Codes of Desarguesian projective planes of even order, projective triads and $(q+t,t)$-arcs of type $(0,2,t)$

Peter Vandendriessche*

Author's Affiliation: Ghent University
Email address: Peter.Vandendriessche@UGent.be
Phone number: +3292644917 (email preferred)
Postal Address:
Vakgroep WE01
Krijgslaan 281 - building S22
9000 Gent
Belgium

Abstract

We study the binary dual codes associated with Desarguesian projective planes $\mathrm{PG}(2,q)$, with $q=2^h$, and their links with $(q+t,t)$-arcs of type $(0,2,t)$, by considering the elements of $\mathbb{F}_q$ as binary h-tuples. Using a correspondence between $(q+t,t)$-arcs of type $(0,2,t)$ and projective triads in $\mathrm{PG}(2,q)$, q even, we present an alternative proof of the classification result on projective triads. We construct a new infinite family of $(q+t,t)$-arcs of type $(0,2,t)$ with $t=\frac{q}{4}$, using a particular form of the primitive polynomial of the field $\mathbb{F}_q$.

Keywords: Projective plane, LDPC codes, projective triads, $(q+t,t)$-arcs of type $(0,2,t)$

1 Introduction

Originally introduced by Gallager [6], low density parity check (LDPC) codes are frequently used 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 [15]. In general, a binary LDPC code C is a linear block code defined by a sparse parity check matrix H, this is a matrix that contains a lot more 0s than 1s.

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 [11, 17], such as generalized quadrangles [9, 14], linear representations [18, 22, 23] and partial and semipartial geometries [7, 12].

*The author is supported by a PhD fellowship of the Research Foundation - Flanders (FWO)

In particular, codes derived from projective planes have been used in several high-end modern data transmission systems [2, 3]. In this paper, we will take a deeper look at the structure of this LDPC code.

The incidence matrix M_q of $\mathrm{PG}(2,q)$, with $q = p^h$ and p prime, has a p-rank of $\binom{p+1}{2}^h + 1$ [21] and is symmetric, because of the self-duality of $\mathrm{PG}(2,q)$. Two linear codes related to this matrix are commonly studied: the p-ary $[q^2+q+1, \binom{p+1}{2}^h + 1]$-code generated by M_q over $\mathbb{F}_p$, which we denote by C_{gen}, and the p-ary $[q^2+q+1, 2\binom{q+1}{2} - \binom{p+1}{2}^h]$ code with M_q as its parity check matrix over $\mathbb{F}_p$, which we denote by C_{pcm}. In this paper, when studying C_{gen}, we let the points of the geometry correspond to the positions of the code, and when studying C_{pcm}, we let the lines of the geometry correspond to the positions of the code. For example, in the case of a binary code ($p = 2$), a code word of C_{pcm} is a set of lines such that each point is contained in an even number of these lines, and a code word of C_{gen} is the binary sum of any number of incidence vectors of lines.

The reason why we use a different setting for each code is the following. Since we will study the row span of C_{gen}, and in particular the dimension of certain subspaces of it, we are interested in linear combinations of rows of the incidence matrix M of $\mathrm{PG}(2,q)$ which yield the zero vector. Now in the tranposed matrix M^T, where columns correspond to lines and rows correspond to points, this is a linear combination of columns yielding the zero vector, which is well-known to correspond to a code word of the code defined by M^T as its parity check matrix, which is in our case C_{pcm}. A code word of C_{pcm} hence corresponds to a set of lines hitting each point an even number of times.

In [1], it is shown that the minimum distance of C_{gen} is $q+1$ and that the code words of minimum weight are exactly the incidence vectors of the projective lines. The minimum weight of C_{pcm} is not known in general. For $p = 2$, the minimum weight of C_{pcm} is $q+2$ and the code words of minimum weight are exactly the dual hyperovals [1].

In 1991, G.E. Moorhouse [16] found and proved an explicit basis for the rows of the incidence matrix, in the case $h = 1$ (i.e. $\binom{p+1}{2} + 1$ rows which are linearly independent). The construction is as follows: fix one line L and let $S = \{L\}$. Now consider the line L as the line at infinity of the projective plane. Then add to S all p affine lines through one point of L. Then add to S any $p-1$ affine lines through another point of L. Continue in this way, and finally add to S any one affine line through the second last point of L. Do nothing for the last point of L. Then S forms a basis for the p-ary row space of the incidence matrix.

For $q = p^h$, with p prime and $h > 1$, the existence of a similar result has been an open problem for nearly 20 years now. The nature of finite fields of non-prime order suggests that any generalization of this result will no longer allow to pick the points/lines in arbitrary order. This is, however, not a though restriction: a general construction, even in one particular order, would already be an interesting result.

In Section 3, we provide a detailed conjecture, backed up by computer simulations, of how such a generalized Moorhouse basis for $\mathrm{PG}(2,q)$ can look like for the case $p = 2$, i.e. $q = 2^h$. We discuss a strong relationship with (dual) $(q+t,t)$-arcs of type $(0,2,t)$, a special type of small code words of C_{pcm}. In Section 5, we construct a new infinite class of such arcs with $t = q/4$, parameters which were previously unknown to exist. We end by listing some possibilities for further work.

2 Preliminaries

The following structure will be shown to be closely related to the dual code of the projective plane of even order.

Definition 2.1. A $(q+t,t)$-arc of type $(0,2,t)$ in $\mathrm{PG}(2,q)$ 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 2.1 was introduced in [10] and it is proven that $(q+t,t)$-arcs of type $(0,2,t)$ with $1<t<q$ 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 $r\leq h$. They also provide a construction of such arcs if $h-r$ divides h. From now on, we will assume that q is even (and hence is a power of 2) and t divides q.

Remark 2.2. 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 $(0,2,q)$.

Definition 2.3. A $(q+t,t)$-arc of type $(0,2,t)$ in $\mathrm{PG}(2,q)$, $q=2^h$, is said to have a t-nucleus if all the t-secants are concurrent.

In [10] it is proven that all $(q+t,t)$-arcs of type $(0,2,t)$ have a t-nucleus if $h-r+1\neq\gcd(h,r-1)$, conjecturing that it holds for all r,h. That conjecture was proven in [5].

Conjecture 2.4 ([10])**.** If 4 divides t and t divides q, then there exists a $(q+t,t)$-arc of type $(0,2,t)$.

Conjecture 2.4 is open for more than 20 years now. In [10] it is proven that a $(2^h+2^r,2^r)$-arc exists when $h-r$ is a proper divisor of h. Later, in [5] the authors prove another infinite class of such arcs for which $h-r$ is not a proper divisor of h; more precisely they construct

- a $(2^{hr}+2^{h(r-1)},2^{h(r-1)})$-arc of type $(0,2,2^{h(r-1)})$ in $\mathrm{PG}(2,2^{hr})$;
- a $(2^{hr}+2^{h(r-1)+1},2^{h(r-1)+1})$-arc of type $(0,2,2^{h(r-1)+1})$ in $\mathrm{PG}(2,2^{hr})$;
- a $(2^{hr}+2^{h(r-1)+s},2^{h(r-1)+s})$-arc of type $(0,2,2^{h(r-1)+s})$ in $\mathrm{PG}(2,2^{hr})$ if there exists a $(2^h+2^s,2^s)$-arc of type $(0,2,2^s)$ in $\mathrm{PG}(2,2^h)$.

Since then, no new infinite classes have been found. Some $(40,8)$-arcs of type $(0,2,8)$ in $\mathrm{PG}(2,32)$ were found in [13] via computer searches. Shortly after, a $(36,4)$-arc of type $(0,2,4)$ in $\mathrm{PG}(2,32)$ was discovered in [8], also via computer searches. Hence, in $\mathrm{PG}(2,32)$, there are $(32+t,t)$-arcs of type $(0,2,t)$ for all divisors t of 32. The next open cases are $(68,4)$-arcs of type $(0,2,4)$ in $\mathrm{PG}(2,64)$, and $(128+t,t)$-arcs of type $(0,2,t)$ for $t=4,8,16,32$. In Section 5 we construct a new infinite class of $(q+q/4,q/4)$-arcs of type $(0,2,q/4)$, for all $q=2^h$, $h\geq 3$.

Definition 2.5. A dual $(q+t,t)$-arc of type $(0,2,t)$ in $\mathrm{PG}(2,q)$ is a set S of $q+t$ lines in $\mathrm{PG}(2,q)$ for which every projective point lies on either 0, 2 or t lines of S.

Note that the (binary) sum of the incidence vectors of the lines in a dual $(q+t,t)$-arc is equal to the zero word, since t is necessarily even.

It is clear that, since $\mathrm{PG}(2,q)$ is self-dual, arcs are equivalent to dual arcs, and all properties for arcs also hold for dual arcs (and vice versa). In a similar fashion one can use concepts such as *dual t-nucleus*, which is just the dual of the t-nucleus. In the next section we will work completely in the dual setting.

3 A basis for $\mathrm{PG}(2, q)$, q even

From now on, we limit ourselves to the case that q is even, i.e. $q = 2^h$.

Notation 3.1. We will denote

$$S(h, i) := \sum_{k=i}^{h} \binom{h}{k}.$$

For any projective point $p(0, 1, \beta)$ with

$$\beta = a_{h-1}\alpha^{h-1} + a_{h-2}\alpha^{h-2} + \cdots + a_1\alpha + a_0 \in \mathbb{F}_q,$$

where α is a primitive element of $\mathbb{F}_q$ and all $a_i \in \mathbb{F}_2$, we denote $lc(p) = \max\{i : a_i \neq 0\} + 1$ and we call this the *leading coefficient* of the point. The leading coefficient of $(0, 1, 0)$ is defined to be 0 and the leading coefficient of $(0, 0, 1)$ is defined to be $+\infty$.

A standard way to find a basis of any vector space, is to start from the zero vector space and sequentially add all vectors to it. A basis is then the set of vectors which caused an increase in dimension when they were added.

Using a row-reduced form to store the basis, this can be implemented efficiently in software. Applying this standard technique to the vector space spanned by the rows of the matrix of $\mathrm{PG}(2, q)$, with $q = 2^h$, we find that the following pattern holds for all $q \leq 512$. We conjecture it to hold for all q.

Conjecture 3.2. Let L be the projective line with equation $X_0 = 0$, and let A be the $1 \times (q^2 + q + 1)$-matrix containing the point-incidence vector of L. We again consider this line L as the line at infinity of an affine plane. Now, for

$$p \in [(0, 1, 0), (0, 1, 1), (0, 1, \alpha), (0, 1, \alpha + 1), (0, 1, \alpha^2), \ldots, (0, 1, \alpha^{h-1} + \cdots + \alpha + 1), (0, 0, 1)],$$

in that order, we add the incidence vectors of each of the q affine lines through p to the set of rows of A. Then the rank of A increases by $S(h, i)$ when adding the lines through a point p with $lc(p) = i$, for $i = 0, 1, \ldots, h, +\infty$.

This yields us a more structural rank formula: the rank of the incidence matrix of $\mathrm{PG}(2, q)$ is $3^h + 1$, which can be written as

$$1 + S(h, 0) + S(h, 1) + \underbrace{S(h, 2) + S(h, 2)}_{\text{2 terms}} + \underbrace{S(h, 3) + \cdots + S(h, 3)}_{\text{4 terms}} + \cdots .$$

Hard to verify by computer, but structurally more important, is the following Conjecture 3.3. Conjecture 3.3 provides a structural explanation for Conjecture 3.2 and on itself greatly generalizes Conjecture 2.4.

Conjecture 3.3. The numbers from Conjecture 3.2 can be explained as follows.

- The vanishing of the term $\binom{h}{0}$ when adding any point p with $lc(p) > 0$, is explained by the presence of dual $(2q, q)$-arcs of type $(0, 2, q)$ in $\mathrm{PG}(2, q)$ with as its dual t-secants: p and the points with lc at most 0 (i.e. $(0, 1, 0)$).
- The vanishing of the term $\binom{h}{1}$ when adding any point p with $lc(p) > 1$, is explained by the presence of dual $\left(\frac{3}{2}q, \frac{1}{2}q\right)$-arcs of type $\left(0, 2, \frac{1}{2}q\right)$ in $\mathrm{PG}(2, q)$ with as its dual t-secants: p and the points with lc at most 1.

- The vanishing of the term $\binom{h}{i}$ when adding any point p with $lc(p) > i$, for $i = 0, \ldots, h-1$, is explained by the presence of dual $\left(2^h + 2^{h-i}, 2^{h-i}\right)$-arcs of type $(0, 2, 2^{h-i})$ in $\mathrm{PG}(2, q)$ with as its dual t-secants: p and the points with lc at most i.
- The vanishing of the term $\binom{h}{h-1}$ when adding any point p with $lc(p) > h-1$, is explained by the presence of dual hyperovals that do not contain the line $X_0 = 0$, and in which p and the points with lc at most $h-1$ are dual secants. These can be seen as $\left(2^h + 2, 2\right)$-arcs of type $(0, 2, 2)$ in $\mathrm{PG}(2, q)$ with as its dual t-secants: p and the points with lc at most $h-1$.
- The vanishing of the term $\binom{h}{h}$ when adding the point p with $lc(p) = +\infty$ (which is equivalent to $lc(p) > h$), is explained by the presence of a dual hyperoval that does contain the line $X_0 = 0$ and in which all points on that line are dual secants. (To some extent, after removing the line at infinity this can be seen as $\left(2^h + 1, 1\right)$-arcs of type $(0, 2, 1)$ in $\mathrm{PG}(2, q)$, with as its dual t-secants the whole line $X_0 = 0$. Adding the line at infinity yields a code word of C_{pcm} as in the cases above.

Conjecture 3.3 is a strong generalization of Conjecture 2.4, which only claims the existence of the code words mentioned in Conjecture 3.3. Conjecture 2.4 has been open for over 20 years now. We hope that this more structural conjecture can give a new impulse to the problem. In particular, the author believes that one can find $(q+t, t)$-arcs of type $(0, 2, t)$ for all parameters in Conjecture 2.4, with the additional requirement that these arcs are defined by sets of lines with linear $\mathbb{F}_2$-equations on their coefficients when considering $\mathbb{F}_{2^h}$ as $\mathbb{F}_2^h$, as in the examples constructed in Section 5.

To support the plausibility of Conjecture 3.3, let us look at some particular cases.

- The last bullet of Conjecture 3.3 is clear, since for each affine line ℓ there exist dual regular hyperovals containing both $X_0 = 0$ and ℓ.
- The first bullet is easily shown as follows: let L be a line intersecting $X_0 = 0$ in a point $p \neq (0, 1, 0)$. Then the incidence vector of L can be written as the sum of all incidence vectors of the other lines through p and the incidence vectors of all lines through $(0, 1, 0)$.
- The second bullet is not trivial anymore. We will prove this part in Lemma 4.3, which fully classifies all $(q + q/2, q/2)$-arcs of type $(0, 2, q/2)$ and gives a more concise construction than the one in [10].
- The third and fourth bullet are still open. Computer results suggest that the weight of each code word in the code generated by all lines through points with $lc \leq i$, is always a multiple of 2^{h-i+1}; but a proof of this is still unknown. However, despite Conjecture 3.3 only being a conjecture, an interesting result pops up: our linear dependence search yields code words of C_{pcm} which use only a small number of points on $X_0 = 0$. **If** Conjecture 3.3 holds, **then** these code words are likely to be the sum of one or more $(q+t, t)$-arcs of type $(0, 2, t)$. Using this idea, we obtained a new infinite family of $(q+t, t)$-arcs of type $(0, 2, t)$, which is an interesting result on its own, and which also greatly improves the plausibility of Conjecture 3.3. This new infinite family is presented in Section 5.

When considering the points on $X_0 = 0$ in a different order, it seems that the rank of the matrix consisting of the line incidence vectors is never larger than what is claimed in Conjecture 3.2. With random ordering, it is also not true that using at most 2^i points of $X_0 = 0$, the weight of the obtained code words of C_{pcm} is always a multiple of 2^{h-i+1}. For example, for $q = 64$ and $i = 2$, one can obtain code words of weight 120 when the points are taken on an $\mathbb{F}_4$-subline.

In Section 4, we will prove the second bullet, and we discuss an interesting corollary about projective triads. As said before, if Conjecture 3.3 is true, then one should be able to construct dual $(q+t, t)$-arcs of type $(0,2,t)$ by looking at linear dependencies between incidence vectors of lines. In particular, we exploited this idea by studying the linear dependencies between the incidence vectors of lines through the points $(0,0,1)$, $(0,1,0)$, $(0,1,1)$, $(0,1,\alpha)$ and $(0,1,\alpha^2)$. Adding these vectors to a vector space in a well-chosen order and using the standard technique from the start of this section, we found linear dependencies between these lines resulting in $(q+q/4,q/4)$-arcs of type $(0,2,q/4)$ for all $q \geq 512$. For $q=128$ and $q=512$, this resulted in arcs of previously unknown parameters. And again, the fact that this technique works again strengthens the plausibility of Conjecture 3.3. In Section 5, we used the above observation and the arcs derived from it, to obtain a general construction of dual $(q+q/4,q/4)$-arcs of type $(0,2,q/4)$ in $\mathrm{PG}(2,q)$, q even. For $q=2^h$ with h odd, such arcs were not previously known.

4 Projective triads and $(q+t,t)$-arcs of type $(0,2,t)$

Definition 4.1. In $\mathrm{PG}(2,q)$, q even, consider three lines ℓ_1,ℓ_2,ℓ_3, concurrent at a point r. A *projective triad* is a set S of $\frac{3}{2}q+1$ points of $\mathrm{PG}(2,q)$, contained in $\ell_1 \cup \ell_2 \cup \ell_3$ and containing r, such that each line ℓ_i contains $\frac{q}{2}+1$ points of S, and each projective line not through r intersects S in 1 or 3 points.

Projective triads are mainly studied in the context of blocking sets.

Remark 4.2. Let S be a projective triad and let $S' = (\ell_1 \cup \ell_2 \cup \ell_3) \setminus S$. Then

- each line ℓ_i contains $(q+1) - \left(\frac{q}{2}+1\right) = \frac{q}{2}$ points from S',
- each other line through r contains $1-1=0$ points from S',
- each line not through r contains $3-i$ points from S' with $i \in \{1,3\}$, hence each such line contains 0 or 2 points from S'.

All in all, each line contains 0, 2 or $\frac{q}{2}$ points of S'. Since $|S'| = (3q+1) - \left(\frac{3}{2}q+1\right) = q+\frac{q}{2}$, it follows that S' is a $(q+t,t)$-arc of type $(0,2,t)$, for $t=\frac{q}{2}$.

On the other hand, if S' is a $(q+t,t)$-arc of type $(0,2,t)$ with $t=\frac{q}{2}$, then it has a t-nucleus r, and hence it is contained in three lines ℓ_1,ℓ_2,ℓ_3. In a similar fashion, $S = (\ell_1 \cup \ell_2 \cup \ell_3) \setminus S'$ is now a projective triad.

Hence, a projective triad uniquely corresponds to a $(q+t,t)$-arc of type $(0,2,t)$ with $t=\frac{q}{2}$. We will now classify the (dual) $(q+t,t)$-arcs of type $(0,2,t)$ with $t=\frac{q}{2}$. Without loss of generality we may assume the dual nucleus to be the line $X_0=0$ and by a coordinate transformation, we can let the dual secants be $(0,0,1)$, $(0,1,0)$ and $(0,1,1)$.

Lemma 4.3. The subset of C_{pcm} of code words consisting of the lines through $(0,0,1)$, $(0,1,0)$ and $(0,1,1)$, different from the line $X_0=0$, is a subcode of dimension $h+2 = 0+\binom{h}{0}+\left(\binom{h}{0}+\binom{h}{1}\right)$ with weight polynomial $1+(4q-4)X^{3q/2}+3X^{2q}$.

Proof. We will completely classify the code words of this code. Denote our three points by $p_0(0,0,1)$, $p_1(0,1,0)$, $p_2(0,1,1)$. We recall that a code word here corresponds to a set of lines through one of p_0, p_1 or p_2, such that each point outside of $X_0=0$ is contained in an even number of lines (and hence in either 0 or 2 lines) of the set.

Let c be any code word. Denote by s, t, u respectively the number of lines in supp(c) through p_0, p_1, p_2. If at least one of s, t, u is zero, there are only four code words: the empty word and the $\binom{3}{2} = 3$ words formed by the $(2q, q)$-arcs of type $(0, 2, q)$. Now consider any other word with $s, t, u > 0$. Any line through p_0 must intersect exactly $t + u$ lines through the other two points, hence $t + u = q$. Similarly, $s + t = q$ and $s + u = q$. Solving this system of equations, we get $s = t = u = q/2$.

Now coordinatize the lines of supp(c) as follows:

- write the lines through $p_0(0, 0, 1)$ as $[\mu, 1, 0]$ with $\mu \in S$, $|S| = q/2$,
- write the lines through $p_1(0, 1, 0)$ as $[\mu, 0, 1]$ with $\mu \in T$, $|T| = q/2$,
- write the lines through $p_2(0, 1, 1)$ as $[\mu, 1, 1]$ with $\mu \in U$, $|U| = q/2$.

The condition that each point $(1, x, y)$ should be contained in an even number of lines of supp(c), is equivalent to saying that for each $x, y \in \mathbb{F}_q$, an even number of the statements $x \in S$, $y \in T$, $x + y \in U$ should be fulfilled. In particular, for fixed $x \notin S$ we have $x + T = U$ and $x + U = T$, hence $\forall x, x', x'' \notin S$ we have $x + x' + x'' + T = x + T$. This means that, considering $(\mathbb{F}_q, +)$ as a h-dimensional vector space over $\mathbb{F}_2$, the elements of S form an affine subspace. Similarly, T and U also need to be affine subspaces. From their sizes, S, T and U are affine hyperplanes.

For hyperplanes. it follows from $x + T = U$ that T and U need to be equal or parallel. Similarly, S, T, U all belong to the same parallel class. Hence, for some $c, c', c_0, c_1, \ldots, c_{h-1} \in \mathbb{F}_2$,

$$S = \{a_{h-1}\alpha^{h-1} + \cdots + a_1\alpha + a_0 : c_{h-1}a_{h-1} + \cdots + c_1a_1 + c_0a_0 = c\},$$

$$T = \{a_{h-1}\alpha^{h-1} + \cdots + a_1\alpha + a_0 : c_{h-1}a_{h-1} + \cdots + c_1a_1 + c_0a_0 = c'\},$$

$$U = \{a_{h-1}\alpha^{h-1} + \cdots + a_1\alpha + a_0 : c_{h-1}a_{h-1} + \cdots + c_1a_1 + c_0a_0 = c + c' + 1\},$$

where we remind that an even number of $c, c', c + c' + 1$ are zero, for each $c, c' \in \{0, 1\}$.

Clearly, for each binary choice of these $h + 2$ parameters, we get a different code word of weight $\frac{3}{2}q$, and the degenerate choice $c_0 = c_1 = \cdots = c_{h-1} = 0$ yields the 4 code words mentioned at the start of the proof, having weight different from $\frac{3}{2}q$. □

As a by-product, we find a complete classification of the projective triads. A classification equivalent to Corollary 4.4 was found before in [20], and implicitly in [19].

Corollary 4.4. Let ℓ_1, ℓ_2, ℓ_3 in PG$(2, q)$, q even, be any three concurrent lines. Let $A \in$ PGL$(3, q)$ be the coordinate transformation which maps these lines to $[0, 0, 1], [0, 1, 0], [0, 1, 1]$, let Π_t be any hyperplane in AG$(h, 2)$, with equation $c_{h-1}X_{h-1} + \cdots + c_1X_1 + c_0X_0 = t$, and let $c, c' \in \{0, 1\}$. If we let

$$\begin{aligned} S = \ & \{(1,0,0)\} \\ & \cup\{(a_{h-1}\alpha^{h-1} + \cdots + a_1\alpha + a_0, 0, 1) | (a_{h-1}, \ldots, a_1, a_0) \in \Pi_c\} \\ & \cup\{(a_{h-1}\alpha^{h-1} + \cdots + a_1\alpha + a_0, 1, 0) | (a_{h-1}, \ldots, a_1, a_0) \in \Pi_{c'}\} \\ & \cup\{(a_{h-1}\alpha^{h-1} + \cdots + a_1\alpha + a_0, 1, 1) | (a_{h-1}, \ldots, a_1, a_0) \in \Pi_{c+c'}\}, \end{aligned}$$

then $\{A^{-1}s | s \in S\}$ forms a projective triad on ℓ_1, ℓ_2, ℓ_3. Moreover, if $q > 2$, all $4q - 4$ projective triads on ℓ_1, ℓ_2, ℓ_3 arise from this construction.

5 A new construction

For an n-dimensional vector space V and a vector $v \in V$, we can computationally find v as a linear combination of a given basis $\{v_1, \ldots, v_n\}$ of V. Using only incidence vectors of lines as basis, and with v also an incidence vector of a different line, the linear combination $v = \sum_{i \in I} v_i$ shows that the corresponding set of lines forms a code word of C_{pcm}. If Conjecture 3.3 is true, every code word is composed of a linear combination of $(q+t, t)$-arcs of type $(0, 2, t)$. For $t = q/4$, we found that in some cases, code words obtained in this way can be equal to such an arc. This observation led us to several examples, which we could embed in the following construction.

Let $\mathbb{F}_q$ be a finite field, with $q = 2^h$, $h \geq 4$, built up with

$$\alpha^h = a_{h-1}\alpha^{h-1} + a_{h-2}\alpha^{h-2} + \cdots + a_1\alpha + a_0$$

with all $a_i \in \{0, 1\}$, as its primitive polynomial. From [4] it follows that we may choose $a_{h-1} = a_{h-2} = 0$ for $h \geq 8$. For $h = 4, 5, 6, 7$ one can easily verify that respectively $\alpha^4 + \alpha + 1 = 0$, $\alpha^5 + \alpha^2 + 1 = 0$, $\alpha^6 + \alpha + 1 = 0$ and $\alpha^7 + \alpha^3 + 1 = 0$ are primitive polynomials of degree h with $a_{h-1} = a_{h-2} = 0$.

Consider the projective line in $\mathrm{PG}(2, q)$ with equation $X_0 = 0$, and consider the points $(0, 0, 1)$, $(0, 1, 0)$, $(0, 1, 1)$, $(0, 1, \alpha)$ and $(0, 1, \alpha^2)$; these points will be the dual t-secants and the line $X_0 = 0$ will be the dual t-nucleus. Now we write all other lines through $(0, 0, 1)$ as $\langle (0, 0, 1), (1, t, 0) \rangle$ with $t \in \mathbb{F}_q$ and we write all other lines through $(0, 1, x)$ as $\langle (0, 1, x), (1, 0, t) \rangle$ with $t \in \mathbb{F}_q$.

Any element $z \in \mathbb{F}_q$ can be written uniquely as

$$z = z_{h-1}\alpha^{h-1} + z_{h-2}\alpha^{h-2} + \cdots + z_1\alpha + z_0,$$

with each $z_i \in \{0, 1\}$. By $(z)_i$ we will denote z_i. We will now construct two (very similar) classes of examples: let *par* $\in \{0, 1\}$ be a fixed element of $\mathbb{F}_2$; our infinite class will depend on *par*. Consider the following five sets of lines.

- $A := \{\langle (0, 0, 1), (1, t, 0) \rangle$ with $t_{h-2} = 0, t_{h-3} = 1\}$,
- $B := \{\langle (0, 1, 0), (1, 0, t) \rangle$ with $t_{h-1} = 0, t_{h-2} = 1\}$,
- $C := \{\langle (0, 1, 1), (1, 0, t) \rangle$ with $t_{h-2} = 0, t_{h-3} + t_{h-4} + \cdots + t_0 = par\}$,
- $D := \{\langle (0, 1, \alpha), (1, 0, t) \rangle$ with $t_{h-1} + t_{h-2} = 1, t_{h-3} + t_{h-4} + \cdots + t_0 = par\}$,
- $E := \{\langle (0, 1, \alpha^2), (1, 0, t) \rangle$ with $t_{h-1} = 0, t_{h-2} + t_{h-3} + t_{h-4} + \cdots + t_0 = par\}$,

then we will show that these form a dual $(q + q/4, q/4)$-arc of type $(0, 2, q/4)$. That the set $A \cup B \cup C \cup D \cup E$ contains $q + q/4$ lines, is clear. That there are 5 points in which $q/4$ lines meet is also clear. What is not clear, is that each point with coordinates $(1, x, y)$ lies on either 0 or 2 of these lines. This will be proven in what follows.

Notation 5.1. Denote by S the set of lines of $A \cup B \cup C \cup D \cup E$.

From now on, we consider $X_0 = 0$ to be the line at infinity and we consider its complement as the affine plane $\mathrm{AG}(2, q)$.

Lemma 5.2. The union of the affine points contained in any line of a set A, B, C, D or E, is for each of the 5 sets as follows:

- $p_A := \{(1,x,y) : x_{h-2} = 0, x_{h-3} = 1\}$,
- $p_B := \{(1,x,y) : y_{h-1} = 0, y_{h-2} = 1\}$,
- $p_C := \{(1,x,y) : x_{h-2} + y_{h-2} = 0, x_{h-3} + x_{h-4} + \cdots + x_0 + y_{h-3} + y_{h-4} + \cdots + y_0 = par\}$,
- $p_D := \{(1,x,y) : x_{h-2} + x_{h-3} + y_{h-1} + y_{h-2} = 1, x_{h-4} + \cdots + x_0 + y_{h-3} + y_{h-4} + \cdots + y_0 = par\}$,
- $p_E := \{(1,x,y) : x_{h-3} + y_{h-1} = 0, x_{h-4} + \cdots + x_0 + y_{h-2} + y_{h-3} + y_{h-4} + \cdots + y_0 = par\}$.

Proof. For A, B and C, this is obvious. For D, let the primitive polynomial be $\alpha^h = a_{h-3}\alpha^{h-3} + a_{h-4}\alpha^{h-4} + \cdots + a_1\alpha + a_0$ as assumed before. Then

$$\begin{array}{rcl} \alpha x & = & x_{h-1}\alpha^h + x_{h-2}\alpha^{h-1} + x_{h-3}\alpha^{h-2} + x_{h-4}\alpha^{h-3} + \cdots + x_0\alpha \\ & = & x_{h-2}\alpha^{h-1} + x_{h-3}\alpha^{h-2} + (x_{h-4} + x_{h-1}a_{h-3})\alpha^{h-3} + \cdots \\ & & \quad +(x_0 + x_{h-1}a_1)\alpha + x_{h-1}a_0. \end{array}$$

Hence, $t_{h-1} + t_{h-2} = (\alpha x + y)_{h-1} + (\alpha x + y)_{h-2} = 1$ reduces to $x_{h-2} + x_{h-3} + y_{h-1} + y_{h-2} = 1$ and

$$t_{h-3} + t_{h-4} + \cdots + t_0 = (\alpha x + y)_{h-3} + (\alpha x + y)_{h-4} + \cdots + (\alpha x + y)_0 = par$$

reduces to

$$x_{h-1}(a_{h-3} + a_{h-4} + \cdots + a_0) + x_{h-4} + \cdots + x_0 + y_{h-3} + y_{h-4} + \cdots + y_0 = par.$$

Since $a_{h-3} + a_{h-4} + \cdots + a_0 = 0$ (otherwise 1 is a root of the primitive polynomial), the latter reduces to

$$x_{h-4} + \cdots + x_0 + y_{h-3} + y_{h-4} + \cdots + y_0 = par$$

as claimed. Finally, for E,

$$\begin{array}{rcl} \alpha^2 x & = & \alpha(x_{h-1}\alpha^h + x_{h-2}\alpha^{h-1} + x_{h-3}\alpha^{h-2} + x_{h-4}\alpha^{h-3} + \cdots + x_0\alpha) \\ & = & \alpha(x_{h-2}\alpha^{h-1} + x_{h-3}\alpha^{h-2} + (x_{h-4} + x_{h-1}a_{h-3})\alpha^{h-3} \\ & & \quad + \cdots + (x_0 + x_{h-1}a_1)\alpha + x_{h-1}a_0) \\ & = & x_{h-2}\alpha^h + x_{h-3}\alpha^{h-1} + (x_{h-4} + x_{h-1}a_{h-3})\alpha^{h-2} + \cdots \\ & & \quad +(x_0 + x_{h-1}a_1)\alpha^2 + x_{h-1}a_0\alpha \\ & = & (x_{h-3} + a_{h-1}x_{h-2})\alpha^{h-1} + (x_{h-4} + x_{h-1}a_{h-3} + x_{h-2}a_{h-2})\alpha^{h-2} \\ & & \quad + \cdots + (x_0 + x_{h-1}a_1 + x_{h-2}a_2)\alpha^2 \\ & & \quad +(x_{h-1}a_0 + x_{h-2}a_1)\alpha + x_{h-2}a_0 \\ & = & x_{h-3}\alpha^{h-1} + (x_{h-4} + x_{h-1}a_{h-3})\alpha^{h-2} \\ & & \quad +(x_{h-5} + x_{h-1}a_{h-4} + x_{h-2}a_{h-3})\alpha^{h-3} + \cdots \\ & & \quad +(x_0 + x_{h-1}a_1 + x_{h-2}a_2)\alpha^2 + (x_{h-1}a_0 + x_{h-2}a_1)\alpha \\ & & \quad +x_{h-2}a_0. \end{array}$$

Hence, $t_{h-1} = (\alpha^2 x + y)_{h-1} = 0$ reduces to $x_{h-3} + y_{h-1} = 0$ and

$$\begin{array}{l} t_{h-2} + t_{h-3} + t_{h-4} + \cdots + t_0 \\ \quad = (\alpha^2 x + y)_{h-2} + (\alpha^2 x + y)_{h-3} + (\alpha^2 x + y)_{h-4} + \cdots + (\alpha^2 x + y)_0 \\ \quad = par \end{array}$$

reduces to

$$(x_{h-1} + x_{h-2})(a_{h-3} + \cdots + a_0) + x_{h-4} + \cdots + x_0 + y_{h-2} + y_{h-3} + y_{h-4} + \cdots + y_0 = par.$$

Since again $a_{h-3} + \cdots + a_0 = 0$, this reduces to

$$x_{h-4} + \cdots + x_0 + y_{h-2} + y_{h-3} + y_{h-4} + \cdots + y_0 = par$$

as claimed. □

Lemma 5.3. Let ℓ_1, ℓ_2, ℓ_3 be three concurrent lines of S. Then ℓ_1, ℓ_2, ℓ_3 all belong to the same set A, B, C, D or E.

Proof. It is clear that if two of them belong to different sets, they all belong to a different set. So what we have to verify is that

$$p_A \cap p_B \cap p_C = \emptyset, p_A \cap p_B \cap p_D = \emptyset, \dots, p_C \cap p_D \cap p_E = \emptyset.$$

If we define $c := x_{h-4} + \cdots + x_0 + y_{h-4} + \cdots + y_0 + par$, then the systems of equations obtained in Lemma 5.2 become:

- $p_A := \{(1, x, y) : x_{h-2} = 0, x_{h-3} = 1\}$,
- $p_B := \{(1, x, y) : y_{h-1} = 0, y_{h-2} = 1\}$,
- $p_C := \{(1, x, y) : x_{h-2} + y_{h-2} = 0, x_{h-3} + y_{h-3} + c = 0\}$,
- $p_D := \{(1, x, y) : x_{h-2} + x_{h-3} + y_{h-1} + y_{h-2} = 1, y_{h-3} + c = 0\}$,
- $p_E := \{(1, x, y) : x_{h-3} + y_{h-1} = 0, y_{h-2} + y_{h-3} + c = 0\}$,

and one can easily verify that any three of these yield an inconsistent system of linear equations over $\mathbb{F}_2$. □

Theorem 5.4. The set of lines S is a dual $(q + q/4, q/4)$-arc of type $(0, 2, q/4)$.

Proof. As we remarked before, all that is left to prove is that each affine point lies on either 0 or 2 lines of S. From Lemma 5.3, it follows that an affine point cannot lie on three or more lines. Hence, each point lies on either 0, 1 or 2 lines. Now assume that there exists an affine point p which only lies on one line $L \in S$. The q lines in the 4 sets not containing L, intersect L in one affine point each, different from p. By the pigeonhole principle (q incidences for $q - 1$ possible points), there must be two such lines intersecting L in the same point, a contradiction with Lemma 5.3. Hence, every affine point lies on 0 or 2 lines of S. □

6 Conclusions and further work

We have proposed several detailed conjectures on Desarguesian projective planes of even order, and their links with $(q + t, t)$-arcs of type $(0, 2, t)$. Considering the elements of $\mathbb{F}_q$ as binary h-tuples and using a particular form of the primitive polynomial of the field $\mathbb{F}_q$, we have constructed a new infinite class of $(q + t, t)$-arcs of type $(0, 2, t)$ with previously unknown parameters. We have given a full classification of the projective triads in $\mathrm{PG}(2, q)$, q even. We finish this paper by discussing some options for possible further work.

Clearly, proving Conjecture 2.4 or Conjecture 3.3 would be an important achievement. However, it seems that this is a difficult problem. Intermediate results, improving our understanding of these structures, would be a good way to go. In particular, proving Conjecture 3.2 by other methods could be a good first step, and finding more infinite classes of arcs could also potentially bring us closer to an answer to the problem.

Lemma 4.3 shows that all $(q + t, t)$-arcs of type $(0, 2, t)$ are linear (i.e. they arise from linear equations considering $\mathbb{F}_q$ as $\mathbb{F}_2^h$) if $t = q/2$. For $t = q$, this is also clearly the case. For $t = 2$, this is trivially fulfilled since every two points in $\mathrm{AG}(2,h)$ form an affine subspace. A natural question would be if there exist $(q+t,t)$-arcs of type $(0,2,t)$ which are not linear, for $4 \leq t \leq q/4$. If not, this would be a major step towards proving Conjecture 3.3, and an important result on its own. It would also allow more efficient computer searches for classifying $(q+t,t)$-arcs of type $(0,2,t)$ in small planes.

An important step in the construction of the new class of arcs was the result that the coefficient of α^{h-1} and α^{h-2} can be assumed to be zero in the primitive polynomial of the field. Without this assumption, several extra terms would usually be added to the equations and we would no longer be able to cancel out the extra terms $a_0 + \cdots + a_{h-3}$. It would be very interesting to see a general construction without assumptions on the primitive polynomial – in particular, to understand how adding the terms α^{h-1} or α^{h-2} affects the form of the linear $\mathbb{F}_2$-equations imposed on t. A better understanding of this behavior would bring us closer to a general construction.

A last (minor) possibility for further work would be to try to find a similar construction to obtain an infinite family of $(q+q/8, q/8)$-arcs of type $(0,2,q/8)$, since [4] allows to choose the first three coordinates zero, where we only used this for the first two coordinates. Examples of such arcs however do not roll easily out of the projective plane matrix, which is why we have not yet been able to construct such a family.

Acknowledgement. The author wants to thank Leo Storme for his detailed proofreading and useful suggestions.

References

[1] E.F. Assmus Jr and J.D. Key, Designs and their Codes, Cambridge University Press (1992), Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[2] I.B. Djordjevic and B.V. Vasic, Projective geometry LDPC codes for ultralong-haul WDM high-speed transmission, *IEEE Photonics Technology Letters* **15** (2003), 784–786.

[3] I.B. Djordjevic, S. Sankaranarayanan and B.V. Vasic, Projective-Plane Iteratively Decodable Block Codes for WDM High-Speed Long-Haul Transmission Systems, *J. Lightwave Technol.* **22** (2004), 695–702.

[4] S. Fan and W. Han, Character sums over Galois rings and primitive polynomials over finite fields, *Fin. Fields Appl.* **10** (2004), 36–52.

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

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

[7] S.J. Johnson and S.R. Weller, Codes for Iterative Decoding From Partial Geometries, *IEEE Trans. Commun.* **52** (2004), 236–243.

[8] J.D. Key, T.P. McDonough and V.C. Mavron, An upper bound for the minimum weight of the dual codes of Desarguesian planes, *European J. Combin.* **30** (2009), 220–229.

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

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

[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* **47** (2001), 2711–2736.

[12] X. Li, C. Zhang and J. Shen, Regular LDPC codes from semipartial geometries, *Acta Appl. Math.* **102** (2008), 25–35.

[13] J. Limbupasiriporn, Partial Permutation Decoding for Codes from Designs and Finite Geometries, PhD Thesis, Clemson University (2005).

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

[15] D.J.C. MacKay and R. M. Neal, Near Shannon limit performance of low density parity check codes, *Electron. Lett.* **32** (1996), 1645–1646.

[16] G.E. Moorhouse, Bruck nets, codes, and characters of loops, *Des. Codes Cryptogr.* **1** (1991), 7–29.

[17] T.M.N. Ngatched, F. Takawira and M. Bossert, An improved decoding algorithm for finite-geometry LDPC codes, *IEEE Trans. Commun.* **57** (2009), 302–306.

[18] V. Pepe, L. Storme and G. Van de Voorde, Small weight codewords in the LDPC codes arising from linear representations of geometries, *J. Combin. Des.* **17** (2009), 1–24.

[19] D. Senato, Blocking sets di indice tre, *Rend. Accad. Sci. Fis. Mat. Napoli* **19** (1982), 89–95.

[20] T. Szőnyi, Combinatorial Problems for Abelian Groups Arising from Geometry, *Periodica Polytechnica* **19** (1991), 91–100.

[21] K.J.C. Smith, On the p-rank of the incidence matrix of points in hyperplanes in a finite projective geometry, *J. Comb. Theory* **7** (1969), 122–129.

[22] P. Vandendriessche, Some low-density parity-check codes derived from finite geometries, *Des. Codes Cryptogr.* **54** (2010), 287–297.

[23] P. Vandendriessche, LDPC codes associated with linear representations of geometries, *Adv. Math. Commun.* **4** (2010), 405–417.