entanglement-assisted quantum decoding [4].

In [12], the authors show that LDPC codes derived from partial and semipartial geometries have excellent empirical performance under LDPC decoding methods based on belief propagation, and they derive bounds on the dimension and minimum distance of these codes. In this paper, we will improve the known bounds on the minimum distance and we provide several new theoretical results and computer results about it. Similar techniques can be used for other relevant parameters such as stopping distance, trapping distance or pseudodistance, but this falls beyond the scope of this paper.

2 Finite Geometry LDPC codes

To obtain the best decoding performance, one usually refrains from working with random $\{0, 1\}$-matrices. Instead, one will work with codes associated with finite combinatorial structures, and in particular, finite geometry codes. From now on, we will assume that $\mathbb{F}$ is a prime field, as the $\mathbb{F}_{p^h}$-code associated to a $\{0, 1\}$-parity check matrix is equivalent to the direct sum of h copies of the associated $\mathbb{F}_p$-code, and hence has the same minimum distance.

In this section, we provide a new lower bound on the minimum distance of finite geometry LDPC codes with girth at least 6 in their associated Tanner graph. For all point-line finite geometries, this condition is fulfilled. In many cases, our bound turns out to be better than the best known bounds. In particular, it also improves the known bounds on the minimum distance of general partial and semipartial geometry codes.

Definition 4. *An incidence structure* $(\mathcal{P}, \mathcal{B}, I)$ *consists of a finite set* $\mathcal{P}$*, the elements of which are called* points*, a finite set* $\mathcal{B}$*, the elements of which are called* blocks*, and a relation* $I \subseteq \mathcal{P} \times \mathcal{B}$*, which is called the* incidence relation*. Often,* $\mathcal{B}$ *is a collection of subsets of* $\mathcal{P}$ *and the incidence relation is simply* $\in$*. If additionally, any two distinct points are contained in at most one common block (or equivalently, any two distinct blocks contain at most one common point), the blocks are sometimes called* lines*.*

The fact that the Tanner graph has girth at least 6 can be stated equivalently (geometrically) as the fact that two different blocks have at most one common point or, again equivalently, as the fact that two different points are contained in at most one common block.

Definition 5. *The* dual *incidence structure to an incidence structure* $(\mathcal{P}, \mathcal{B}, I)$ *is the incidence structure* $(\mathcal{B}, \mathcal{P}, I')$ *with* $pIb \Leftrightarrow bI'p$ *for all* $p \in \mathcal{P}$ *and all* $b \in \mathcal{B}$. *For example, the dual of* $(\mathcal{P}, \mathcal{B}, \in)$ *is* $(\mathcal{B}, \mathcal{P}, \ni)$.

Definition 6. *The* incidence matrix *of an incidence structure* $(\mathcal{P}, \mathcal{B}, I)$, *with* $\mathcal{P} = \{p_1, \ldots, p_m\}$ *and* $\mathcal{B} = \{b_1, \ldots, b_n\}$ *is the* $m \times n$ *matrix, in which the rows are labeled by the points and the columns are labeled by the blocks, such that* $H_{ij} = 1$ *if* $p_i I b_j$, *and* $H_{ij} = 0$ *otherwise. The incidence matrix of the dual incidence structure is then simply the transposed of this matrix.*

Definition 7. *Given an incidence structure* $(\mathcal{P}, \mathcal{B}, I)$, *we define* $C_{\mathbb{F}}$ *to be the code over* $\mathbb{F}$ *having its parity check matrix* H *equal to the incidence matrix of an incidence structure* $(\mathcal{P}, \mathcal{B}, I)$. *If the field* $\mathbb{F}$ *is clear from the context, we will simply write* C.

This gives the code a nice interpretation: a code word c of the code corresponds to a map $\varphi : \mathcal{B} \to \mathbb{F}$ such that, for each point $r \in \mathcal{P}$, we have $\sum_{L \ni r} \varphi(L) = 0$ over $\mathbb{F}$. We call $\varphi(L)$ the *coefficient* of the line L in the code word c, and we denote this by c_L. Similarly, when considering the code derived from the dual structure, a code word is a map $\varphi : \mathcal{P} \to \mathbb{F}$ such that, for each block $L \in \mathcal{B}$, we have $\sum_{r \in L} \varphi(r) = 0$ over $\mathbb{F}$.

For arbitrary incidence structures, the dimension of the corresponding code can easily be determined in polynomial time, by simple row reduction. The minimum distance is however not at all easy to determine. In fact, it has been shown [26] that the determination of the minimum distance is an NP-complete problem in general, and even in the special case of LDPC codes, the problem remains unfeasible [11]. In the general case, we can only expect upper and lower bounds on the minimum distance. The best known bound is the following.

Theorem 1 ([1]). *Let* C *be an LDPC code defined by a* $\{0,1\}$*-parity check matrix* H *over the finite field* $\mathbb{F}_p$. *If* v *is the minimum number of ones in a column of the parity check matrix* H, *and* r *is the maximum number of common ones in any two different columns, then*

$$d \geq \frac{2}{p}\left((p-1)\frac{v}{r} + 1\right) . \tag{1}$$

3 Partial and Semipartial Geometries

However, for several infinite families of incidence structures, in particular those from finite geometries, we can find strongly improved bounds or even the exact minimum distance, using geometrical techniques.

We focus on the case where the largest set ($\mathcal{P}$ or $\mathcal{B}$) corresponds to the positions, as this results in the highest code rates, which is important for LDPC transmission. In case anything noteworthy can be said about the other (lower-rate) code, we will add this in a remark.

Definition 8. *An* (s, t, α)-partial geometry *is an incidence structure* $(\mathcal{P}, \mathcal{B}, \in)$ *for which:*

(a) each block contains exactly $s+1$ *points and each point is contained in exactly* $t+1$ *blocks;*
(b) any two distinct blocks have at most one point in common; and
(c) for any non-incident point-block pair (p, L) *there are exactly* α *blocks which contain* p *and which intersect* L*.*

A partial geometry is called proper *when* $1 < \alpha < \min(s, t)$*.*

Clearly, the dual of an (s, t, α)-partial geometry is a (t, s, α)-partial geometry. In an (s, t, α)-partial geometry $(\mathcal{P}, \mathcal{B}, I)$, one has $|\mathcal{P}| = \frac{(s+1)(st+\alpha)}{\alpha}$ and $|\mathcal{B}| = \frac{(t+1)(st+\alpha)}{\alpha}$. Hence, $|\mathcal{P}| \geq |\mathcal{B}|$ is equivalent to $s \geq t$.

Definition 9. *Slightly more general, an* (s, t, α, μ)-semipartial geometry *is an incidence structure* $(\mathcal{P}, \mathcal{B}, \in)$ *for which:*

(a) each block contains exactly $s+1$ *points and each point is contained in exactly* $t+1$ *blocks;*
(b) any two distinct blocks have at most one point in common;
(c) for any non-incident point-block pair (p, L)*, there are either* 0 *or exactly* α *blocks which contain* p *and which intersect* L*; and*
(d) for any two points p, p' *not contained in a common block, there are exactly* μ *points which are contained in a common block with* p *and in a common block with* p'*.*

A semipartial geometry is called proper *when it is not a partial geometry, and* $1 < \alpha < \min(s, t)$*.*

Clearly, $\mu \leq \alpha(t+1)$, with $\mu = \alpha(t+1)$ if and only if the semipartial geometry is a partial geometry. The dual of a semipartial geometry is in general not a semipartial geometry, hence we will not consider the dual structure here. It can be proven [10, Theorem 26.7.5] that if a semipartial geometry is not a partial geometry, then $|\mathcal{B}| \geq |\mathcal{P}|$. Hence, for semipartial geometries, we will let $\mathcal{B}$ correspond to the positions of the code words.

Definition 10. *An* (n, k)-arc $\mathcal{K}$ *in* $\mathrm{PG}(2, q)$ *is a set of* n *points of* $\mathrm{PG}(2, q)$*, such that each line intersects* $\mathcal{K}$ *in at most* k *points. Clearly, the size* $|\mathcal{K}| = n$ *of an* (n, k)*-arc is at most* $1 + (q+1)(k-1) = qk - q + k$*, since each of the* $q+1$ *lines through any one point of* $\mathcal{K}$ *can contain at most* $k-1$ *other points of* $\mathcal{K}$*.*

Definition 11. *A* maximal (n, k)-arc $\mathcal{K}$ *in* $\mathrm{PG}(2, q)$ *(often incorrectly referred to as a* maximal (n, k)-arc *or* maximal (n, k)-arc*) is an* (n, k)*-arc of size* $n = qk - q + k$*, with* $1 < k < q$*. It has been shown [2] that maximal* (n, k)*-arcs in* $\mathrm{PG}(2, q)$ *only exist when* q *is even and* k *divides* q*. In that case, each line intersects* $\mathcal{K}$ *in either* 0 *(and then the line is called* skew*) or* k *(and then the line is called* secant*) points. A maximum* 2*-arc is called a* hyperoval*. When it is not necessary to specify* k*, or when the parameters are clear from the context, we will simply write* maximal arc*.*

Up to dualization, only two infinite classes of proper partial geometries are known, and both of them are related to maximal arcs. We now provide a construction of these geometries below. We also provide a construction for the common proper semipartial geometries, listed in [10].

(a) Let $\mathcal{K}$ be a maximal (n,k)-arc in $\mathrm{PG}(2,q)$, with q even. Define $S(\mathcal{K}) = (\mathcal{P}, \mathcal{B}, \in)$ as follows: $\mathcal{P}$ is the set of points outside of $\mathcal{K}$, and $\mathcal{B}$ is the set of lines which contain at least one (and hence exactly k) points of $\mathcal{K}$. Then $S(\mathcal{K})$ is an (s,t,α)-partial geometry, where $s = q-k$, $t = q-\frac{q}{k}$ and $\alpha = q-\frac{q}{k}+1-k$.

(b) Let again $\mathcal{K}$ be a maximal (n,k)-arc in $\mathrm{PG}(2,q)$, with q even. Define $T_2^*(\mathcal{K}) = (\mathcal{P}, \mathcal{B}, \in)$ as follows: embed this $\mathrm{PG}(2,q)$ (containing $\mathcal{K}$) as a plane π_0 in $\mathrm{PG}(3,q)$, let $\mathcal{P}$ be the set of points of $\mathrm{PG}(3,q)$ outside of π_0 and let $\mathcal{B}$ be the set of lines of $\mathrm{PG}(3,q)$ which intersect π_0 in a point of $\mathcal{K}$ (and in no points of $\pi_0 \setminus \mathcal{K}$). Then $T_2^*(\mathcal{K})$ is an (s,t,α)-partial geometry, where $s = q-1$, $t = |\mathcal{K}|-1 = qk-q+k-1$ and $\alpha = k-1$.

(c) Similarly, let $\mathcal{K}$ be a Baer subplane in $\mathrm{PG}(2,q)$, with $q = p^h$, h even, and repeat the construction from (b). Then $T_2^*(\mathcal{K})$ is an (s,t,α,μ)-semipartial geometry, where $s = q-1$, $t = q+\sqrt{q}$, $\alpha = \sqrt{q}$ and $\mu = \sqrt{q}(\sqrt{q}+1)$.

(d) Similarly, let $\mathcal{K}$ be a Hermitian arc in $\mathrm{PG}(2,q)$, with $q = p^h$, h even, and repeat the construction from (b). Then $T_2^*(\mathcal{K})$ is an (s,t,α,μ)-semipartial geometry, where $s = q-1$, $t = q\sqrt{q}$, $\alpha = \sqrt{q}$ and $\mu = q(q-1)$.

(e) Let Π_{n-2} be an $(n-2)$-dimensional subspace of the projective n-space $\mathrm{PG}(n,q)$, with $n \geq 3$. As the point set $\mathcal{P}$, we take the lines of $\mathrm{PG}(n,q)$ which have no point in common with Π_{n-2}. As the block set $\mathcal{B}$, we take the planes of $\mathrm{PG}(n,q)$ which have exactly one point in common with Π_{n-2}. Then $(\mathcal{P}, \mathcal{B}, \subset)$ is an (s,t,α,μ)-semipartial geometry, where now $s = q^2-1$, $t = q^{n-2}+q^{n-3}+\cdots+q$, $\alpha = q$ and $\mu = q(q+1)$.

(f) Consider the projective n-space $\mathrm{PG}(n,q)$, with $n \geq 3$. As the point set $\mathcal{P}$, we take the lines of $\mathrm{PG}(n,q)$. As the block set $\mathcal{B}$, we take the planes of $\mathrm{PG}(n,q)$. Then $(\mathcal{P}, \mathcal{B}, \subset)$ is an (s,t,α,μ)-semipartial geometry, where $s = q(q+1)$, $t = q^{n-2}+q^{n-3}+\cdots+q$, $\alpha = q+1$ and $\mu = (q+1)^2$.

Similar to [12], C is a linear code over a finite field $\mathbb{F}$, having its parity check matrix H equal to the incidence matrix of a partial or semipartial geometry. Important hereby is that we will always set $q = p^h$, with $\mathbb{F} = \mathbb{F}_p$. Hence, the characteristic of the code's field and of the geometry's field coincide. This is known experimentally to yield the highest code rates. We will now further study each of these codes, and we study the minimum distance of these codes. We improve the existing bounds from [12] and we try to determine when the bounds are sharp. We finish this section with a definition, which will appear to be useful in the study of several of the listed partial and semipartial geometries.

Definition 12. *The* support *of a code word $c \in C$ is defined as the set of nonzero (as elements of $\mathbb{F}_p$) positions of the code word, and is denoted by* $\mathrm{supp}(c)$*. The* weight *or* Hamming weight *of that code word is then the number of elements in its support.*

Geometrically, supp(c) corresponds to the following. When positions correspond to points, supp(c) is a set of points, namely

$$\text{supp}(c) = \{r \in \mathcal{P} : \varphi(r) \neq 0\} \ . \tag{2}$$

When positions correspond to lines, supp(c) is a set of lines, namely

$$\text{supp}(c) = \{\ell \in \mathcal{B} : \varphi(\ell) \neq 0\} \ . \tag{3}$$

In the binary case, i.e. when $p = 2$, the support uniquely determines its code word c: in this case, c is simply the characteristic vector of its support. Often in this case, we will identify the support of a codeword with its corresponding set of points or lines.

4 The codes arising from $S(\mathcal{K})$

To begin with, we will study the LDPC codes derived from our first structure: $S(\mathcal{K})$, with $\mathcal{K}$ a maximal (n,k)-arc in $\mathrm{PG}(2,q)$. Since maximal (n,k)-arcs only exist when q is even, we will only consider binary codes in this section.

For the geometry $S(\mathcal{K})$, it turns out that we do not need to study the two types of codes separately (once for points corresponding to positions, once for lines corresponding to positions), as we will now show.

Definition 13. *Let $\mathcal{K}$ be a maximal (n,k)-arc. Consider the set of lines of* $\mathrm{PG}(2,q)$ *skew to $\mathcal{K}$. Clearly, each point lies on either* 0 *or $\frac{q}{k}$ of these lines, hence it is the dual of a maximum $\frac{q}{k}$-arc. This maximum $\frac{q}{k}$-arc is called the* dual maximal arc *of $\mathcal{K}$.*

Theorem 2. *Let $\mathcal{K}$ be a maximal arc and let $\mathcal{K}'$ be its dual. Then the block code derived from $\mathcal{K}$ is equivalent to the point code derived from $\mathcal{K}'$.*

Hence, in the remainder of this section, we will only study the point code C. The following conjecture was proven in [3, Theorem 3.10] when $\mathcal{K}$ is a regular hyperoval; we conjecture it to be true for arbitrary maximal arcs.

Conjecture 1. Let $\mathcal{K}$ be a maximal arc in $\mathrm{PG}(2,q)$, q even. Then the incidence vector of each line in $\mathrm{PG}(2,q)$ can be written as a linear combination of incidence vectors of secant lines to $\mathcal{K}$.

Computer simulations show that Conjecture 1 is true for all maximal arcs in $\mathrm{PG}(2,q)$ with $q \leq 32$, and for all known maximal arcs in $\mathrm{PG}(2,q)$, $q \leq 64$. We conjecture it to be true for arbitrary q; it would be interesting to prove this in general. However, this appears to be a nontrivial problem even for $k = 2$ (when $\mathcal{K}$ is a nonregular hyperoval). An equivalent way of stating this problem is to ask whether the binary rank of the incidence matrix is always equal to $3^h + 1$, the binary rank of the incidence matrix of $\mathrm{PG}(2,q)$, for q even [22].

A large class of maximal arcs in $\mathrm{PG}(2,q)$, q even, was constructed by Denniston [5]. In particular, he constructed an example for all possible values of k and q. However, other examples have been constructed as well, notably by Mathon [19] and others. We have been able to prove Conjecture 1 for Denniston arcs.

Theorem 3. *If $\mathcal{K}$ is an arc of Denniston type, then Conjecture 1 is true.*

From now on, we assume $\mathcal{K}$ to be a maximal (n, k)-arc for which Conjecture 1 holds (for example, a maximal arc of Denniston type).

Theorem 4. *The code C is the subset of the dual projective plane code $C^{\perp}_{\mathrm{PG}(2,q)}$ consisting of code words which do not contain any point of $\mathcal{K}$ in their support. In particular,*

$$\dim(C) = (q^2 + q + 1 - |\mathcal{K}|) - (3^h + 1) , \tag{4}$$

where $q = 2^h$.

Theorem 5. *The minimum distance of C has $d(C) \geq q + 2$, and equality is attained if and only if there exists a hyperoval disjoint from $\mathcal{K}$.*

For $q \leq 16$, brute-force calculations have shown that there always exists a hyperoval skew to $\mathcal{K}$ when $1 < k < q$, yielding $d(C) = q + 2$ for every maximal arc in $\mathrm{PG}(2, q)$, with $q \leq 16$. It would be interesting to find out if this holds in general.

5 The codes arising from $T_2^*(\mathcal{K})$

Definition 14. *A $(q + t, t)$-arc of type $(0, 2, t)$ in $\mathrm{PG}(2, q)$, with $2 < t < q$, is a set S of $q + t$ points in $\mathrm{PG}(2, q)$ for which every projective line ℓ meets S in either 0, 2 or t points.*

Definition 14 was introduced in [14] and it was proven that $(q + t, t)$-arcs of type $(0, 2, t)$ can only exist if q is even. Moreover, they prove that t needs to be a divisor of q, i.e. $t = 2^r$ with $r \leq h$. Several infinite families of these arcs are known, see [8, 14, 25]. A hyperoval in $\mathrm{PG}(2, q)$, $q = 2^h$ with $h \geq 1$, can be seen as a $(q+2, 2)$-arc of type $(0, 2, 2)$. One can see $(q+t, t)$-arcs of type $(0, 2, t)$ as a generalization of hyperovals. The symmetric difference of two lines of $\mathrm{PG}(2, q)$ can be seen as a $(2q, q)$-arc of type $(0, 2, q)$.

For the geometry $T_2^*(\mathcal{K})$, we have to consider three cases: $\mathcal{K}$ is a maximal (n, k)-arc, $\mathcal{K}$ is a Baer subplane, or $\mathcal{K}$ is a Hermitian arc. In each of these cases, one has $|\mathcal{K}| > q$, hence there are more blocks than points and the code will be constructed using blocks (here: lines) as the positions of the code.

Definition 15. *Let π be any plane different from π_0 such that the line $L = \pi_0 \cap \pi$ contains at least two points of $\mathcal{K}$. Let p_1, p_2 be two distinct points of $\mathcal{K} \cap L$. Define φ as follows: all the lines in $\pi \setminus \pi_0$ through p_1 map to 1, all the lines in $\pi \setminus \pi_0$ through p_2 map to -1 and all other lines map to 0. Then $\sum_{L \ni r} \varphi(L) = 0$ for any point r, since for $r \in \pi$ we get one line with coefficient 1 and one line with coefficient -1 (and all other lines 0), and for $r \notin \pi$ we only sum up lines with coefficient 0; hence this defines a code word of weight $2q$. Such a code word is called a* plane word*.*

In [21, Proposition 5], it is shown that $d \geq q + \sqrt{q}$ (if $\mathcal{K}$ is a Baer subplane or Hermitian arc) or $d \geq q + \frac{q}{k-1}$ (if $\mathcal{K}$ is a maximal (n, k)-arc). In the first case, this bound is sharp when $p = 2$, since Korchmáros and Mazzocca [14] have shown the existence of a $(q + \sqrt{q}, \sqrt{q})$-arc of type $(0, 2, \sqrt{q})$ with the points on a Baer subline as its dual t-secants. For $p \neq 2$ or if $\mathcal{K}$ is a maximal (n, k)-arc with $k > 2$, this bound is no longer sharp, and the exact minimum distance is not known in these cases.

In the second case (when $\mathcal{K}$ is a maximal (n, k)-arc and hence $p = 2$), we can however find partial results. For $k = 2$, one can easily show that $d = 2q$, and the code words of minimum weight correspond to dual $(2q, q)$-arcs of type $(0, 2, t)$, which are exactly the plane words from [23, 24]. For $k > 2$, we can however find a geometrical upper bound on the minimum distance d, in the following theorem, which holds for any maximal arc $\mathcal{K}$.

Theorem 6. *One has $d \leq q + r$, where r is the smallest integer for which there exists a line ℓ in π_0 and a dual $(q + r, r)$-arc of type $(0, 2, r)$ having its dual r-secants contained in $\ell \cap \mathcal{K}$.*

Conjecture 2. The bound in Theorem 6 is always sharp, i.e. $d = q + r$, where r is the smallest integer for which there exists a line ℓ in π_0 and a dual $(q + r, r)$-arc of type $(0, 2, r)$ having its dual r-secants contained in $\ell \cap \mathcal{K}$.

Computer simulations have shown the bound in Theorem 6 to be sharp for small values of q and for several constructions with larger q. We conjecture it to be sharp for all q. In all cases we tested, this resulted in a maximum weight of

$$d = q + \frac{q}{2^{\lfloor \log_2(k-1) \rfloor}} = q + \frac{2q}{k} \,. \tag{5}$$

It would be interesting to prove this in the general case; even for $k = 4$ we only achieved a partial result (the conjecture being that the case after 'or' in Theorem 7 can never occur).

Theorem 7. *When $k = 4$, either (5) holds (i.e. $d = \frac{3q}{2}$) or $d = 4s$ with $\frac{q}{3} \leq s \leq 3\frac{q}{8}$ and the code words of minimum weight consist of four sets of s lines, each concurrent at a point of a fixed line ℓ, with the additional property that each line contains $\frac{3s-q}{2}$ points on 4 of these lines and $\frac{3(q-s)}{2}$ points on two of these lines.*

6 The codes arising from projective planes and lines

Now we will study examples (e) and (f) in our list of partial and semipartial geometries. Here, a code word is a mapping $\mathcal{B} \to \mathbb{F}$, associating an $\mathbb{F}$-coefficient to each plane in $\mathcal{B}$, such that the sum of all coefficients of planes of $\mathcal{B}$ containing a line ℓ is zero, for every $\ell \in \mathcal{P}$. Denote these codes by $C_{(e)}$ and $C_{(f)}$ respectively.

Let $C^{\perp}_{\mathrm{PG}(2,q)}$ be the similar code with spaces one dimension lower: the positions of $C_{\mathrm{PG}(2,q)}$ are the lines of $\mathrm{PG}(2, q)$ and a code word $c \in C_{\mathrm{PG}(2,q)}$ is a map which associates a coefficient in $\mathbb{F}_p$ to each line of $\mathrm{PG}(2, q)$, such that the sum of all coefficients of lines through a given point, equals zero.

Theorem 8. *The codes $C_{(e)}$ and $C_{(f)}$ contain code words of weight $2q^2 - \frac{q-p}{p-1}q$, hence $d \leq 2q^2 - \frac{q-p}{p-1}q$.*

Explicit constructions for code words of this weight are known.

Theorem 9. *In the binary case, i.e. when $p = 2$, equality is attained: $d(C_{(e)}) = d(C_{(f)}) = q(q + 2)$.*

We cannot fully characterize the code words of minimum weight, however, we can greatly reduce the space in which code words have to be searched for.

Theorem 10. *If c is a code word of $C_{(e)}$ or $C_{(f)}$, of weight $w < 2(q^2+q+1)+2$, then* $\mathrm{supp}(c)$ *is contained in a* 3*-space.*

We summarize the new results on the minimum distances in Table 1. In almost all cases, we obtain improvements to the bound in Theorem 1.

Table 1. Summary of the new bounds obtained for partial and semipartial geometry codes. Here, $\approx$ stands for conjectured equality.

Code	$p = 2$	$p \neq 2$
General (semi)partial geometry *(blocks correspond to positions)*	$d \geq s + 2$	$d \geq \frac{2}{p}\left((p-1)s + p\right)$
General (semi)partial geometry *(points correspond to positions)*	$d \geq t + 2$	$d \geq \frac{2}{p}\left((p-1)t + p\right)$
$S(\mathcal{K})$ with $\mathcal{K}$ maximal (n, k)-arc	$d \approx q + 2$	N/A
$T_2^*(\mathcal{K})$ with $\mathcal{K}$ maximal (n, k)-arc	$d \approx q + \frac{2q}{k}$	N/A
$T_2^*(\mathcal{K})$ with $\mathcal{K}$ Baer subplane	$d = q + \sqrt{q}$	$d > q + \sqrt{q}$
$T_2^*(\mathcal{K})$ with $\mathcal{K}$ Hermitian arc	$d = q + \sqrt{q}$	$d > q + \sqrt{q}$
Lines and planes skew to $(n-2)$-space	$d = q(q+2)$	$d \leq q\left(2q - \frac{q-p}{p-1}\right)$
All lines and planes of $\mathrm{PG}(n, q)$	$d = q(q+2)$	$d \leq q\left(2q - \frac{q-p}{p-1}\right)$

References

1. Bagchi, B., Inamdar, S.P.: Projective Geometric Codes. J. Combin. Theory, Ser. A 99, 128–142 (2002)
2. Ball, S., Blokhuis, A., Mazzocca, F.: Maximal arcs in Desarguesian planes of odd order do not exist. Combinatorica 17, 31–41 (1997)
3. Castleberry, C., Hunsberger, K., Mellinger, K.E.: LDPC codes arising from hyperovals. Bull. Inst. Comb. Appl. 58, 59–72 (2010)
4. Clark, D., De Boeck, M., Fujiwara, Y., Tonchev, V.D., Vandendriessche, P.: Entanglement-assisted quantum low-density parity-check codes. Phys. Rev. A 82, id 042338 (2010)
5. Denniston, R.H.F.: Some maximal arcs in finite projective planes. J. Combin. Theory 6, 317–319 (1969)

6. Djordjevic, I.B., Vasic, B.V.: Projective geometry LDPC codes for ultralong-haul WDM high-speed transmission. IEEE Photonics Technology Letters 15, 784–786 (2003)
7. Djordjevic, I.B., Sankaranarayanan, S., Vasic, B.V.: Projective-Plane Iteratively Decodable Block Codes for WDM High-Speed Long-Haul Transmission Systems. J. Lightwave Technol. 22, 695–702 (2004)
8. Gács, A., Weiner, Zs.: On $(q+t,t)$-arcs of type $(0,2,t)$. Des. Codes Cryptogr. 29, 131–139 (2003)
9. Gallager, R.G.: Low density parity check codes. IRE Trans. Inform. Theory 8, 21–28 (1962)
10. Hirschfeld, J.W.P., Thas, J.A., General Galois Geometries. Oxford University Press, Oxford (1991)
11. Hu, X.-Y., Fossorier, M.P.C., Eleftheriou, E.: On the computation of the minimum distance of low-density parity-check codes. In: Proc. IEEE Intl. Conf. Commun. (ICC), pp. 767–771 (2004)
12. Johnson, S.J., Weller, S.R.: Codes for Iterative Decoding From Partial Geometries. IEEE Trans. Commun. 52, 236–243 (2004)
13. Kim, J.-L., Mellinger, K.E., Storme, L.: Small weight code words in LDPC codes defined by (dual) classical generalized quadrangles. Des. Codes Cryptogr. 42, 73–92 (2007)
14. Korchmáros, G., Mazzocca, F.: On $(q+t,t)$-arcs of type $(0,2,t)$ in a Desarguesian plane of order q. Math. Proc. Camb. Phil. Soc. 108, 445–459 (1990)
15. Kou, Y., Lin, S., Fossorier, M.P.C.: Low-density parity-check codes based on finite geometries: a rediscovery and new results. IEEE Trans. Inform. Theory 47, 2711–2736 (2001)
16. Li, X., Zhang, C., Shen, J.: Regular LDPC codes from semipartial geometries. Acta Appl. Math. 102, 25–35 (2008)
17. Liu, Z., Pados, D.A.: LDPC codes from generalized polygons. IEEE Trans. Inform. Theory 51, 3890–3898 (2005)
18. MacKay, D.J.C., Neal, R.M.: Near Shannon limit performance of low density parity check codes. Electron. Lett. 32, 1645–1646 (1996)
19. Mathon, R.: New maximal arcs in Desarguesian planes. J. Combin. Theory, Ser. A 97, 353–368 (2002)
20. Ngatched, T.M.N., Takawira, F., Bossert, M.: An improved decoding algorithm for finite-geometry LDPC codes. IEEE Trans. Commun. 57, 302–306 (2009)
21. Pepe, V., Storme, L., Van de Voorde, G.: Small weight code words in the LDPC codes arising from linear representations of geometries. J. Combin. Des. 17, 1–24 (2009)
22. Smith, K.J.C.: On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry. J. Combin. Theory 7, 122–129 (1969)
23. Vandendriessche, P.: Some low-density parity-check codes derived from finite geometries. Des. Codes Cryptogr. 54, 287–297 (2010)
24. Vandendriessche, P.: LDPC codes associated with linear representations of geometries. Adv. Math. Commun. 4, 405–417 (2010)
25. Vandendriessche, P.: Codes of Desarguesian projective planes of even order, projective triads and $(q+t,t)$-arcs of type $(0,2,t)$. submitted to Finite Fields Appl.
26. Vardy, A.: The intractability of computing the minimum distance of a code. IEEE Trans. Inform. Theory 43, 1757–1766 (1997)