Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 63-69*

Symmetric configurations for bipartite-graph codes

Alexander Davydov adav@iitp.ru
Institute for Information Transmission Problems, Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 127994, RUSSIA

Massimo Giulietti, Stefano Marcugini, Fernanda Pambianco
giuliet, gino, fernanda@dipmat.unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, Perugia, 06123, ITALY

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 have at most one unit in the same position. In terms of Design Theory, such a matrix is an incidence matrix of a symmetric configuration. Also, it gives rise to an n-regular bipartite graphs without 4-cycles, which can be used for constructing bipartite-graph codes so that both the classes of their vertices are associated with local constraints (constituent codes). We essentially extend the region of parameters of such matrices by using some results from Galois Geometries. 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.

1 Introduction

Bipartite-graph codes are studied in the context of low-density parity check (LDPC) codes, see [1],[2],[4],[6]-[8], and the references therein.

In [7] Tanner proposed to associate a bipartite graph T to an $[N, K]$ code $\mathcal{C}$ in the following way. Fix a positive integer U, and for any $i = 1, \ldots, U$ choose a set of n_i distinct positions of codewords of $\mathcal{C}$, that is a subset $j_1, \ldots, j_{n_i}$ of $\{1, \ldots, N\}$. One class of vertices $\{V'_1, \ldots, V'_N\}$ of T correspond to the positions of the codewords of $\mathcal{C}$. Let $\{V''_1, V''_2, \ldots, V''_U\}$ be the other class. A vertex V''_i has degree n_i and is adjacent with $V'_{j_1}, \ldots, V'_{j_{n_i}}$. The $[n_i, k_i]$ subcode $\mathcal{C}_i$ obtained from $\mathcal{C}$ by projection to the positions corresponding to $j_1, \ldots, j_{n_i}$ is called a *local constraint on variables*, while the vertices $V'_1, \ldots, V'_N$ are said to be the *variable vertices* of T. If $n_i - k_i = 1$ holds for all subcodes $\mathcal{C}_i$, one can build the graph T directly using the $U \times N$ parity-check matrix H of the code $\mathcal{C}$: the jth column (ith row) of H is identified with a vertex V'_j (V''_i) and every

nonzero entry into H implies an edge of T. Usually, such variant of T is called the *Tanner graph* of the code $\mathcal{C}$ [8].

We consider the following modification of the construction of [7] , see [2],[1]. 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 $\mathcal{C}$ to 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 $\mathcal{C}$.

To a supporting graph G it can be naturally associated a square 01-matrix $M(m, n)$ of order m with n units in every row and column. The ith row (jth column) of $M(m, n)$ corresponds to the vertex V_i (V_{m+j}). The entry in position (i, j) is 1 if and only if V_i and V_{m+j} are adjacent. It is easily seen that the graph G is 4-cycle free if and only if the matrix $M(m, n)$ does not contain the 2×2 submatrix J_4 consisting of all units. A matrix without submatrix J_4 is called a *J_4-free matrix.*

In order to improve the performance of the code, it is desirable to increase the girth of the graph [7],[8]. We study supporting graphs with girth at least six (i.e. with no 4-cycles). It should be noted that if *the supporting graph* of a bipartite-graph code has girth at least *six*, then the girth of the *Tanner graph* of this code is at least *ten*.

Parameters of the bipartite-graph codes depend on the values of m and n. The goal of this work is *to construct J_4-free matrices $M(m, n)$ with* ***distinct parameters*** *m, n.*

J_4-free matrices for LDPC codes are considered in many papers, see e.g. [1],[4],[8] and the references therein. Mainly, non-square matrices are investigated. It is also known that both symmetric and resolvable non-symmetric 2-$(v, k, 1)$ designs [3] can be used for obtaining J_4-free matrices $M(v, k)$. The reason is that in a 2-$(v, k, 1)$ design every pair of elements is contained in *exactly* one block. Actually, in order to obtain a J_4 -free matrix $M(m, n)$ it is enough that every pair of elements is contained in *at most* one block. An incidence structure with this property is said to be a *configuration* [3, Sec. IV.6]. If a configuration is *symmetric*, then its incidence matrix is a J_4 -free matrix $M(m, n)$.

Even though J_4-free matrices $M(m, n)$ have already been studied in literature, the region of parameters of the constructed matrices is not wide enough if compared to the permanently growing needs of practice, when often exact values of m, n are necessary. Also, it should be considered that distinct con-

structions of matrices have distinct properties, and clearly some choice can be useful.

In this work we propose a number of constructions of both square and non-square J_4-free matrices based on incidence structures in projective spaces $PG(v,q)$ over Galois fields F_q (see [3],[5] for basic facts on Galois Geometries).

We essentially extend the region of parameters of J_4-free square 01-matrices with the same number of units in every row and column. The obtained matrices have new structures that gives wide choice for code implementation. Many of them either are circulant or consist of circulant submatrices: this provides code parity-check matrices consisting of circulant submatrices which give rise to quasi-cyclic (QC) bipartite-graph codes. QC codes can be encoded with complexity linearly proportional to code length [4],[6].

2 Construction A: a single orbit of a collineation group

Construction A. Take any point orbit $\mathcal{P}$ under the action of a collineation group 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: 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 starting space. Let M be the incidence matrix of such a structure.

Theorem 1 *In Construction A the number of lines of $\mathcal{L}(\mathcal{P},n)$ through a point of $\mathcal{P}$ is a constant r_n. If $n=r_n$, the matrix M in Construction A is a J_4-free matrix $M(|\mathcal{P}|,n)$.*

Example 2 i) *We consider a conic $\mathcal{K}$ in $PG(2,q)$, q odd [5, Sec. 8.2]. Let $\mathcal{P}$ be the set of $\frac{1}{2}q(q-1)$* internal points *to $\mathcal{K}$. It is an orbit under the collineation group $G_{\mathcal{K}}$ fixing the conic. Let $n=\frac{1}{2}(q+1)$. Then $\mathcal{L}(\mathcal{P},n)$ is the set of lines external to $\mathcal{K}$. We obtain*

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

Another orbit $\mathcal{P}_2$ of the group $G_{\mathcal{K}}$ is the set of $\frac{1}{2}q(q+1)$ external points *to $\mathcal{K}$. We form the set $\mathcal{L}(\mathcal{P}_2,\frac{1}{2}(q-1))$ from $\frac{1}{2}q(q+1)$ bisecants. As a result, we obtain a matrix*

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

ii) *Let $\mathcal{P}$ be the complement of a Baer subplane π of $PG(2,q)$, q a square. It is an orbit of the collineation group fixing π. The set $\mathcal{L}(\mathcal{P},q)$ is the set of tangents to π. We obtain*

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

iii) *In $PG(2,q)$, q a square, let $\mathcal{P}$ be the complement of the Hermitian curve [5, Sec. 7.3]. It is an orbit of the group $PGU(3,q)$ fixing the point $(0,0,1)$. We obtain*

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

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.

3 Construction B: an union of orbits of a Singer subgroup

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 $a = xb$, $x \in F_q$. Let α be a primitive element of F_{q^3}. The point represented by α^i is denoted by P_i. Then $PG(2,q) = \{P_0, P_1, \ldots, P_{q^2+q}\}$. The map $\sigma : P_i \mapsto P_{i+1 \pmod{q^2+q+1}}$ is a projectivity of $PG(2,q)$. The group S of order q^2+q+1 generated by σ is called the Singer group of $PG(2,q)$ [5, Sec. 4.2]. Clearly, $P_i = \sigma^i(P_0)$.

For any divisor d of q^2+q+1, the group S has a unique cyclic subgroup $\widehat{S}_d$ of order d, namely the group generated by σ^t, $t = (q^2+q+1)/d$. It is well known that under the action of a cyclic collineation group *the point set and the line set of a projective plane have the same cyclic structure.*

Let $O_0, O_1, \ldots, O_{t-1}$ be the orbits of points of $PG(2,q)$ under the action of the subgroup $\widehat{S}_d$. Clearly, $|O_i| = d$. We arrange indexes so that $P_0 \in O_0$, $O_v = \sigma^v(O_0)$. Then

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

Let ℓ_0 be a fixed line of $PG(2,q)$ and let $\ell_i = \sigma^i(\ell_0)$. Then the set of lines of $PG(2,q)$ is $L = \{\ell_0, \ell_1, \ell_2, \ldots, \ell_{q^2+q}\}$. Let $L_0, \ldots, L_{t-1}$ be the orbits of the set L under the action of $\widehat{S}_d$. Clearly, $|L_i| = d$. We arrange indexes in such a way that $\ell_0 \in L_0$, $L_v = \sigma^v(L_0)$. Then

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

Theorem 3 *Let $t = (q^2+q+1)/d$ and let $O_0, \ldots, O_{t-1}$ (resp. $L_0, \ldots, L_{t-1}$) be the point (resp. line) orbits under the action of the Singer subgroup $\widehat{S}_d$ of order d. Assume that for points, lines, and orbits, indexes are arranged as in (1) and (2). 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 $w_u = |\ell_0 \cap O_u|$, $u = 0, 1, \ldots, t-1$.*

Corollary 4 *Let d and t be as in Theorem 3. The J_4-free incidence $(q^2+q+1)\times(q^2+q+1)$ matrix V of the plane $PG(2,q)$ can be represented as follows*:

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

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

Weights w_u of the submatrices $C_{i,j}$ can be written as the circulant $t\times t$ matrix

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

Remark 5 *We use in the sequel the following natural* decomposition of square circulant *01*-matrices*, cf. [8, Sec. IV, B]. From now on, we assume that in circulant matrices rows are shifted to the right. A binary circulant $d\times d$ matrix C of weight w is defined by the vector $s(C)=(s_1,s_2,\dots,s_w)$ where the s_i 's are the positions of the units in the first row of C, arranged in such a way that $s_1<s_2<\ldots<s_w$. Let $I_d=I_d(0)$ 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 positions. The matrix C can be treated as the superposition of w matrices $I_d(s_i)$, $i=1,\dots,w$. From the matrix C one can obtain a circulant matrix $C^{(\delta)}$ of weight $w-\delta$ using the superposition of any $w-\delta$ distinct matrices $I_d(s_i)$. It should also be noted that* if the starting matrix C is J_4 -free then any matrix $C^{(\delta)}$ is J_4-free too.

Construction B. Fix some integers $u_1,\dots,u_r$, $0\le u_i\le t-1$. Let V' be a matrix obtained from V by replacing the circulant submatrices $C_{i,j}$ such that $j-i=u_k \pmod t$ with $d\times d$ matrices $C_{i,j}^{(\delta_{u_k})}$ as in Remark 5. Here, and in the rest of the paper, the subscript difference $j-i$ is calculated modulo t. Let $W(V')$ be the matrix $W(V)$ in which corresponding elements w_{j-i} are changed by $w'_{j-i}=w_{j-i}-\delta_{j-i}$. If an $\frac{m}{d}\times\frac{m}{d}$ submatrix of $W(V')$ is such that the sum of elements of every row and every column is equal to the same number n, then the corresponding submatrix of V' is a J_4-free matrix $M(m,n)$.

Example 6 *The matrix $C_{i,j}^{(\delta)}$, obtained from the submatrix $C_{i,j}$ of V as in Remark 5, is a circulant matrix $M(d,w_{j-i}-\delta)$. So, we can form a family of J_4-free circulant matrices.*

$$M(m,n): m=d,\ n=w_u-\delta,\ u=0,1,\dots,t-1,\ \delta=0,1\dots,w_u-1. \quad (3)$$

Example 7 *By Remark 5, from the matrix V several families of J_4-free matrices $M(m,n)$ can be obtained. Significantly, every such matrix consists of circulant submatrices. Sometimes some conditions on weights w'_u of submatrices $C_{i,j}^{(\delta_{j-i})}$ are needed. Here, we provide a list of parameters m,n of some of these families of J_4-free matrices $M(m,n)$.*

i) $m = q^2+q+1$, $n = \sum_{u=0}^{t-1}(w_u - \delta_u) = q+1-\sum_{u=0}^{t-1}\delta_u$, $\delta_u = 0, 1 \ldots, w_u$.

ii) $m = cd$, $n = (c-h)w$, $c = 1, 2, \ldots, \left\lceil \frac{k}{2} \right\rceil$, $h = 0, 1, \ldots, c-1$.

(for $w'_0 = w'_1 = \ldots = w'_{k-1} = w$, $k \geq 2$);

iii) $m = cd$, $n = w_0 - \delta_0 + (c-h)w$, $\delta_0 = 0, 1, \ldots, w_0$, $c = 2, 3, \ldots, t-1$, $h = 1, \ldots, c$.

(for $w'_0 = w_0 - \delta_0 \neq w$, $w'_1 = \ldots = w'_{t-1} = w$);

iv) $m = 2d$, $n = 2w$

(for $w'_i = w'_{i+m} = w'_{i+m+k} = w'_{i+2m+k} = w$, $k \geq 1$, $m \geq 1$);

v) $m = (k+1)d$, $n = w'_0 + w'_1 + ... + w'_k$.

(for $w'_{k+1} = w'_0$, $w'_{k+2} = w'_1, \ldots, w'_{2k} = w'_{k-1}$, $k \geq 1$).

Remark 8 *Assume that $M(m,n)$ is a circulant matrix, see e.g. Example 6. Let $M(m,n)$ be defined by the vector $s(M(m,n)) = (s_1, s_2, \ldots, s_n)$, see Remark 5. We consider $M(m,n)$ as a superposition of n circulant permutation $m \times m$ matrices $I_m(s_i)$, $i = 1, \ldots, n$. Assume that for constituent $[n, k_t]$ codes $\mathcal{C}_t$ we have $\mathcal{C}_1 = \ldots = \mathcal{C}_m$, $\mathcal{C}_{m+1} = \ldots = \mathcal{C}_{2m}$. Let $r_t = n - k_t$. Let also $[c_{j,1}^{(t)} c_{j,2}^{(t)} \ldots c_{j,r_t}^{(t)}]$ be the jth column of a parity check matrix H_t of the q-ary code $\mathcal{C}_t$. Finally, let $H_1 = \ldots = H_m$, $H_{m+1} = \ldots = H_{2m}$. Then the parity check matrix H corresponding to the code associated to the matrix $M(m,n)$ has the form*

$$H = \begin{bmatrix} c_{1,1}^{(1)} I_m & c_{2,1}^{(1)} I_m & \ldots & c_{n,1}^{(1)} I_m \\ \vdots & \vdots & \vdots & \vdots \\ c_{1,r_1}^{(1)} I_m & c_{2,r_1}^{(1)} I_m & \ldots & c_{n,r_1}^{(1)} I_m \\ c_{1,1}^{(m+1)} I_m(s_1) & c_{2,1}^{(m+1)} I_m(s_2) & \ldots & c_{n,1}^{(m+1)} I_m(s_n) \\ \vdots & \vdots & \vdots & \vdots \\ c_{1,r_{m+1}}^{(m+1)} I_m(s_1) & c_{2,r_{m+1}}^{(m+1)} I_m(s_2) & \ldots & c_{n,r_{m+1}}^{(m+1)} I_m(s_n) \end{bmatrix}.$$

The matrix H consists of circulant submatrices, and therefore it defines a QC code, cf. [4],[8]. QC codes can be implemented with relatively small complexity [6].

References

[1] V. B. Afanassiev, A. A. Davydov, V. V. Zyablov, Low density concatenated codes with Reed-Solomon component codes, *Proc. XI Intern. Symp. Problems Redund. Inf. Contr. Syst.*, S.-Petersburg, Russia, 2007, 47-51.

[2] A. Barg, G. Zémor, Distances properties of expander codes, *IEEE Trans. Inform. Theory* 52, 2006, 78-90.

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

[4] E. Gabidulin, A. Moinian, B. Honary, Generalized construction of quasi-cyclic regular LDPC codes based on permutation matrices, *Proc. Intern. Symp. ISIT 2006*, Seattle, USA, 2006, 679-683.

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

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

[7] R. M. Tanner, A recursive approach to low complexity codes, *IEEE Trans. Inform. Theory* 27, 1981, 533-547.

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