# Some Combinatorial Aspects of Constructing Bipartite-Graph Codes

**Alexander A. Davydov,[1] Massimo Giulietti,[2] Stefano Marcugini,[2] Fernanda Pambianco[2]**

[1]*Institute for Information Transmission Problems, Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 127994, Russian Federation, E-mail: adav@iitp.ru*

[2]*Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, Perugia, 06123, Italy*
*E-mail: giuliet@dipmat.unipg.it; gino@dipmat.unipg.it; fernanda@dipmat.unipg.it*

**Abstract: We propose geometrical methods for constructing square 01-matrices with the same number $n$ of units in every row and column, and such that any two rows of the matrix contain at most one unit in common. These matrices are equivalent to $n$-regular bipartite graphs without 4-cycles, and therefore can be used for the construction of efficient bipartite-graph codes such that both the classes of its vertices are associated with local constraints. We significantly extend the region of parameters $m, n$ for which there exist an $n$-regular bipartite graph with $2m$ vertices and without 4-cycles. In that way we essentially increase the region of lengths and rates of the corresponding bipartite-graph codes. Many new matrices are either circulant or consist of circulant submatrices: this provides code parity-check matrices consisting of circulant submatrices, and hence quasi-cyclic bipartite-graph codes with simple implementation.**

**Keywords**: *Low-density parity-check (LDPC) codes, bipartite-graph codes, configurations in combinatorics, projective and affine spaces*

# 1 Introduction

Bipartite-graph codes are studied in the context of low-density parity-check (LDPC) codes, i.e., error correcting codes with a strongly sparse parity check matrix. These codes were first presented by Gallager [1] in 1962, see also [2]-[30] and the references therein.

The general idea of connecting linear LDPC codes to bipartite graphs first appeared in Tanner's seminal paper [2]. In the Tanner graph of an LDPC code $\mathcal{C}$, the vertices of one class (variable vertices) correspond to code symbols and those of the other class are associated with subcodes (local constraints on variables). The case where the subcodes are linear codes with a single parity-check has been intensively investigated, see e.g. [2],[6],[8] -[15],[19]-[24]. In this case, each parity-check of the code $\mathcal{C}$ is represented by a subcode vertex.

In a number of papers, see e.g. [3]-[5],[16],[28],[29], codes $\mathcal{C}$ in which the local constraints on variables have few parity-checks are considered. The subcodes are called component or constituent codes, and $\mathcal{C}$ is said to be a generalized LDPC (GLDPC) code. It is natural to refer to the corresponding bipartite graph as to the *generalized Tanner graph* of $\mathcal{C}$.

Sipser and Spielman [3] significantly developed the approach in [2] by using graph expansion parameters and spectral properties of the Tanner graph for decoding analysis; they also suggested the term *expander codes* for code families whose analysis relies on graph expansion.

Variants of Tanner's construction were proposed in several papers. In the codes $\mathcal{C}$ investigated in [7],[17],[20],[25]-[27], the code symbols correspond to the edges of a bipartite graph $G$; each vertex $v$ of $G$ is associated with a local constraint $\mathcal{C}_v$ of length equal to the degree of the vertex. The subcode $\mathcal{C}_v$ coincides with the projection of $\mathcal{C}$ on the positions corresponding to the edges containing $v$. Usually, the graph $G$ is assumed to be regular (i.e. each vertex has the same degree) or biregular (i.e. each vertex from the same class has the same degree). This allows the use of the same local constraint for each vertex $v$ from the same class, and therefore facilitates decoding analysis. According to [17] and [27], such a code is called a *bipartite-graph code* (BG code for short). It should be noted that the graph $G$ is distinct from the generalized Tanner graph of $\mathcal{C}$. Throughout the paper we refer to $G$ as the *supporting graph* of $\mathcal{C}$.

In order to improve the performance of a bipartite-graph code, it is desirable to increase the *girth* of the graph, that is, the minimum length of its cycles [6],[8]-[15],[19]-[25]. In this paper, the combinatorial aspects of this issue are dealt with. In particular, we investigate the spectrum $\Sigma$ of parameters $m_1, m_2, n_1, n_2$ for which there exists a biregular bipartite graph $(V_1 \cup V_2, E)$ free from 4-cycles and such that $|V_i| = m_i$, $\deg(v) = n_i$ for all $v$ in $V_i$. A number of new geometrical methods for constructing these graphs are proposed, so that the spectrum of parameters of bipartite-graph codes is significantly extended, especially for the case $m_1 = m_2$, $n_1 = n_2$. It should be noted that if the supporting graph of a BG code has girth at least six, then the girth of the generalized Tanner graph of this code (considered as a GLDPC code) is at least ten.

A key tool in our investigation is the 01-matrix $M(G)$ corresponding to a biregular bipartite graph $G$ with parameters $m_1, m_2, n_1, n_2$ and without 4-cycles: each row corresponds to a vertex in $V_1$, each column to a vertex in $V_2$, and the entry in position $(i, j)$ is 1 if and only if there is an edge joining the vertices corresponding to the $i$-th row and the $j$-th column. The matrix $M(G)$ is an $m_1 \times m_2$ matrix, with $n_1$ units in every row and $n_2$ units in every column; also, since $G$ has no 4-cycles, the $2 \times 2$ matrix $J_4$ consisting of all units is not a submatrix of $M(G)$. We denote the class of such matrices as $M(m_1, m_2, n_1, n_2)$. For the sake of simplicity, we write $M(m, n)$ for $M(m, m, n, n)$. Clearly, from a matrix $M$ in $M(m_1, m_2, n_1, n_2)$ one can construct a bipartite biregular graph $G(M)$ free from 4-cycles with parameters $m_1, m_2, n_1, n_2$. Most of the paper is devoted to the construction of matrices of type $M(m_1, m_2, n_1, n_2)$ - and hence of bipartite biregular graphs with parameters $m_1, m_2, n_1, n_2$ - mainly based on incidence structures in finite projective spaces $PG(v, q)$ over Galois fields $F_q$ (see [31],[32] for basic facts on Galois Geometries).

We remark that $J_4$-free matrices are studied in connection with LDPC codes not just as matrices of supporting graphs, see e.g. [6],[8]-[15],[19]-[25], and the references therein. Mainly, non-square matrices are investigated; exceptions can be found in [13],[19]-[21],[25]. Matrices of type $M(m, n)$ are also relevant in design theory. The fact that the incidence matrix of a 2-$(v, k, 1)$ design which is either symmetric or resolvable non-symmetric (see [32]) gives rise to matrices of type $M(v, k)$ is well known, and has already been used in some works on LDPC codes, see [8, 9, 10]. We point out that weaker incidence structures such as *symmetric configurations* (see [32, Section IV.6],[33]-[35]) give rise to matrices of type $M(m, n)$ as well, and we will significantly rely on this remark throughout the paper. Also, methods from Graph Theory have turned out to be very useful for constructing of matrices of type $M(m, n)$, see e.g. [13],[36],[37], and the references therein.

Despite matrices $M(m_1, m_2, n_1, n_2)$ having been thoroughly investigated, the spectrum of parameters in $\Sigma$ seems to be not wide enough if compared to the permanently growing needs of practice, where exact values of $m_i$ and $n_i$ are often necessary. Also, it should be taken into consideration that distinct constructions provide matrices with distinct properties, and clearly some choice can be useful.

The paper is organized as follows. First, we provide a construction (Construction A) based on incidence structures whose point-set consists of a single orbit of points under the action of a collineation group of a finite affine or projective plane, see Section 3.

In Section 4 we provide Construction B. The starting point is any cyclic symmetric configuration $\mathcal{I}$. Then we consider incidence substructures in which the point-set is the union of orbits under the action of subgroups of the automorphism group of $\mathcal{I}$. Construction B turns out to be very productive, as it gives rise to numerous matrices $M(m, n)$ and $M(m_1, m_2, n_1, n_2)$ with distinct parameters. Moreover, the new matrices $M(m, n)$ are either *circulant* or consist of *circulant submatrices*. Therefore, not only the spectrum $\Sigma$ is significantly extended, but also parity-check matrices with interesting and useful structure are provided, see Remarks 4.7 and 4.11. In particular, we obtain parity-check matrices consisting of circulant submatrices. The corresponding bipartite-graph codes are *quasi-cyclic* (QC). Interestingly, QC codes can be encoded with the help of shift-registers with complexity linearly proportional to their code length, see [11],[18].

In Sections 5 and 6 we apply the general results obtained in Section 4 to two well-known classes of cyclic symmetric configurations. This allows us to obtain further parameters of matrices $M(m, n)$ and $M(m_1, m_2, n_1, n_2)$. We give also a number of computer results.

Finally, in Section 7 constructions not arising from collineation groups are described, and in Section 8 a summary of new symmetric configurations is given.

Some of the results from this work were presented without proofs in [30].

# 2 Preliminaries. Problem Statement

## 2.1 Constructions of Codes

We consider some constructions of codes on bipartite graphs. Let an $[n, k]$ code be a linear code of length $n$ and dimension $k$. Note that the methods developed in the present paper are suitable for both binary and non-binary codes.

*Tanner graphs.* In [2] Tanner proposed the following way to associate a bipartite graph $T$ to an $[N, K]$ code $\mathcal{C}$ defined by an $R \times N$ parity-check matrix $H$ with $R \geq N - K$. One class of vertices $\{V'_1, \ldots, V'_N\}$ of $T$, called *variable vertices*, corresponds to the $N$ positions of the codewords of $\mathcal{C}$. Every vertex $V''_i$ of the other class $\{V''_1, V''_2, \ldots, V''_R\}$ is called a *subcode vertex* and is associated with the parity-check relation corresponding to the $i$-th row of $H$. In other words, the $j$-th column ($i$-th row) of $H$ is identified with a vertex $V'_j$ ($V''_i$) and a nonzero entry on a position $(i, j)$ of $H$ determines an edge of $T$ connecting $V'_j$ and $V''_i$. Note that a subcode corresponding to a vertex $V''_i$ can be treated as an $[n_i, n_i - 1]$ code $\mathcal{C}_i$ of codimension one whose parity-check matrix consists of the $i$-th row of $H$. This construction is considered in numerous works, see e.g. [6],[8]-[15],[19]-[24], and the references therein. The graph $T$ is called a *Tanner graph* of the code $\mathcal{C}$.

The above construction was generalized as follows, see e.g. [3]-[5],[16],[28],[29]. To a vertex $V''_i$ it is associated an $[n_i, k_i]$ subcode $\mathcal{C}_i$ with $n_i - k_i > 1$ redundancy symbols. In this case subcodes are called component or constituent codes and the code $\mathcal{C}$ is said to be a *generalized* LDPC code. We refer to the bipartite graph $T$ as to the *generalized Tanner graph* of $\mathcal{C}$. The degree of $V''_i$ is equal to the length $n_i$, and the code $\mathcal{C}_i$ is the projection of $\mathcal{C}$ on the positions associated with the vertices $V'_{j_1}, \ldots, V'_{j_{n_i}}$ adjacent to $V''_i$. Let $R^*$ denote the number of constituent codes. Clearly, $R = \sum_{i=1}^{R^*}(n_i - k_i)$ holds. The binary $R^* \times N$ matrix $S$, in which columns (rows) correspond to vertices $V'_j$ ($V''_i$) and the entry in position $(i, j)$ is 1 if and only if there is an edge of $T$ joining $V'_j$ and $V''_i$, will be called a *skeleton* (*framework*) for the $R \times N$ parity-check matrix $H$. Note that $H$ can be obtained from $S$ by substituting every unit on the $i$-th row of $S$ with a ($(n_i - k_i)$ -positional) column of a parity-check matrix $H_i$ of $\mathcal{C}_i$.

Another connection between codes and bipartite graphs is now considered, see e.g. [7],[17],[20],[25]-[27]. The main difference with respect to Tanner's construction is that a subcode is associated to *each* vertex of the graph, whereas code-symbols correspond to its edges.

*Basic construction of BG codes* ([17]). Let $G$ be an $n$ -regular bipartite graph with two classes of vertices $\{V_1, \ldots, V_m\}$ and $\{V_{m+1}, \ldots, V_{2m}\}$ (i.e. any vertex is adjacent to exactly $n$ vertices, but any two vertices from the same class are not adjacent). Let $\mathcal{C}_t$ be an $[n, k_t]$ *constituent code*, $t = 1, 2, \ldots, 2m$. A *bipartite-graph code* $\mathcal{C} = \mathcal{C}(G; \mathcal{C}_1, \ldots, \mathcal{C}_{2m})$ is a linear $[N, K]$ code with length equal to the number of edges of $G$, that is $N = mn$. Coordinates of $\mathcal{C}$ are in one-to-one correspondence with the edges of $G$. In addition, the projection of a codeword of $\mathcal{C}$ on the positions corresponding to the $n$ edges incident to the vertex $V_t$ must be a codeword of the constituent code $\mathcal{C}_t$. We call $G$ a *supporting graph* of the bipartite-graph code $\mathcal{C}$. Straightforward relations between the parameters of $G$ and $\mathcal{C}$ are the following:

$$N = mn,\ K \leq N - \sum_{t=1}^{2m}(n-k_t) = \sum_{t=1}^{2m} k_t - mn. \tag{2.1}$$

In [20] the case $\mathcal{C}_1 = \ldots = \mathcal{C}_{2m}$ is considered. In general, the constituent codes can be different. In [17] the case $\mathcal{C}_1 = \ldots = \mathcal{C}_m$, $\mathcal{C}_{m+1} = \ldots = \mathcal{C}_{2m}$, $k_1 \neq k_{m+1}$, is investigated. In [25] $k_1 = \ldots = k_{2m}$, but $2m$ distinct generalized Reed-Solomon codes $\mathcal{C}_t$ are used.

*Generalized basic construction of BG codes* (see e.g. [27] ). Let the supporting bipartite graph $G$ be biregular, and let $\{V_1, \ldots, V_{m_1}\}$ and $\{V_{m_1+1}, \ldots, V_{m_1+m_2}\}$ be its classes of vertices. Also, let the degree of every vertex from the first (second, resp.) class be equal to $n_1$ ($n_2$, resp.). Then $m_1 n_1 = m_2 n_2$. The constituent code $\mathcal{C}_t$ is an $[n_1, k_t]$ code for $t \leq m_1$ and an $[n_2, k_t]$ code for $t > m_1$. The parameters of the $[N, K]$ BG code $\mathcal{C}$ satisfy

$$N = m_1 n_1 = m_2 n_2,$$

$$K \leq N - \sum_{t=1}^{m}(n_1 - k_t) - \sum_{t=m+1}^{2m}(n_2 - k_t) = \sum_{t=1}^{2m} k_t - m_1 n_1. \tag{2.2}$$

## 2.2 Parity-check matrices of BG codes

The parity-check matrix $H$ of a BG code $\mathcal{C}$ can be obtained in two steps, see [25]. First, a skeleton matrix of $H$ is constructed. From codes arising from the basic construction, such skeleton matrix is a binary $2m \times N$ matrix $S(m, n)$ in which the $t$-th row is associated with the vertex $V_t$. The $j$-th column contains two units in the positions corresponding to the vertexes incident with the $j$ -th edge. In other words, $S(m, n)$ is the incidence matrix ("*edges-vertices*") of the supporting graph $G(M(m, n))$. Then, $H$ can be obtained from $S(m, n)$ by substituting every unit on the $t$-th row of $S(m, n)$ with a ($(n-k_t)$ -positional) column of a parity-check matrix $H_t$ of $\mathcal{C}_t$. For codes arising from the generalized basic construction the procedure is similar.

In Sections 4,5 we construct *circulant* matrices $M(m, n)$. The corresponding skeleton $S(m, n)$ can be represented as a block matrix consisting of $n$ identity matrices of order $m$ and $n$ circulant permutation matrices of size $m \times m$, see Remarks 4.7 and 4.11. Moreover, if the constituent codes are such that $\mathcal{C}_1 = \ldots = \mathcal{C}_m$ and $\mathcal{C}_{m+1} = \ldots = \mathcal{C}_{2m}$, then the parity-check matrix $H$ obtained from $S(m, n)$ consists of circulant submatrices and defines a QC code with relatively simple implementation.

From the skeleton $S$ of a BG code (considered as a GLDPC code) it is straightforward to obtain its generalized Tanner graph. In fact, it is the graph whose adjacency matrix is $S$.

## 2.3 Problem Statement

Let $M$ be a matrix of type either $M(m,n)$ or $M(m_1,m_2,n_1,n_2)$, and let $G=G(M)$. Since $M$ is $J_4$-free, the graph $G$ has girth at least 6. This improves performance of BG code $\mathcal{C}$ whose supporting graph is $G$. Also, if $\mathcal{C}$ is viewed as a GLDPC code, it is easily seen that the girth of its generalized Tanner graph is at least 10. By (2.1),(2.2), parameters $N$ and $K$ of the BG code $\mathcal{C}$ depend on the values of $m,n,m_1,m_2,n_1,n_2$.

Our *goal* is to provide *as many distinct parameters of BG codes with 4-cycle-free supporting graphs as possible.* This is equivalent to construct $J_4$-free matrices $M(m,n)$ and $M(m_1,m_2,n_1,n_2)$ with as many distinct parameters as possible.

## 2.4 Incidence structures

Many of the new matrices of type $M(m_1,m_2,n_1,n_2)$ constructed in this paper arise from incidence matrices of incidence structures. An incidence structure is a pair $\mathcal{I}=(\mathcal{P},\mathcal{L})$, where $\mathcal{P}$ is a set whose elements are called *points*, and $\mathcal{L}$ is a collection of subsets of $\mathcal{P}$ called *blocks* (or *lines* ). A point $P$ and a block $\ell$ are said to be *incident* if $P\in\ell$. An incidence matrix of $\mathcal{I}$ is a 01-matrix $M(\mathcal{I})$ where rows corresponds to blocks, columns to points, and an entry is 1 if and only if the corresponding point belongs to the corresponding block.

It is easily seen that the matrix $M(\mathcal{I})$ is a matrix of type $M(m_1,m_2,n_1,n_2)$ if and only if the incidence structure $\mathcal{I}$ satisfies the following properties: the number of points in each block is a constant $n_1$, the number of blocks containing a point is a constant $n_2$, and no point pair is contained in more than one block (note that $m_1$ is the number of blocks, and $m_2$ is the number of points). An incidence structure with this property is said to be a *configuration* [32, Section IV.6].

If $n_1=n_2=k$ (or, equivalently, the configuration has the same number $v$ of points and blocks), then $\mathcal{I}$ is said to be a *symmetric* $(v,k)$*-configuration*. In this case, $M(\mathcal{I})$ is of type $M(m,n)$, where $m=|\mathcal{P}|=|\mathcal{L}|$ and $n=n_1=n_2$. Projective and affine spaces over finite fields are well-known examples of symmetric configurations.

# 3 A Geometrical Construction of $J_4$-free matrices

Incidence matrices of several geometrical structures are widely used for obtaining parity-check matrices of LDPC codes, see [6],[8]-[10],[12],[15],[20]-[30] and the references therein.

In this section, we consider some configurations arising from projective and affine spaces, in order to obtain matrices of types $M(m,n)$ and $M(m_1,m_2,n_1,n_2)$.

**Construction A**. Take any point orbit $\mathcal{P}$ under the action of a collineation group $\Gamma$ in an affine or projective space of order $q$. Choose an integer $n\le q+1$ such that the set $\mathcal{L}(\mathcal{P},n)$ of lines meeting $\mathcal{P}$ in precisely $n$ points is not empty. Define the following incidence structure $\mathcal{I}$: the points are the points of $\mathcal{P}$, the lines are the lines of $\mathcal{L}(\mathcal{P}, n)$, the incidence is that of the ambient space. Let $M$ be the incidence matrix of $\mathcal{I}$.

**Theorem 3.1.** *The incidence structure $\mathcal{I}$ in Construction A is a configuration such that its incidence matrix is a matrix $M(|\mathcal{P}|, n)$ or $M(|\mathcal{L}(\mathcal{P}, n)|, |\mathcal{P}|, n, r_n)$, where $r_n$ denotes the number of lines of $\mathcal{L}(\mathcal{P}, n)$ through a point in $\mathcal{P}$.*

*Proof.* The number of points in a block is $n$. The number of lines through a point is a constant $r_n$: this depends on the key property that the collineation group $\Gamma$ acts transitively on $\mathcal{P}$. Finally, no two points lie in more than one block. We obtain a matrix $M(|\mathcal{P}|, n)$ if $n = r_n$ or a matrix $M(|\mathcal{L}(\mathcal{P}, n)|, |\mathcal{P}|, n, r_n)$ otherwise. □

**Example 3.2.** We consider a regular hyperoval $\mathcal{O}$ in the projective plane $PG(2, q)$, $q$ even, see [31, Section 8.4]. Let $\mathcal{P} = PG(2, q) \setminus \mathcal{O}$. Then $|\mathcal{P}| = q^2 - 1$. The set $\mathcal{P}$ is an orbit under the action of the collineation group $\Gamma \cong PGL(2, q)$ fixing $\mathcal{O}$. Let $n = q + 1$. The set $\mathcal{L}(\mathcal{P}, q + 1)$ consists of $\frac{1}{2}q(q - 1)$ lines external to $\mathcal{O}$. Every point of $\mathcal{P}$ lies on $\frac{1}{2}q$ such lines, as $\mathcal{O}$ has no tangents. We obtain a matrix of type

$$M(m_1, m_2, n_1, n_2) : m_1 = \frac{q(q-1)}{2},\ m_2 = q^2 - 1,\ n_1 = q + 1,\ n_2 = \frac{q}{2},\ q \text{ even}.$$

Note that the dual incidence structure is the 2-$(\frac{1}{2}q(q - 1), \frac{1}{2}q, 1)$ oval design [9].

**Example 3.3.** We consider a conic $\mathcal{K}$ in $PG(2, q)$, $q$ odd, see [31, Section 8.2].

1. Let $\mathcal{P}$ be the set of $\frac{1}{2}q(q - 1)$ *internal points* to $\mathcal{K}$. It is an orbit under the action of the collineation group $\Gamma_{\mathcal{K}} \cong PGL(2, q)$ fixing the conic.

   For $n = \frac{1}{2}(q - 1)$, the set $\mathcal{L}(\mathcal{P}, n)$ consists of $\frac{1}{2}q(q + 1)$ bisecants of $\mathcal{K}$. Every internal point lies on $r_n = \frac{1}{2}(q + 1)$ bisecants. We obtain a matrix of type

   $$M(m_1, m_2, n_1, n_2) : m_1 = \frac{q(q+1)}{2},\ m_2 = \frac{q(q-1)}{2},\ n_1 = \frac{q-1}{2},\ n_2 = \frac{q+1}{2},\ q \text{ odd}.$$

   For $n = \frac{1}{2}(q + 1)$, we take as $\mathcal{L}(\mathcal{P}, n)$ the set of $\frac{1}{2}q(q - 1)$ lines external to $\mathcal{K}$. Every internal point lies on $r_n = \frac{1}{2}(q + 1)$ external lines. We obtain a matrix of type

   $$M(m, n) : m = \frac{q(q-1)}{2},\ n = \frac{q+1}{2},\ q \text{ odd}.$$

2. Another orbit $\mathcal{P}_2$ of the group $\Gamma_{\mathcal{K}}$ is the set of $\frac{1}{2}q(q + 1)$ *external points* to $\mathcal{K}$. Let $n = \frac{1}{2}(q - 1)$. We form the set $\mathcal{L}(\mathcal{P}_2, \frac{1}{2}(q - 1))$ from $\frac{1}{2}q(q + 1)$ bisecants. Every external point lies on $r_n = n = \frac{1}{2}(q - 1)$ bisecants. We obtain a matrix of type

   $$M(m, n) : m = \frac{q(q+1)}{2},\ n = \frac{q-1}{2},\ q \text{ odd}.$$

**Example 3.4.** In $PG(2,q)$, with $q$ a square, let $\mathcal{P}$ be the complement of the Hermitian curve $\mathcal{H}$ of equation $x_0^{\sqrt{q}+1} + x_1^{\sqrt{q}+1} + x_2^{\sqrt{q}+1} = 0$ [31, Section 7.3],[32, Section 7.11]. It is an orbit under the action of the projective unitary group $PGU(3,q)$. As $\mathcal{H}$ contains $q\sqrt{q}+1$ rational points, we have $|\mathcal{P}| = q^2+q-q\sqrt{q}$. In $PG(2,q)$ there are $q^2+q-q\sqrt{q}$ lines meeting $\mathcal{H}$ in $\sqrt{q}+1$ points and $\mathcal{P}$ in $q-\sqrt{q}$ points. Every point of $\mathcal{P}$ lies on $q-\sqrt{q}$ such lines. We obtain a matrix of type

$$M(m,n) : m = q^2+q-q\sqrt{q},\ n = q-\sqrt{q},\ q \text{ square}.$$

The remaining $q\sqrt{q}+1$ lines of $PG(2,q)$ are tangent to $\mathcal{H}$ and meet $\mathcal{P}$ in $q$ points. Every point of $\mathcal{P}$ lies on $\sqrt{q}+1$ such lines. We obtain a matrix of type

$$M(m_1,m_2,n_1,n_2) : m_1 = q\sqrt{q}+1,\ m_2 = q^2+q-q\sqrt{q},\ n_1 = q,\ n_2 = \sqrt{q}+1,\ q \text{ square}.$$

It should be noted that Construction A works for any 2-$(v,k,1)$ design $D$ and for any group of automorphisms of $D$. The role of $q+1$ is played by the size of any block in $D$.

# 4 A construction from cyclic symmetric configurations

The aim of this section is to use automorphisms of symmetric $(v,k)$ -configurations $\mathcal{I}$ in order to obtain matrices of type $M(m,n)$ other than $M(\mathcal{I})$. In particular, we are interested in cyclic automorphism groups of $\mathcal{I}$.

**Definition 4.1.** A symmetric $(v,k)$-configuration $\mathcal{I} = (\mathcal{P},\mathcal{L})$ is *cyclic* if there exists a permutation $\sigma$ of $\mathcal{P}$ mapping blocks to blocks, and acting regularly on both $\mathcal{P}$ and $\mathcal{L}$.

We recall two well-known examples from Finite Geometry.

**Example 4.2.** Any Desarguesian projective plane $PG(2,q)$ is a cyclic symmetric $(q^2+q+1, q+1)$-configuration.

**Example 4.3.** Fix a point $P$ and a line $\ell$ in $PG(2,q)$ with $P \notin \ell$. Let $\mathcal{P}$ be the point set consisting of the points of $PG(2,q)$ distinct from $P$ and not lying on $\ell$. Let $\mathcal{L}$ be the line set consisting of lines of $PG(2,q)$ distinct from $\ell$ and not passing through $P$. Then $(\mathcal{P},\mathcal{L})$ is a cyclic symmetric $(q^2-1,q)$-configuration. In [35] such a configuration is called an *anti-flag*.

For a cyclic symmetric $(v,k)$-configuration $\mathcal{I} = (\mathcal{P},\mathcal{L})$ let $S$ be the cyclic group generated by $\sigma$. Let $\mathcal{P} = P_0,\ldots,P_{v-1}$ and $\mathcal{L} = \ell_0,\ldots,\ell_{v-1}$. Arrange indexes in such a way that

$$\begin{aligned} \sigma &: P_i \mapsto P_{i+1 \pmod v}, \\ \ell_i &= \sigma^i(\ell_0). \end{aligned} \tag{4.1}$$

Clearly,

$$P_i = \sigma^i(P_0), \quad P_{i+\delta} = \sigma^\delta(P_i). \tag{4.2}$$

For any divisor $d$ of $v$ the group $S$ has an unique cyclic subgroup $\widehat{S}_d$ of order $d$ generated by $\sigma^t$ where

$$t = \frac{v}{d}. \tag{4.3}$$

Let $O_0, O_1, \dots, O_{t-1}$ be the orbits of $\mathcal{P}$ under the action of the subgroup $\widehat{S}_d$. Clearly, $|O_i| = d$. We arrange indexes so that $P_0 \in O_0$ and $O_w = \sigma^w(O_0)$, whence $\sigma^w(O_c) = O_{c+w \pmod t}$. Therefore,

$$O_i = \{P_i, \sigma^t(P_i), \sigma^{2t}(P_i), \dots, \sigma^{(d-1)t}(P_i)\},\ i = 0, 1, \dots, t-1. \tag{4.4}$$

By (4.2),(4.4), each orbit $O_i$ consists of $d$ points $P_u$ with $u$ equal to $i$ modulo $t$.

Let $L_0, \dots, L_{t-1}$ be the orbits of the set $\mathcal{L}$ under the action of $\widehat{S}_d$. Obviously, $|L_i| = d$. We arrange indexes in such a way that $\ell_0 \in L_0$ and $L_w = \sigma^w(L_0)$. As a result,

$$L_i = \{\ell_i, \sigma^t(\ell_i), \sigma^{2t}(\ell_i), \dots, \sigma^{(d-1)t}(\ell_i)\},\ i = 0, 1, \dots, t-1. \tag{4.5}$$

Let

$$w_u = |\ell_0 \cap O_u|,\ u = 0, 1, \dots, t-1. \tag{4.6}$$

Clearly,

$$w_0 + w_2 + \ldots + w_{t-1} = k. \tag{4.7}$$

**Theorem 4.4.** *Let $\mathcal{I} = (\mathcal{P}, \mathcal{L})$ be a cyclic symmetric $(v,k)$-configuration. Let $d$ and $t$ be integers as in (4.3). Let $O_0, \dots, O_{t-1}$ and $L_0, \dots, L_{t-1}$ be, respectively, orbits of points and lines of $\mathcal{I}$ under the action of $\widehat{S}_d$. Assume also that for points, lines, and orbits, indexes are arranged as in (4.1), (4.2), (4.4), (4.5). Then for any $i$ and $j$, every line of the orbit $L_i$ meets the orbit $O_j$ in the same number of points $w_{j-i \pmod t}$, where $w_u$ is defined by (4.6).*

*Proof.* Fix some $j \in \{0, 1, \dots, t-1\}$. For any $a = 0, 1, \dots, v-1$, let $s_a$ be such that $0 \le s_a \le t-1$ and $s_a \equiv j - a \pmod t$. As $\sigma^a$ maps the orbit $O_{s_a}$ on $O_j$,

$$|\ \sigma^a(l_0) \cap O_j\ | = |l_0 \cap O_{s_a}| = w_{s_a}$$

holds. This proves that for any $i = 0, 1, \dots, t-1$ the line orbit $L_i$ consists of lines meeting $O_j$ in the same number of points $w_{j-i \pmod t}$. Then, as $O_j$ and $L_i$ have the same size, through any point $P \in O_j$ there pass exactly $w_{j-i \pmod t}$ lines in $L_i$, each of which meets $O_j$ in $w_{j-i \pmod t}$ points. $\square$

**Definition 4.5.** An $i \times j$ matrix $A$ is said to be *$d$-block circulant* if

$$A = \begin{bmatrix} C_{0,0} & C_{0,1} & \dots & C_{0,j/d-1} \\ C_{1,0} & C_{1,1} & \dots & C_{1,j/d-1} \\ \vdots & \vdots & \vdots & \vdots \\ C_{i/d-1,0} & C_{i/d-1,1} & \dots & C_{i/d-1,j/d-1} \end{bmatrix} \tag{4.8}$$

for some binary *circulant* $d \times d$ matrices $C_{\lambda,\mu}$, $0 \le \lambda \le i/d - 1$, $0 \le \mu \le j/d - 1$.

For a $d$-block circulant $i \times j$ matrix $A$ as in (4.8), the weight matrix $W(A)$ of $A$ is the $\frac{i}{d} \times \frac{j}{d}$ matrix whose entry in position $\lambda, \mu$ is the weight of $C_{\lambda,\mu}$, that is, the number of units in each row of $C_{\lambda,\mu}$.

We remark that in [35] square $i \times i$ $d$-block circulant matrices are called $(i,d)$-polycirculant.

**Corollary 4.6.** *Let $\mathcal{I}$ be as in Theorem 4.4. Then the $J_4$-free incidence $v \times v$ matrix $V$ of $\mathcal{I}$ is $d$-block circulant. More precisely, it can be represented as a $t \times t$ block matrix*

$$V = \begin{bmatrix} C_{0,0} & C_{0,1} & C_{0,2} & \dots & C_{0,t-1} \\ C_{1,0} & C_{1,1} & C_{1,2} & \dots & C_{1,t-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ C_{t-1,0} & C_{t-1,1} & C_{t-1,2} & \dots & C_{t-1,t-1} \end{bmatrix} \tag{4.9}$$

*where $C_{i,j}$ is a $J_4$-free binary* circulant *$d \times d$ matrix of weight $w_{j-i \pmod t}$. The weight matrix $W(V)$ is the circulant matrix*

$$W(V) = \begin{bmatrix} w_0 & w_1 & w_2 & w_3 & \dots & w_{t-2} & w_{t-1} \\ w_{t-1} & w_0 & w_1 & w_2 & \dots & w_{t-3} & w_{t-2} \\ w_{t-2} & w_{t-1} & w_0 & w_1 & \dots & w_{t-4} & w_{t-3} \\ w_{t-3} & w_{t-2} & w_{t-1} & w_0 & \dots & w_{t-5} & w_{t-4} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ w_1 & w_2 & w_3 & w_4 & \dots & w_{t-1} & w_0 \end{bmatrix}. \tag{4.10}$$

*Proof.* A submatrix $C_{i,j}$ corresponds to the intersections of the lines of the orbit $L_i$ with the points of orbit $O_j$. The submatrix is circulant due to the arrangements of (4.1), (4.2), (4.4), (4.5). $\square$

**Remark 4.7.** Let $C$ be a $J_4$-free binary circulant $d \times d$ matrix of weight $w$. Then several $J_4$-free matrices with different parameters can be constructed by using the natural *decomposition of square circulant* 01-*matrices*, cf. [23, Section IV, B]. Such new matrices are circulant or consist of circulant submatrices.

From now on, we assume that in circulant matrices rows are shifted to the right. For a circulant matrix $C$, consider the set $s(C) = \{s_1, s_2, \dots, s_w\}$ of the positions of the units in the first row of $C$, arranged in such a way that $1 \le s_1 < s_2 < \dots < s_w \le d$.

Let $I_d = I_d(1)$ be the identity matrix of order $d$ and let $I_d(v)$ be the circulant permutation $d \times d$ matrix obtained from $I_d$ by shifting of every row by $v-1$ positions. The matrix $C$ can be viewed as the superposition of $w$ matrices $I_d(s_i)$, $i = 1, 2, \ldots, w$.

Taking into account that the "starting" matrix $C$ is $J_4$-free, it is easy to see that the following holds:

1. The superposition of any $w-\delta$ distinct matrices $I_d(s_i)$ gives a $J_4$-free circulant $d \times d$ matrix of weight $w - \delta$.

2. Let $S_i$ be a subset of $s(C)$ with $|S_i| = w - \delta_i$. Let $C(S_i)$ be the superposition of $w - \delta_i$ matrices $I_d(s_u)$ with $s_u \in S_i$. A matrix consisting of distinct submatrices of type $C(S_i)$ is $J_4$-free provided that the subsets $S_i$ are pairwise disjoint.

3. If the subsets $S_1, S_2$ are disjoint, then the following matrix is $J_4$-free:
$$\begin{bmatrix} C(S_1) & C(S_2) \\ C(S_2) & C(S_1) \end{bmatrix}.$$

**Remark 4.8.** Let a matrix $M(m,n)$ be $d$-block circulant. Then, by Remark 4.7, a matrix $M(m, n-\delta)$ can be constructed for any $\delta \leq n$.

We are now in a position to describe our second construction of matrices $M(m_1, m_2, n_2, n_2)$. From now on, the subscript difference $j - i$ is calculated modulo $t$.

**Construction B.** Let $\mathcal{I} = (\mathcal{P}, \mathcal{L})$ be a cyclic symmetric $(v,k)$-configuration. Let $d$ and $t$ be integers as in (4.3). Let $V$ be as in (4.9). Fix some non-negative integers $u_1, \ldots, u_r$, $0 \leq u_i \leq t-1$. Let $V'$ be a matrix obtained from $V$ by replacing the circulant submatrices $C_{i,j}$ such that $j - i = u_k$ with $d \times d$ matrices $C_{i,j}(S_k)$ with $|S_k| = w_{j-i} - \delta_k$, as in Remark 4.7. Let $W(V')$ be the weight matrix of $V'$. If an $\frac{m_1}{d} \times \frac{m_2}{d}$ submatrix of $W(V')$ is such that the sum of the elements of every row (column) is equal to $n_1$ ($n_2$), then the corresponding submatrix of $V'$ is a $J_4$-free matrix $M(m_1, m_2, n_1, n_2)$. For $m_1 = m_2$ and $n_1 = n_2$, a matrix $M(m,n)$ is obtained.

**Example 4.9.** The matrices $C_{i,j}(S)$ obtained from the submatrix $C_{i,j}$ of (4.9) as in Remark 4.7, are circulant matrices $M(d, w_{j-i} - \delta)$, where $|S| = w_{j-i} - \delta$. Therefore, a family of $J_4$-free circulant matrices with the following parameters is obtained (cf. Remark 4.8):

$$M(m,n) : m = d,\ n = w_u - \delta,\ u = 0, 1, \ldots, t-1,\ \delta = 0, 1 \ldots, w_u - 1.$$

**Example 4.10.** By Remark 4.7, for any sequence of non-negative integers $w'_0, w'_1, \ldots, w'_{t-1}$ such that $w'_i \leq w_i$ there exists a $d$ -block circulant submatrix $V'$ of $V$ with

$$W(V') = \begin{bmatrix} w'_0 & w'_1 & w'_2 & w'_3 & \ldots & w'_{t-2} & w'_{t-1} \\ w'_{t-1} & w'_0 & w'_1 & w'_2 & \ldots & w'_{t-3} & w'_{t-2} \\ w'_{t-2} & w'_{t-1} & w'_0 & w'_1 & \ldots & w'_{t-4} & w'_{t-3} \\ w'_{t-3} & w'_{t-2} & w'_{t-1} & w'_0 & \ldots & w'_{t-5} & w'_{t-4} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ w'_1 & w'_2 & w'_3 & w'_4 & \ldots & w'_{t-1} & w'_0 \end{bmatrix}.$$

By Construction B, several $J_4$-free matrices $M(m,n)$ and $M(m_1,m_2,n_1,n_2)$ can be obtained as submatrices of $V'$. Here, we provide a list of parameters $m,n,m_1,m_2,n_1,n_2$ for some of these matrices. Significantly, every such matrix consists of circulant submatrices.

1. The matrix $V'$ itself is a matrix in $M(m,n)$. Taking into account (4.7), the possible choices for $V'$ give rise to matrices of type

$$M(m,n):m=v,\ n=\sum_{u=0}^{t-1}(w_u-\delta_u)=k-\delta,\ \delta\le k-1.$$

2. Assume that $w'_0=w'_1=\ldots=w'_{u-1}=w$, $u\ge 2$. Then for each non-negative integer $c\le\lceil\frac{u}{2}\rceil$ the submatrix of $V'$

$$(C'_{i,j})_{i=c-1,\ldots,2c-2,\ j=0,\ldots,c-1}$$

is a matrix of type

$$M(m,n):m=cd,\ n=cw,\ c=1,2,\ldots,\left\lceil\frac{u}{2}\right\rceil.$$

Matrices of type

$$M(m,n):m=cd,\ n=(c-h)w,\ c=1,2,\ldots,\left\lceil\frac{u}{2}\right\rceil,\ h=1,\ldots,c-1.$$

can be easily obtained by substituting some of the submatrices $C'_{i,j}$ with the null $d\times d$ matrix. Finally, the submatrices of $V'$

$$(C'_{i,j})_{i=c_1-1,\ldots,c_1+c_2-2,\ j=0,\ldots,c_1-1},\ 1\le c_1\le u,\ 1\le c_2\le u+1-c_1$$

are of type

$$\begin{aligned}M(m_1,m_2,n_1,n_2)\quad &:\quad m_1=c_1d,\ m_2=c_2d,\ n_1=c_2w,\\ n_2\quad &=\quad c_1w,\ c_1=1,2,\ldots,u,\ c_2=1,2,\ldots,u+1-c_1.\end{aligned}$$

3. Similarly to ii), if $w'_1=\ldots=w'_{t-1}=w, w'_0\neq w$ then matrices of the following types can be obtained:

$$M(m,n):m=cd,\ n=w'_0+(c-h)w,\ c=2,3,\ldots,t-1,\ h=1,2,\ldots,c.$$

4. Assume that $w'_i=w'_{i+f}=w'_{i+f+u}=w'_{i+2f+u}=w, f,u\ge 1$. Then the submatrix of $V'$

$$\begin{bmatrix} C'_{0,i+f} & C'_{0,i+2f+u}\\ C'_{f,i+f} & C'_{f,i+2f+u}\end{bmatrix}$$

is a matrix of type

$$M(m,n):m=2d,\ n=2w.$$

5. Assume that $w'_{u+1} = w'_0,\ w'_{u+2} = w'_1, \ldots, w'_{2u} = w'_{u-1},\ u \geq 1$. Then the submatrix of $V'$
$$(C'_{i,j})_{i=u,\ldots,2u,\ j=0,\ldots,u}$$
is a matrix of type
$$M(m,n) : m = (u+1)d,\ n = w'_0 + w'_1 + \ldots + w'_u.$$

6. Assume that $w'_{i_1} = w'_{i_2} = \ldots = w'_{i_u} = w,\ 2 \leq u \leq t$. Then for any $c$-subset $B$ of $\{i_1, i_2, \ldots, i_u\}$ the matrix
$$(C'_{0,j})_{j \in B}$$
is a matrix of type
$$M(m_1, m_2, n_1, n_2) : m_1 = d,\ m_2 = cd,\ n_1 = cw,\ n_2 = w,\ c = 2, 3, \ldots, u.$$

**Remark 4.11.** Assume that $M(m,n)$ is circulant (an instance is provided by Example 4.9). Let $s(M(m,n)) = (s_1, s_2, \ldots, s_n)$, cf. Remark 4.7. We consider $M(m,n)$ as a superposition of $n$ circulant permutation $m \times m$ matrices $I_m(s_i),\ i = 1, \ldots, n$. Then the skeleton $S(m,n)$ of the parity-check matrix $H$ of any BG code with supporting graph $G(M(m,n))$ is the following matrix consisting of circulant permutation $m \times m$ submatrices:
$$S(m,n) = \left[ \begin{array}{cccc} I_m & I_m & \ldots & I_m \\ I_m(s_1) & I_m(s_2) & \ldots & I_m(s_n) \end{array} \right]. \tag{4.11}$$
Such a structure of the skeleton matrix can be useful for code implementation. Assume that for constituent $[n, k_t]$ codes $\mathcal{C}_t$ we have $\mathcal{C}_1 = \ldots = \mathcal{C}_m,\ \mathcal{C}_{m+1} = \ldots = \mathcal{C}_{2m}$, (cf. Section 2). Let $r_t = n - k_t$. Let also $[c^{(t)}_{j,1} c^{(t)}_{j,2} \ldots c^{(t)}_{j,r_t}]$ be the $j$th column of a parity-check matrix $H_t$ of the code $\mathcal{C}_t$. We choose parity check matrices for constituent codes in such a way that $H_1 = \ldots = H_m,\ H_{m+1} = \ldots = H_{2m}$. Then the parity-check matrix $H$ corresponding to the skeleton (4.11) has the form
$$H = \left[ \begin{array}{cccc} c^{(1)}_{1,1} I_m & c^{(1)}_{2,1} I_m & \ldots & c^{(1)}_{n,1} I_m \\ \vdots & \vdots & \vdots & \vdots \\ c^{(1)}_{1,r_1} I_m & c^{(1)}_{2,r_1} I_m & \ldots & c^{(1)}_{n,r_1} I_m \\ c^{(m+1)}_{1,1} I_m(s_1) & c^{(m+1)}_{2,1} I_m(s_2) & \ldots & c^{(m+1)}_{n,1} I_m(s_n) \\ \vdots & \vdots & \vdots & \vdots \\ c^{(m+1)}_{1,r_{m+1}} I_m(s_1) & c^{(m+1)}_{2,r_{m+1}} I_m(s_2) & \ldots & c^{(m+1)}_{n,r_{m+1}} I_m(s_n) \end{array} \right].$$
The matrix $H$ consists of circulant submatrices and defines a QC code, cf. [6],[12],[19],[22]-[24]. QC codes can be encoded with the help of shift-registers with relatively small complexity, see e.g. [11], [18].

# 5 Intersection Numbers of Orbits of Singer Subgroups

In this section, the general results of Section 4 are applied to the special case $\mathcal{I} = PG(2,q)$ when $v = q^2+q+1$, $k = q+1$. We treat points of $PG(2,q)$ as nonzero elements of $F_{q^3}$. Elements $a, b$ of $F_{q^3}$ correspond to the same point if and only if $a = xb$, $x \in F_q$. All points can be represented by the set $\{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{q^2+q}\}$ where $\alpha$ is a a primitive element of $F_{q^3}$. Every class of elements of $F_{q^3}$ corresponding to the same point has one representative into the set. The point represented by $\alpha^i$ is denoted by $P_i$, i.e., $PG(2,q) = \{P_0, P_1, P_2, \ldots, P_{q^2+q}\}$. It is well-known that the map

$$\sigma : P_i \mapsto P_{i+1 \pmod{q^2+q+1}}$$

is a projectivity of $PG(2,q)$ acting regularly on the set of points and on the set of lines in $PG(2,q)$. The group $S$ generated by $\sigma$ is called the Singer group of $PG(2,q)$, whereas groups $\widehat{S}_d$ as defined in Section 4 are said to be Singer subgroups of $PG(2,q)$.

We investigate the possible cardinalities of the intersections of a fixed line of $PG(2,q)$ with point orbits of Singer subgroups, i.e., the values of $w_u$, see (4.6) and Theorem 4.4. It is a relevant problem for the purposes of this paper, as the parameters of the new $J_4$-free matrices, obtained by Construction B, depend on the features of the sequence $w_0, w_1, \ldots, w_{t-1}$, see (4.7) and Examples 4.9,4.10.

Let $q = p^h$ for some prime $p$. We use the notations of the previous section. The map

$$\tau : P_i \mapsto P_{ip \pmod{q^2+q+1}}$$

is a permutation on the points of $PG(2,q)$. Actually, it is easy to see that $\tau$ is a collineation of $PG(2,q)$, that is, $\tau$ maps collinear points onto collinear points. It is well known (see e.g. [38, Section 2.3.1]) that under the action of a cyclic collineation group of a finite projective plane, the point set and the line set have the same cyclic structure. Therefore, as $\tau$ fixes $P_0$, at least one line has to be left invariant by $\tau$. Arrange indexes in such a way that this fixed line is $\ell_0$, cf. (4.1), (4.6). By (4.4), $\tau$ acts on the set of orbits $O_0, \ldots, O_{t-1}$ as follows: $\tau(O_i) = O_{pi \pmod{t}}$. The orbit $O_0$ always is fixed by $\tau$.

Denote by $s(p,t)$ the number of orbits of $\mathbb{Z}_t \setminus \{0\}$ under the action of the permutation group generated by the map $i \mapsto p \cdot i$. Then the following result clearly holds.

**Proposition 5.1.** *The cyclic group generated by $\tau$ acts on the set $O_1, \ldots, O_{t-1}$ with $s(p,t)$ orbits.*

**Proposition 5.2.** *Let $t$ be a prime. Then $s(p,t)$ divides $t-1$ and $s(p,t)$ is the least integer $i$ such that $p \equiv \beta^i \pmod{t}$ for some primitive element $\beta \in \mathbb{Z}_t$.*

*Proof.* Let $e$ be the order of $p \pmod{t}$ in the multiplicative group of $\mathbb{Z}_t$. Then $s(p,t) = \frac{t-1}{e}$, and $p \pmod{t}$ is the $s(p,t)$-th power of a primitive element in $\mathbb{Z}_t$. $\square$

**Remark 5.3.** As $q^2+q+1$ is odd, $t$ is odd too. Also, $t \neq 5$, as it is straightforward to check that $q^2+q+1$ is not divisible by 5 for any prime power $q$.

**Proposition 5.4.** *The following holds*:

1. *If* $t \neq 3$, *then* $s(p,t) \leq \frac{t-1}{2}$.
2. *If* $t$ *does not divide* $p^2-1$, *then* $s(p,t) \leq \frac{t-1}{3}$.
3. $s(p,3) = 2$ *if* $p \equiv 1 \pmod 3$, *and* $s(p,3) = 1$ *if* $p \equiv 2 \pmod 3$.
4. $s(p,7) = 2$ *if* $p \equiv 2$ *or* $4 \pmod 7$, *and* $s(p,7) = 1$ *if* $p \equiv 3$ *or* $5 \pmod 7$.

*Proof.* Explicit values of $s(p,3)$ and $s(p,7)$ are straightforward. Let $m(p,t)$ be the smallest size of an orbit of $\mathbb{Z}_t \setminus \{0\}$ under the action of the group generated by the map $i \mapsto p \cdot i$. If $p \not\equiv 1 \pmod t$, then $m(p,t) \geq 2$. Note that as $(p^{2h}+p^h+1)/t$ must be an integer, the cases $p \equiv \pm 1 \pmod t$ can occur only for $t = 3$. Also, $m(p,t) = 2$ holds if and only if $p^2 \equiv 1 \pmod t$. Otherwise, $m(p,t) \geq 3$. $\square$

Let $v(t)$ be the number of distinct values of the integers $w_u$ of (4.6).

**Lemma 5.5.** *For any non-negative integer* $u \leq t-1$, *values* $w_u$ *and* $w_{pu \pmod t}$ *coincide. Moreover,* $v(t) \leq s(p,t)+1$, *and each value of* $w_u$, *with at most one exception* $w_0$ , *occurs at least* $(t-1)/s(p,t)$ *times.*

*Proof.* By our previous assumption the line $\ell_0$ is fixed by $\tau$. Therefore $w_u = w_{pu \pmod t}$. The other assertions are straightforward. $\square$

The case $s(p,t) = 1$, $v(t) \leq 2$, is investigated in [39].

**Remark 5.6.** By Proposition 5.4 and Lemma 5.5, $v(3) \leq 3$ if $p \equiv 1 \pmod 3$. Actually, in [40] it is proved that equality holds.

**Lemma 5.7.** *Let* $w_i$ *be as in (4.6). Then*

$$\sum_{i=0}^{t-1} w_i^2 = \frac{q^2+(t+1)q+1}{t}. \tag{5.1}$$

*Proof.* We consider the point orbit $O_0$ and the line orbits $L_i$ under the Singer subgroup $\widehat{S}_d$. By Theorem 4.4 and Corollary 4.6, for any $i = 0, \ldots, t-1$, through any point of $O_0$ there pass exactly $w_{-i \pmod t}$ lines in $L_i$, each of which meets $O_0$ in $w_{-i \pmod t}$ points. Therefore, the points on $O_0$ can be counted as follows:

$$d = \frac{q^2+q+1}{t} = 1 + \sum_{i=0}^{t-1} w_i(w_i - 1).$$

Together with (4.7), this proves the assertion. $\square$

**Corollary 5.8.** *Let $O_{i_1}, \dots, O_{i_{s(p,t)}}$ be orbit representatives of the action of $\tau$ on the orbits $O_1, \dots, O_{t-1}$. If $t$ is prime then*

$$\begin{aligned} w_0 + \frac{t-1}{s(p,t)} \sum_{j=1}^{s(p,t)} w_{i_j} &= q+1; \\ w_0^2 + \frac{t-1}{s(p,t)} \sum_{j=1}^{s(p,t)} w_{i_j}^2 &= \frac{q^2+(t+1)q+1}{t}. \end{aligned}$$

*Proof.* The assertions follow from (4.7) and Lemmas 5.5,5.7. ◻

**Proposition 5.9.** *Let $t = 3$, and let $i_0, i_1, i_2$ be such that $w_{i_0} \le w_{i_1} \le w_{i_2}$, $\{i_0, i_1, i_2\} = \{0,1,2\}$. Let $A = (q - \sqrt{q} + 1)/3$, $B = (q + \sqrt{q} + 1)/3$, $C = (q - 2\sqrt{q} + 1)/3$, $D = (q + 2\sqrt{q} + 1)/3$. Then the following holds:*

1. *If $q$ is a non square or $q = p^{2m}$, $p \equiv 1 \pmod 3$, then $w_{i_0} < A$, $A < w_{i_1} < B$, $w_{i_2} > B$.*
2. *If $q = p^{4m+2}$ and $p \equiv 2 \pmod 3$, then $\sqrt{q} \equiv 2 \pmod 3$ and $w_{i_0} = w_{i_1} = A$, $w_{i_2} = D$.*
3. *If $q = p^{4m}$ and $p \equiv 2 \pmod 3$, then $\sqrt{q} \equiv 1 \pmod 3$ and $w_{i_0} = C$, $w_{i_1} = w_{i_2} = B$.*

*Proof.* For the sake of simplicity assume that $i_0 = i$. By (4.7), ( 5.1), $w_0 + w_1 + w_2 = q+1, w_0w_1 + w_1w_2 + w_2w_3 = \frac{1}{2}((q+1)^2 - \frac{1}{3}(q^2+4q+1)) = \frac{1}{3}(q^2+q+1)$. Therefore, $w_0, w_1, w_2$ are the roots of the cubic polynomial

$$T^3 - (q+1)T^2 + \frac{q^2+q+1}{3}T - w_0w_1w_2.$$

The real function $t \mapsto t^3 - (q+1)t^2 + \frac{1}{3}(q^2+q+1)t - w_0w_1w_2$ is increasing in $]-\infty, A]$, decreasing in $[A, B]$, increasing in $[B, +\infty[$.

Clearly, when $q$ is not a square, $w_i = \frac{1}{3}(q \pm \sqrt{q} + 1)$ cannot hold. Also, taking into account Remark 5.6, if $p \equiv 1 \pmod 3$ we have three distinct values of $w_u$. Finally, if $p \equiv 2 \pmod 3$, then, by Proposition 5.4 and Lemma 5.5, $w_0 < w_1 < w_2$ cannot hold. ◻

**Proposition 5.10.** *Let $t = 3$, and let $i_0, i_1, i_2$ be as in Proposition 5.9. Then for any $i, j \in \{0,1,2\}$, the difference $4q - (3(w_i + w_j) - 2(q+1))^2$ equals $3s^2$ for some integer $s$.*

*Proof.* For the sake of simplicity assume that $i_0 = i$. Assume also that $i = 0$, $j = 1$. Consider the integers $X = w_0 + w_1$, $Y = w_0w_1$. By (5.1), $X = (q+1) - w_2$, $Y = \frac{1}{3}(q^2+q+1) - w_2X$, whence $Y = X^2 - (q+1)X + \frac{1}{3}(q^2+q+1)$. As the quadratic polynomial in $T$

$$T^2 - XT + Y = T^2 - XT + X^2 - (q+1)X + \frac{q^2+q+1}{3}$$

has two integer roots $w_0, w_1$, we obtain that

$$X^2 - 4\left(X^2 - (q+1)X + \frac{q^2+q+1}{3}\right) = \frac{4q - (3X - 2(q+1))^2}{3}$$

is the square of an integer. Then the assertion follows. $\square$

From the above Propositions, we obtain an easy algorithm to compute the possible $w_0, w_1, w_2$: for any integer $s < \frac{2}{\sqrt{3}}\sqrt{q}$ compute the difference $\Delta = 4q - 3s^2$. For the square values of $\Delta$, the integers $\frac{1}{3}(\sqrt{\Delta} + 2(q+1))$ are the only possible values of sums $w_i + w_j$.

We now consider the case $t > 3$.

**Proposition 5.11.** *Let $q = p^r$ be a square. Let $t$ be a prime divisor of $q^2+q+1$. Assume that $p \pmod t$ is a generator of the multiplicative group of $\mathbb{Z}_t$. (If $t$ is not prime, than we have to assume that the permutation group generated by the map $i \mapsto p \cdot i$ acts transitively on $\mathbb{Z}_t \setminus \{0\}$). Then $t$ divides either $q + \sqrt{q} + 1$ or $q - \sqrt{q} + 1$, and*

$$w_1 = w_2 = \ldots = w_{t-1} = \frac{q+1 \pm \sqrt{q}}{t},$$
$$w_0 = \frac{q+1 \pm (1-t)\sqrt{q}}{t}.$$

*Proof.* As $\tau^i(O_1) = O_{p^i \pmod t}$, the hypothesis of $p$ being a generator of the multiplicative group of $\mathbb{Z}_t$ ensures that $\tau$ acts transitively on the orbits $O_1, \ldots, O_{t-1}$. By our assumptions $\ell_0$ is a line fixed by $\tau$. Then clearly $w_1 = w_2 = \ldots = w_{t-1}$. Now (4.7) and (5.1) give $w_0 + (t-1)w_1 = (q+1)$, $2w_0w_1 + (t-2)w_1^2 = (q^2+q+1)/t$. Then $w_1$ is a root of

$$tT^2 - 2(q+1)T + \frac{q^2+q+1}{t}.$$

This proves the assertion. $\square$

We remark that the Proposition 5.11 is not empty: for example, for $q = 81$, $t = 7$ its hypothesis are satisfied. Some other values for which this holds are as follows: $q = 2^8$, $t = 13$; $q = 5^4$, $t = 7$; $q = 2^{12}$, $t = 19$; $q = 3^8$, $t = 7$; $q = 2^{16}$, $t = 13$; $q = 17^4$, $t = 7$.

**Proposition 5.12.** *Let $q$ be a square and $d = v(q+\sqrt{q}+1)$, $v \geq 1$. Then $t = \frac{1}{v}(q-\sqrt{q}+1)$ and $w_0 = \sqrt{q} + v$, $w_1 = \ldots = w_{t-1} = v$.*

*Proof.* Let $v = 1$. Then the point orbits $O_0, O_1, \ldots, O_{t-1}$ are Baer subplanes of $PG(2,q)$. The partition of the points $PG(2,q)$ given by the orbits of the map $\sigma^t$ is a partition into Baer subplanes [31, Section 4.3]. Every line of $PG(2,q)$ meets precisely one subplane in $\sqrt{q}+1$ points, and the remaining subplanes in one point. If $v > 1$, every orbit $O_i$ is an union of $v$ subplanes. $\square$

**Example 5.13.** By Proposition 5.12 for $v = 1$, Remarks 4.7, 4.8, and Example 4.10iii one can obtain a family of matrices

$$M(m,n) \quad : \quad m = c(q+\sqrt{q}+1),\ n = \sqrt{q}+c-\delta, \qquad (5.2)$$
$$c = 2,3,\dots,q-\sqrt{q},\ \delta = 0,1,\dots,\sqrt{q}+c-1.$$

**Proposition 5.14.** *Let $q$ be a square and $d = q-\sqrt{q}+1$. Then $t = q+\sqrt{q}+1$ and $w_u \le 2$ for every $u$. There are $v_j$ values of $u$ for which $w_u = j$, where $v_0 = \frac{1}{2}(q+\sqrt{q})$, $v_1 = \sqrt{q}+1$, and $v_2 = \frac{1}{2}(q-\sqrt{q})$.*

*Proof.* Each of the point orbits $O_0, O_1, \dots, O_{t-1}$ are Kestenband-Ebert complete arcs [31, Section 4.3]. The numbers $v_m$ are provided by straightforward computation. □

**Proposition 5.15.** *Let $d = 3$. Then $t = \frac{1}{3}(q^2+q+1)$ and $w_u \le 2$ for every $u$. There are $v_j$ values of $u$ for which $w_u = j$ , where $v_0 = \frac{1}{3}(q^2-2q+1)$, $v_1 = q-1$, and $v_2 = 1$.*

*Proof.* Each orbit $O_u$ consists of 3 non-collinear points. □

**Remark 5.16.** Note that the construction of [37, Theorem 3.8] can be viewed as a particular case of the construction of the present section, cf. Propositions 5.12 and 5.14.

For some $q$ and $d$, sequences $w_0, \dots, w_{t-1}$ are given in Table I. They are obtained from both the results of Sections 4,5 and computer search. As a matter of notation, an entry $s_i$ in a sequence indicates that $s$ should be repeated $i$ times.

Table I only shows some of the partitions arising from Singer subgroups. In fact, one can obtain many other results. For example, we obtained by computer the following pairs $(d, w_0)$ : $(991,15), (721,15), (1093,15), (817,21), (1261,21), (1519,21), (2107,21)$, $(3997,36), (5419,36), (3169,39), (3571,39), (6487,39), (6487,52), (7651,52), (7651,57)$, $(19,4), (61,7), (93,8), (127,9), (217,12), (399,14), (469,16), (1261,25), (1387,27)$, $(1519,28), (2107,31), (3997,43), (4921,48), (5419,49)$. All correspon- ding matrices $M(m,n)$ are circulant, see Example 4.9. By Remark 4.7, several matrices $M(d, w_0-\delta)$, $\delta \ge 0$, can be obtained as well.

# 6 Orbits of Affine Singer Groups

In this section, the general results of Section 4 are applied to the cyclic symmetric $(q^2-1, q)$-configuration described in Example 4.3. Fix the point $P = (1:0:0)$ and the line $\ell : X_0 = 0$ in $PG(2,q)$ . Let $\mathcal{P}$ be the point set consisting of the points of $PG(2,q)$ distinct from $P$ and not lying on $\ell$. Let $\mathcal{L}$ be the line set consisting of lines of $PG(2,q)$ distinct from $\ell$ and not passing through $P$. We treat points of $\mathcal{P}$ as nonzero elements of $F_{q^2}$. All points can be represented by the set $\{\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{q^2-2}\}$ where $\alpha$ is a primitive element of $F_{q^2}$. The point represented by $\alpha^i$ is denoted by $P_i$, i.e., $\mathcal{P} = \{P_0, P_1, P_2, \dots, P_{q^2-2}\}$. It is well-known that the map

$$\sigma : P_i \mapsto P_{i+1 \pmod{q^2-1}}$$

**TABLE I. Construction B. Theoretical and computer results for the case $\mathcal{I} = PG(2, q)$**

| $q$ | $d$ | $t$ | $w_0, w_1, \ldots, w_{t-1}$ | $q$ | $d$ | $t$ | $w_0, w_1, \ldots, w_{t-1}$ |
|---|---|---|---|---|---|---|---|
| 4 | 7 | 3 | $1, 1, 3$ | 53 | 409 | 7 | $12, 9, 9, 5, 9, 5, 5$ |
| 4 | 3 | 7 | $2, 1, 1, 0, 1, 0, 0$ | 61 | 1261 | 3 | $16, 25, 21$ |
| 7 | 19 | 3 | $1, 4, 3$ | 61 | 291 | 13 | $4_2, 3_2, 6_2, 4_2, 6, 4, 11, 4, 3$ |
| 7 | 3 | 19 | $2, 0_7, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1$ | 64 | 1387 | 3 | $27, 19, 19$ |
| 9 | 13 | 7 | $4, 1, 1, 1, 1, 1, 1$ | 64 | 219 | 19 | $11, 3_{18}$ |
| 9 | 7 | 13 | $2, 2, 0, 0, 2, 0, 1, 0, 1, 0, 0, 1, 1$ | 64 | 73 | 57 | $9, 1_{56}$ |
| 11 | 19 | 7 | $0, 1, 1, 3, 1, 3, 3$ | 67 | 1519 | 3 | $21, 28, 19$ |
| 11 | 7 | 19 | $0,1,2,1_2,0,1,0_2,1,0,2,0_5,2,1$ | 67 | 651 | 7 | $8, 13, 13, 7, 13, 7, 7$ |
| 13 | 61 | 3 | $4, 7, 3$ | 73 | 1801 | 3 | $19, 28, 27$ |
| 16 | 91 | 3 | $7, 7, 3$ | 79 | 2107 | 3 | $31, 21, 28$ |
| 16 | 39 | 7 | $2, 1, 1, 4, 1, 4, 4$ | 79 | 903 | 7 | $8, 9, 9, 15, 9, 15, 15$ |
| 16 | 21 | 13 | $5, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1$ | 81 | 949 | 7 | $4, 13, 13, 13, 13, 13, 13$ |
| 16 | 13 | 21 | $1,2_2,0_5,2,0,1,0,1,2,0_2,2,1_2,0,2$ | 81 | 511 | 13 | $4,8,8,6,9,8,9,1,6,4,6,9,4$ |
| 19 | 127 | 3 | $4, 7, 9$ | 83 | 367 | 19 | $5, 8, 4, 4, 4, 1, 1, 8, 3, 5, 4, 4, 5, 1, 5, 5, 8, 5, 4$ |
| 23 | 79 | 7 | $0, 5, 5, 3, 5, 3, 3$ | 97 | 3169 | 3 | $28, 31, 39$ |
| 25 | 217 | 3 | $7, 7, 12$ | 107 | 1651 | 7 | $13, 24, 15, 15, 13, 15, 13$ |
| 25 | 93 | 7 | $8, 3, 3, 3, 3, 3, 3$ | 109 | 3997 | 3 | $31, 43, 36$ |
| 25 | 31 | 21 | $6, 1_{20}$ | 109 | 1713 | 7 | $8, 15, 15, 19, 15, 19, 19$ |
| 25 | 21 | 31 | $2_2, 1_2, 2_2, 0, 2, 0_2, 1, 0, 2, 1, 0, 1, 0_3, 1, 2_2, 0_3, 2, 0_3, 2, 0$ | 125 | 829 | 19 | $4, 9, 9, 9, 9, 4, 4, 9, 9, 4, 9, 9, 4, 4, 4, 4, 9, 4, 9$ |
| 29 | 67 | 13 | $0, 3, 3, 4, 2, 3, 2, 3, 4, 0, 4, 2, 0$ | 137 | 2701 | 7 | $15, 23, 15, 23, 23, 24, 15$ |
| 31 | 331 | 3 | $7, 12, 13$ | 137 | 511 | 37 | $5, 8_2, 2, 5, 4, 5, 2, 6, 2_3, 3, 5, 2, 4, 3, 2, 5, 2, 4, 5, 3, 2, 6, 2_2, 3, 8, 3_2, 4_3, 2, 0, 6$ |
| 32 | 151 | 7 | $0, 5, 5, 6, 5, 6, 6$ | 139 | 1497 | 13 | $10,16_2,10_2,7,10_3,11,7,16,7$ |
| 37 | 469 | 3 | $13, 9, 16$ | 149 | 3193 | 7 | $12, 25, 25, 21, 25, 21, 21$ |
| 37 | 201 | 7 | $8, 3, 3, 7, 3, 7, 7$ | 151 | 3279 | 7 | $32, 19, 19, 21, 19, 21, 21$ |
| 37 | 67 | 21 | $0, 1, 2, 0, 1, 2, 1, 1, 2, 4, 1, 2, 4, 3, 2, 0, 1, 2, 4, 1, 4$ | 163 | 8911 | 3 | $63, 49, 52$ |
| 43 | 631 | 3 | $13, 12, 19$ | 163 | 3819 | 7 | $32, 25, 25, 19, 25, 19, 19$ |
| 49 | 817 | 3 | $13, 21, 16$ | 163 | 1407 | 19 | $6, 12, 6, 6, 9, 6, 7, 6, 9, 7, 13, 7, 12, 12, 9, 5, 6, 13, 13$ |
| 49 | 57 | 43 | $8, 1_{42}$ | 163 | 1273 | 21 | $9, 9, 5, 7, 9, 7, 7, 7, 5, 11, 5, 5, 7, 5, 16, 11, 9, 7, 11, 5, 7$ |

is a collineation of the incidence structure $\mathcal{I} = (\mathcal{P}, \mathcal{L})$ acting regularly on both $\mathcal{P}$ and $\mathcal{L}$. The group $S$ generated by $\sigma$ is called the affine Singer group of $\mathcal{I}$, whereas groups $\widehat{S}_d$, as defined in Section 4, are said to be affine Singer subgroups of $\mathcal{I}$.

The cases $d = q + 1$ and $d = q - 1$ are of particular interest. Every orbit under the action of the group $\widehat{S}_{q-1}$ is precisely the intersection of a line of $PG(2, q)$ through $P$ with the point set $\mathcal{P}$. We will refer to this intersection as to the *trace* of the line. On the other hand, the orbits under the action of the group $\widehat{S}_{q+1}$ are (disjoint) conics. Denote by $v(t)$ the number of distinct values of the integers $w_u$ of (4.6).

**Proposition 6.1.** *Let $t$ be a divisor of $q+1$. Then $v(t) = 2$ and $w_1 = w_2 = \ldots = w_{t-1} = (q + 1)/t$, $w_0 = (q + 1)/t - 1$.*

*Proof.* Let $\ell'$ be a line of $\mathcal{L}$ and let $(\ell')^*$ be the line of $PG(2, q)$ through $P$ meeting the removed line $\ell$ in the same point as $\ell'$. Then $\ell'$ is disjoint from the trace of $(\ell')^*$ but meets all the remaining $q$ traces. Each orbit $\mathcal{O}$ under the action of $\widehat{S}_d$ with $d = (q^2 - 1)/t = (q-1)(q+1)/t$ is a union of the traces of $(q+1)/t$ lines of $PG(2, q)$ through $P$. Therefore, the line $\ell'$ meets the orbit $\mathcal{O}$ in $(q + 1)/t$ points if $(\ell')^* \notin \mathcal{O}$ and in $(q + 1)/t - 1$ points if $(\ell')^* \in \mathcal{O}$. □

**Example 6.2.** Using Proposition 6.1 for $t = q+1$, Remarks 4.7, 4.8, and Examples 4.10ii, 4.10iii, one can obtain a family of matrices

$$M(m, n) \;:\; m = c(q-1),\ n = c - \delta,\ \delta = 0, 1, \ldots, c-1, \qquad c = 2, 3, \ldots, b,\ b = q \text{ if } \delta \geq 1,\ b = \left\lceil \frac{q}{2} \right\rceil \text{ if } \delta = 0. \tag{6.1}$$

**Proposition 6.3.** *Let $t$ be a divisor of $q-1$. Then $v(t) \leq 2(q-1)/t$ and $w_u \leq 2(q-1)/t$ for every $u$.*

*Proof.* Each orbit under the action of $\widehat{S}_d$ with $d = (q^2 - 1)/t = (q+1)(q-1)/t$ is a union of $(q-1)/t$ disjoint conics. Therefore, each line of $\mathcal{L}$ meets this orbit in at most $2(q-1)/t$ points. □

For some $q$ and $t$ such that $t$ does not divide $q + 1$, sequences $w_0, \ldots, w_{t-1}$ obtained from computer search are given in Table II.

# 7 Constructions not Arising from Collineation Groups

## 7.1 Product of Parabolas

Let $AG(r, q)$ be the $r$-dimensional affine space over $F_q$ (which is sometimes denoted as the Euclidean space $EG(r, q)$.) A point in $AG(r, q)$ corresponds to a vector in $F_q^r$. Following [41], in $AG(2v, q)$ with $q$ even we consider the product $K$ of $v$ parabolas, that is, the set of size $q^v$

$$K = \{(a_1, a_1^2, a_2, a_2^2, \ldots, a_v, a_v^2) \mid a_1, \ldots, a_v \in F_q\} \subset AG(2v, q).$$

In terms of [42, Section 2], $K$ is a maximal translation cap.

**TABLE II. Construction B. Theoretical and computer results for the case $\mathcal{I} = AG(2, q)$**

| $q$ | $d$ | $t$ | $w_0, w_1, \ldots, w_{t-1}$ | $q$ | $d$ | $t$ | $w_0, w_1, \ldots, w_{t-1}$ |
|---|---|---|---|---|---|---|---|
| 7 | 16 | 3 | $1, 2, 4$ | 31 | 160 | 6 | $5, 6, 8, 4, 2, 6$ |
| 7 | 8 | 6 | $1, 2, 2, 0, 0, 2$ | 37 | 456 | 3 | $9, 12, 16$ |
| 9 | 20 | 4 | $1, 2, 4, 2$ | 37 | 342 | 4 | $9, 12, 10, 6$ |
| 9 | 10 | 8 | $1, 2, 2, 2, 0, 0, 2, 0$ | 37 | 114 | 12 | $1, 4_4, 6, 2, 0, 4, 2, 4, 2$ |
| 11 | 24 | 5 | $3, 2, 2, 0, 4$ | 41 | 420 | 4 | $13, 8, 8, 12$ |
| 11 | 15 | 8 | $3, 1, 1, 1, 0, 2, 1, 2$ | 41 | 336 | 5 | $5, 12, 10, 6, 8$ |
| 11 | 12 | 10 | $1, 2_2, 0, 2_2, 0_3, 2$ | 41 | 140 | 12 | $3, 2_3, 5, 2, 4, 5_2, 4, 2, 5$ |
| 13 | 56 | 3 | $5, 2, 6$ | 43 | 616 | 3 | $17, 10, 16$ |
| 13 | 42 | 4 | $5, 2, 2, 4$ | 49 | 800 | 3 | $17, 20, 12$ |
| 13 | 28 | 6 | $3, 0, 2, 2, 2, 4$ | 49 | 600 | 4 | $9, 12, 16, 12$ |
| 13 | 21 | 8 | $1, 1, 2, 2, 4, 1, 0, 2$ | 49 | 300 | 8 | $1, 6, 8, 6, 8, 6, 8, 6$ |
| 13 | 14 | 12 | $1, 0_2, 2_4, 0, 2, 0_2, 2$ | 53 | 702 | 4 | $17, 12, 10, 14$ |
| 17 | 72 | 4 | $5, 2, 4, 6$ | 61 | 1240 | 3 | $25, 16, 20$ |
| 17 | 36 | 8 | $1, 0, 2, 2, 4, 2, 2, 4$ | 61 | 930 | 4 | $13, 18, 18, 12$ |
| 17 | 24 | 12 | $3, 1, 2_2, 1_2, 0, 2, 1, 0, 2_2$ | 81 | 1312 | 5 | $9, 18, 18, 18, 18$ |
| 19 | 120 | 3 | $9, 6, 4$ | 81 | 656 | 10 | $1, 8, 10, 8, 10, 8, 10, 8, 10, 8$ |
| 19 | 60 | 6 | $3, 2, 2, 6, 4, 2$ | 89 | 1980 | 4 | $25, 18, 20, 26$ |
| 19 | 45 | 8 | $3, 4, 2, 4, 2, 1, 2, 1$ | 97 | 3136 | 3 | $37, 34, 26$ |
| 25 | 208 | 3 | $5, 10, 10$ | 103 | 3536 | 3 | $41, 32, 30$ |
| 25 | 156 | 4 | $5, 8, 8, 4$ | 109 | 2970 | 4 | $29, 32, 26, 22$ |
| 25 | 104 | 6 | $1, 4, 6, 4, 6, 4$ | 121 | 4880 | 3 | $33, 44, 44$ |
| 27 | 91 | 8 | $1, 3, 3, 3, 6, 4, 3, 4$ | 121 | 2440 | 6 | $13, 20, 24, 20, 24, 20$ |
| 29 | 210 | 4 | $5, 6, 10, 8$ | 121 | 1220 | 12 | $1, 10, 12, 10, 12, 10, 12, 10, 12, 10, 12, 10$ |
| 29 | 120 | 7 | $5, 2, 4, 4, 8, 4, 2$ | 169 | 4080 | 7 | $13, 26, 26, 26, 26, 26, 26$ |
| 31 | 320 | 3 | $9, 8, 14$ | 169 | 2040 | 14 | $1, 12, 14, 12, 14, 12, 14, 12, 14, 12, 14, 12, 14, 12$ |
| 31 | 192 | 5 | $7, 4, 6, 4, 10$ | | | | |

Let $A = AG(2v, q)\backslash K$ be the complement of $K$. Clearly, $|A| = q^v(q^v - 1)$. In $AG(2v, q)$, there are $q^{2v-1}B_{q,v}$ lines, where $B_{q,v} = (q^{2v} - 1)/(q - 1)$ is the number of lines through every point. Since $K$ is a cap, it is easily seen that $q^v B_{q,v} - q^v(q^v - 1)/2$ lines meet $K$ and $q^v(q^{v-1} - 1)B_{q,v} + q^v(q^v - 1)/2$ lines lie entirely in $A$.

**Proposition 7.1.** *The number of lines contained in $A$ through a given point is constant and equal to $B_{q,v} - q^v + \frac{1}{2}(q - 2)$.*

*Proof.* As $K$ is a maximal translation cap in $AG(2v, q)$, from [42, Proposition 2.5 ] it follows that through any point in $A$ there pass exactly $\frac{1}{2}(q-2)$ secants of $K$. In addition, we have exactly $q^v - q + 2$ tangents to $K$. □

By Proposition 7.1, the incidence structure whose points are the points in $A$ and whose lines are the lines contained in $A$ is a configuration. Matrices in $M(m_1, m_2, n_1, n_2)$ are then obtained for the following values of the parameters:

$$\begin{aligned} m_1 &= q^v(q^{v-1}-1)\frac{q^{2v}-1}{q-1} + \frac{q^v(q^v-1)}{2},\ n_1 = q, \\ m_2 &= q^v(q^v-1),\ n_2 = \frac{q^{2v}-1}{q-1} - q^v + \frac{q-2}{2},\ q \text{ even.} \end{aligned}$$

## 7.2 Projective Spaces and Subspaces

Fix $h$ and $q$, and an integer $s$, with $0 \le s \le h-1$. Consider the following incidence structure: points are subspaces of $PG(h,q)$ of dimension $s$; blocks are subspaces of $PG(h,q)$ of dimension $s+1$; incidence is set-theoretical inclusion. This structure is a configuration. By [31, Theorem 3.1], the numbers of points and blocks are, respectively,

$$v_{h,s} = \prod_{i=h-s+1}^{h+1}(q^i-1)\prod_{i=1}^{s+1}\frac{1}{q^i-1},\ b_{h,s} = \prod_{i=h-s}^{h+1}(q^i-1)\prod_{i=1}^{s+2}\frac{1}{q^i-1};$$

the number of points in a block is $(q^{s+2}-1)/(q-1)$ (by duality, the number of hyperplanes in a space of dimension $s+1$ is the number of points of the space); the number of blocks through a point is $(q^{h-s}-1)/(q-1)$ (again by duality, the number of subspaces of dimension $s+1$ containing a given subspace of dimension $s$ coincides with the number of hyperplanes of a subspace of dimension $h-1-s$). Clearly, no two points are contained in two distinct blocks. Then matrices of the following type are obtained:

$$M(m_1, m_2, n_1, n_2) : m_1 = b_{h,s},\ m_2 = v_{h,s},\ n_1 = \frac{q^{s+2}-1}{q-1},\ n_2 = \frac{q^{h-s}-1}{q-1}.$$

When $h-s = s+2$, that is $h = 2c$ is even and $s = \frac{h}{2}-1 = c-1$, we have $b_{h,s} = v_{h,s}$, $n_1 = n_2$. This gives matrices

$$M(m,n) : m = \prod_{i=c+2}^{2c+1}(q^i-1)\prod_{i=1}^{c}(q^i-1)^{-1},\ n = \frac{q^{c+1}-1}{q-1}, c \ge 1.$$

If $h = 2$ the incidence structure is just the projective plane. For $h = 4$, $c = 2$, $s = 1$, we obtain the following parameters

$$M(m,n) : m = (q^2+1)(q^4+q^3+q^2+q+1), n = q^2+q+1.$$

### 7.3 $q$-Cancellation Construction

This construction is given in [37, Constructions 3.2,3.3], see also the references therein and [25].

In the projective plane $PG(2,q)$ we fix a line $\ell$ and a point $P$ and assign an integer $s \geq 0$. If $P \in \ell$ we choose $s$ points on $\ell$ distinct from $P$, and $s$ lines through $P$ distinct from $\ell$. If $P \notin \ell$ we choose $s$ arbitrary points on $\ell$ and consider the $s$ lines connecting $P$ with these points. The incidence structure obtained from $PG(2,q)$ by dismissing all the lines through the $s+1$ selected points and all the points lying on the $s+1$ selected lines provides a matrix

$$M(m,n) : n = q - s,\ m = \begin{cases} q^2 - qs & \text{if } P \in \ell \\ q^2 - (q-1)s - 1 & \text{if } P \notin \ell \end{cases}. \tag{7.1}$$

It should be noted that Example 4.3 describes a particular case of this construction with $P \notin \ell$, $s = 0$. Significantly, in this case the incidence structure has a cyclic automorphism group. It essentially extends the list of parameters and gives matrices consisting of circulant submatrices, see Proposition 6.1 and Example 6.2.

# 8 Summary of new symmetric configurations

For $q$ a power prime, the constructions using complements of Baer subplanes [35] and Example 4.2 give rise to symmetric configurations with parameters $(q^4-q, q^2)$ and $(q^2+q+1, q+1)$. Such configurations, together with configurations with parameters $(m,n)$ where $m,n$ are as in (7.1), will be referred to as *classical* . In [33] symmetric configurations with the following parameters $(m^*, n^*)$ are obtained: $(69,8), (89,9), (111,10), (145,11), (171,12),$ $(213,13),$ $(255,14), (303,15), (355,16), (399,17), (433,18),$ $(493,19),$ $(567,20), (667,21),$ $(713,22), (745,23), (851,24),$ $(961,25)$. In [33] it is also proved that symmetric configurations with parameters $(m_1, n^*)$ with $m_1 > m^*$ exist for every pair $(m^*, n^*)$. Therefore, it would be interesting to obtain *non-classical* configurations with parameters $(m_2, n^*)$ with $m_2 < m^*$.

In [35] configurations with the following parameters $(m_2, n^*)$ are constructed: $(98,10),$ $(242,14), (338,16),$ $(338,17),$ $(578,21), (722,23)$.

The following new parameters $(m_2, n^*)$ with $m_2 < m^*$ are obtained from the constructions proposed in Sections 3-7 : $n^* = 8$, $m_2 = 65$; $n^* = 11$, $m_2 = 133$; $n^* = 12$, $m_2 = 168$; $n^* = 13$, $m_2 = 183, 189$; $n^* = 14$, $m_2 = 210, 231, 252$; $n^* = 15, m_2 = 231, 252, 272, 273$; $n^* = 16$, $m_2 = 273, 288, 307, 324, 341, 342$; $n^* = 17$, $m_2 = 307, 342, 360, 372, 381$; $n^* = 18$, $m_2 = 360, 381, 403$; $n^* = 19$, $m_2 = 381, 434, 462, 465, 484$; $n^* = 20$, $m_2 = 465,$ $484, 496,$ $506, 525, 527, 528, 552, 553, 558, 651$; $n^* = 21$, $m_2 = 496, 506, 527, 552, 553, 558, 576, 589,$ $598, 600, 620, 624, 644, 650, 651$; $n^* = 22, m_2 = 527, 528, 553, 558, 576, 589, 600, 620, 624,$ $650, 651, 672, 676, 700, 702$; $n^* = 23$, $m_2 = 553, 558, 589, 600, 620, 650, 651, 672, 676, 700,$

$702, 728$; $n^* = 24$, $m_2 = 589, 620, 624, 651, 676, 702, 728, 756, 780, 784, 806, 810, 812, 837, 840$; $n^* = 25, m_2 = 651, 702, 756, 784, 810, 812, 837, 840, 868, 870, 899, 900, 930$.

Table III illustrates how to obtain some of the above parameters $m_2$. In column "C", $a, b$ and $c$ stand for Examples 3.4, 5.13, and 6.2, respectively, whereas $d$ (resp. $e$ ) means that the parameters are obtained by applying Remark 4.7i to the cyclic structures of Examples 4.2 (resp. 4.3); $f$ stands for Example 4.10iii.

**TABLE III. Obtaining the new parameters**

| $n^*$ | $m_2$ | C | $q$ | $c$ | $\delta$ | $n^*$ | $m_2$ | C | $q$ | $c$ | $\delta$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | 65 | $b$ | 9 | 5 | 0 | 16, 17 | 342 | $c$ | 19 | 19 | 3, 2 |
| 11 | 133 | $d$ | 11 | | 1 | 17, 18 | 360 | $d$ | 19 | | 2, 1 |
| 12 | 168 | $b$ | 16 | 8 | 0 | 17 | 372 | $b$ | 25 | 12 | 0 |
| 13 | 183 | $d$ | 13 | | 1 | 17,18,19 | 381 | $d$ | 19 | | 3,2,1 |
| 13 | 189 | $b$ | 16 | 9 | 0 | 18 | 403 | $b$ | 25 | 13 | 0 |
| 14 | 210 | $b$ | 16 | 10 | 0 | 19 | 434 | $f$ | 25 | 2 | |
| 14,15 | 231 | $b$ | 16 | 11 | 1, 0 | 19 | 462 | $c$ | 23 | 21 | 2 |
| 14,15 | 252 | $b$ | 16 | 12 | 2, 1 | 19, 20 | 465 | $b$ | 25 | 15 | 1, 0 |
| 15 | 272 | $c$ | 17 | 17 | 2 | 19, 20 | 484 | $c$ | 23 | 22 | 3, 2 |
| 15,16 | 273 | $d$ | 16 | | 2, 1 | 20, 21 | 496 | $b$ | 25 | 16 | 1, 0 |
| 16 | 288 | $e$ | 17 | | 1 | 20, 21 | 506 | $c$ | 23 | 23 | 3, 2 |
| 16,17 | 307 | $d$ | 17 | | 2, 1 | 20 | 525 | $a$ | 25 | | |
| 16 | 324 | $c$ | 19 | 18 | 2 | 20,21,22 | 527 | $b$ | 25 | 17 | 2,1,0 |
| 16 | 341 | $b$ | 25 | 11 | 0 | 20 | 528 | $c$ | 25 | 22 | 2 |

# Acknowledgments

The authors would like to thank Valentine B. Afanassiev and Victor V. Zyablov for useful discussions of code aspects of the problems investigated, and Marien Abreu, Domenico Labbate and Vito Napolitano for helpful discussions on symmetric configurations.

# References

[1] R. G. Gallager, Low-Density Parity-Check Codes. Cambridge, MA: MIT Press, 1963.

[2] R. M. Tanner, A recursive approach to low complexity codes, IEEE Trans. Inf. Theory 27 (1981), 533-547.

[3] M. Sipser and D. Spielman, Expander codes, IEEE Trans. Inf. Theory 42 (1996), 1710-1722.

[4] M. Lentmaier and K. Sh. Zigangirov, On generalized low-density parity-check codes based on Hamming component codes, IEEE Commun. Lett. 3 (1999), 248-260.

[5] J. Boutros, O. Pothier, and G, Zémor, Generalized low density (Tanner) codes, in Proc. IEEE Int. Conf. Commun. (ICC) 1, Vancouver, BC, Canada. (1999), 441-445.

[6] Y. Kou, S. Lin, M. P. C. Fossorier, Low-density parity-check codes based on finite geometries: a rediscovery and new results, IEEE Trans. Inf. Theory 47 (2001), 2711-2736.

[7] A. Barg and G. Zémor, Error exponents of expander codes, IEEE Trans. Inf. Theory 48 (2002), 1725-1729.

[8] S. J. Johnson and S. R. Weller, Resolvable 2-designs for regular low-density parity-check codes, IEEE Trans. Commun 51 (2003), 1413-1419.

[9] S. R. Weller and S. J. Johnson, Regular low-density parity-check codes from oval designs, Eur. Trans. Telecommun. 14 (2003), 399-409.

[10] S. J. Johnson and S. R. Weller, High-rate LDPC codes from unital designs, in Proc. IEEE Globecom Conf., San Francisco, CA, USA. (2003), 150-152.

[11] S. Lin and D. J. Costello, Jr., Error Control Coding: Fundamental and Applications, Upper Saddle River, NJ: Prentice Hall, 2nd edition, 2004.

[12] M. P. C. Fossorier, Quasi-cyclic low-density parity-check codes from circulant permutation matrices, IEEE Trans. Inf. Theory 50 (2004), 1788-1793.

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

[14] 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. Inf. Theory 50 (2004), 2966-2984.

[15] H. Tang, J. Xu, S. Lin, and K. A. S. Abdel-Ghaffar, Codes on finite geometries, IEEE Trans. Inf. Theory 51 (2005), 572-596.

[16] N. Miladinović and M. Fossorier, Generalized LDPC codes with Reed-Solomon and BCH codes as component codes for binary channels, in Proc. IEEE Global Comm. Conf. (Globecom), St. Luis, MO, USA, 3. (2005), 6-10.

[17] A. Barg and G. Zémor, Distances properties of expander codes, IEEE Trans. Inf. Theory 52 (2006), 78-90.

[18] Z.-W. Li, L. Chen, L. Zeng, S. Lin, and W. H. Fong, Efficient encoding of quasi-cyclic low-density parity-check codes, IEEE Trans. Commun. 54 (2006), 71-81.

[19] E. Gabidulin, A. Moinian, and B. Honary, Generalized construction of quasi-cyclic regular LDPC codes based on permutation matrices, in Proc. Int. Symp. Inf. Theory 2006, ISIT 2006, Seattle, USA. (2006), 679-683.

[20] T. Høholdt and J. Justesen, Graph codes with Reed-Solomon component codes, in Proc. Int. Symp. Inf. Theory 2006, ISIT 2006, Seattle, USA. (2006), 2022-2026.

[21] E. M. Gabidulin, On LDPC matrices equivalent to Vandermonde matrices, in Proc. X Int. Workshop Algebraic Comb. Coding Theory, ACCT 2006, Zvenigorod, Russia, Sep. 2006, 97-101. Available at: http://dcn.infos.ru/acct/ACCT2006/papers/gabi.pdf

[22] G. Liva, S. Song, L. Lan, Y. Zhang, S. Lin, and W. E. Ryan, Design of LDPC codes: a survey and new results, J. Comm. Software Syst. 2 (2006), 191-211.

[23] J. Xu, L. Chen, I. Djurdjevic, and K. Abdel-Ghaffar, Construction of regular and irregular LDPC codes: geometry decomposition and masking, IEEE Trans. Inf. Theory 53 (2007), 121-134.

[24] L. Lan, L. Zeng, Y. Y. Tai, L. Chen, S. Lin, and K. Abdel-Ghaffar, Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: a finite field approach, IEEE Trans. Inf. Theory 53 (2007), 2429-2458.

[25] V. B. Afanassiev, A. A. Davydov, and V. V. Zyablov, Low density concatenated codes with Reed-Solomon component codes, in Proc. XI Int. Symp. on Problems of Redundancy in Inf. and Control Syst., St.-Petersburg, Russia. (2007), 47-51. Available at: http://k36.org/redundancy2007

[26] A. Mazumdar, Analysis of bipartite graph codes on the binary erasure channel, in Proc. 4-5 Annual Allerton Conf., UIUC, Illinois, USA. (2007), 897-904. Available at: http://www.csl.uiuc.edu/allerton/archives/allerton07/PDFs/papers/0030.pdf

[27] A. Barg and A. Mazumdar, Thresholds for bipartite-graph codes on the binary symmetric channel, preprint, 2008. Available at: http://www.ece.umd.edu/~arya/bgbsc.pdf

[28] N. Miladinović and M. P. C. Fossorier, Generalized LDPC codes and generalized stopping sets, IEEE Trans. Commun. 56 (2008), 201-212.

[29] V. Zyablov, R. Johannesson, M. Lončar, and P. Rybin, On the error-correcting capabilities of low-complexity decoded LDPC codes with constituent Hamming codes, in Proc. XI Int. Workshop Algebraic Comb. Coding Theory, ACCT2008,

Pamporovo, Bulgaria. (2008), 325-337. Available at: http://www.moi.math.bas.bg/acct2008/b54.pdf

[30] A. A. Davydov, M. Giulietti, S. Marcugini and F. Pambianco, Symmetric configurations for bipartite-graph codes, in Proc. XI Int. Workshop Algebraic Comb. Coding Theory, ACCT2008, Pamporovo, Bulgaria. (2008), 63-69. Available at: http://www.moi.math.bas.bg/acct2008/b11.pdf

[31] J. W. P. Hirschfeld, Projective Geometries over Finite Fields, 2nd ed., Oxford, U.K.: Oxford Science, 1998.

[32] C. J. Colbourn and J. Dinitz, Eds., The CRC Handbook of Combinatorial Designs, 2-nd edition. Boca Raton, FL: CRC Press, 2006.

[33] H. Gropp, On the existence and non-existence of configurations $n_k$, J. Combin. Inform. System Sci. 15 (1990), 34-48.

[34] H. Gropp, Non-symmetric configurations with deficiencies 1 and 2, in: Combinatorics 90, Ann. Discrete Math. 52 (1992), 227-239.

[35] M. Funk, D. Labbate, V. Napolitano, Tactical (de-)compositions of symmetric configurations, Discr. Math. 309 (2009), 741-747.

[36] M. Abreu, M. Funk, D. Labbate, and V. Napolitano, On (minimal) regular graphs of girth 6, Australas. J. Combin. 35 (2006), 119-132.

[37] A. Gács and T. Héger, On geometric constructions of $(k, g)$-graphs, Contrib. Discr. Math. 3 (2008), 63-80.

[38] P. Dembowski, Finite Geometries, Springer, Berlin, 1968.

[39] N. Hamilton and T. Penttila, Sets of type $(a, b)$ from subgroups of $\Gamma L(1, p^R)$, J. Algebraic Combin. 13 (2001), 67-76.

[40] J. Coykendall and J. Dover, Sets with few intersection numbers from Singer subgroup orbits, Europ. J. Combin. 22 (2001), 455-464.

[41] A. A. Davydov, M. Giulietti, S. Marcugini and F. Pambianco, New inductive constructions of complete caps in $PG(N, q)$, $q$ even, J. Comb. Des., to appear.

[42] M. Giulietti, Small complete caps in $PG(N, q)$, $q$ even, J. Comb. Des. 15 (2007), 420-436.

[43] A. A. Davydov, M. Giulietti, S. Marcugini and F. Pambianco, On sharply transitive sets in $PG(2, q)$, Innovations Incidence Geom. 6-7 (2009) 139-151.