AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **35** (2006), Pages 119–132

On (minimal) regular graphs of girth 6

M. Abreu* M. Funk*

Dipartimento di Matematica, Università della Basilicata
Viale dell'Ateneo Lucano, 85100 Potenza
Italy
abreu@unibas.it funk@unibas.it

D. Labbate*

Dipartimento di Matematica, Politecnico di Bari
Via E. Orabona, 4, 70125 Bari
Italy
labbate@poliba.it

V. Napolitano*

Dipartimento di Matematica, Università della Basilicata
Viale dell'Ateneo Lucano, 85100 Potenza
Italy
vnapolitano@unibas.it

Abstract

We consider finite simple κ-regular graphs of girth 6 with as few vertices as possible. We construct a class $S(\kappa)$ of κ-regular bipartite graphs of girth 6. The graphs in $S(\kappa)$ are sometimes *minimal*, i.e. they have the smallest number of vertices known so far among the κ-regular graphs of girth 6. In particular, the graph $S(11)$ is an 11-regular graph on 240 vertices which has the same order as a graph due to P. K. Wong (*Internat. J. Math. Math. Sci.* 9 (1986), 561–565). Moreover, for several values of κ, e.g. $\kappa = 13, 19, 21$, $S(\kappa)$ gives new minimal graphs.

Furthermore, we conjecture and prove for $q = 2, 3, 4$ the existence of another class that gives rise to 16- and 15-regular bipartite graphs of girth 6 on 504 and 462 vertices, respectively, that improves the order of the graphs $S(16)$ and $S(15)$. All graphs are constructed via their adjacency matrices using algebraic tools.

* This research was carried out within the activity of INdAM-GNSAGA and supported by the Italian Ministry MIUR.

1 Preliminaries

A (κ, g)-*cage* is a κ-regular finite simple graph (without loops and multiple edges) of girth g with the least possible number of vertices.

We are interested in finding κ-regular graphs of girth 6 with as few vertices as possible. This problem is related to $(\kappa, 6)$-cages. The discussion on $(\kappa, 6)$-cages and minimal regular graphs of girth 6 is based on the widely known fact that classical examples of $(\kappa, 6)$-cages arise from finite projective planes via their *incidence graphs* [4].

A *partial plane* (introduced by M. Hall in 1943 [10]) is an incidence structure $\mathcal{S} = (X, L, |\,)$ such that any two distinct *points* in X are incident with at most one *line* in L. The *incidence graph* $\Gamma(\mathcal{S})$ has vertex set $X \cup L$, while the edges are just the incident point-line pairs (i.e. the vertices $p \in X$ and $l \in L$ make up an edge if and only if one has $p|l$). $\Gamma(\mathcal{S})$ is bipartite and has girth at least 6.

For any prime power $q = p^m$, the incidence graph $\Gamma(PG(2, q))$ of the finite Desarguesian projective plane $PG(2, q)$ gives rise to a $(q + 1, 6)$-cage. Hence, there are always $(\kappa, 6)$-cages, for any integer κ, when $\kappa - 1$ is a prime power. Very little is known when $\kappa - 1$ is not a prime power. For instance, if $\kappa = 7$, there is a unique $(7, 6)$-cage, usually named after O'Keefe and Wong [14], actually first discovered by Baker [1, 2] in terms of an *elliptic semiplane*, i.e. a certain partial plane on 45 points whose incidence graph is the $(7, 6)$-cage.

A partial plane $\mathcal{S} = (X, L, |\,)$ gives rise to a $(0, 1)$-matrix called the *incidence matrix*: fix two labelings $X = \{p_0, \ldots, p_r\}$ and $L = \{l_0, \ldots, l_s\}$, and define $M = (m_{i,j})$ with $m_{i,j} = 1$ if $p_i|l_j$ and $m_{i,j} = 0$ otherwise. The incidence matrix is unique up to reordering of rows and columns since relabeling the points (lines) of $\mathcal{S}$ results in a permutation of the rows (columns) of M.

Lemma 1.1 *A $(0, 1)$-matrix is the incidence matrix of some partial plane if and only if it does not contain any 2×2 submatrix all of whose entries are 1.*

Proof. The forbidden substructure characterizing partial planes consists of two distinct points p_1, p_2 and two distinct lines l_1, l_2 such that for all $i, j \in \{1, 2\}$ one has $p_i|l_j$, whose incidence matrix is $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. □

Recall the definition of the *adjacency matrix* of a simple graph $G = (V, E)$ without loops: fix a labeling $V = \{v_0, \ldots, v_r\}$ and define $A = (a_{i,j})$ with $a_{i,j} = 1$ if $\{v_i, v_j\} \in E$ and $a_{i,j} = 0$ otherwise. The adjacency matrix is unique up to a simultaneous reordering of rows and columns since relabeling the vertices results in a permutation of the rows and columns of A. Obviously, A is symmetric and has entries 0 in its main diagonal.

The following remark is given as an exercise in several Graph Theory text books e.g. [4, p. 11] and [6, p. 8].

Remark 1.2 *Let I be an incidence matrix of a partial plane $\mathcal{S} = (X, L, |\,)$ and A be the adjacency matrix of the incidence graph $\Gamma(\mathcal{S})$, both defined with respect to the* *same labeling for the elements in X and L. Then, we have*

$$A = \begin{pmatrix} O & I \\ I^t & O \end{pmatrix},$$

where O is a matrix all of whose entries are 0 *and I^t is the transpose of I. The graph whose adjacency matrix is A is bipartite.*

We define a $(0,1)$-matrix to be $\mathbf{C_4}$**-free** if it satisfies the hypothesis of Remark 1.2. This name is motivated by the fact that the forbidden substructure characterizing a partial plane (introduced in the Proof of Lemma 1.1) would appear as a 4-cycle in the incidence graph of such a partial plane.

2 Correspondence between $(0,1)$-Blocks and elements of an abelian group $\mathcal{G}$

Large $(0,1)$-matrices are difficult to handle, in particular when checking whether they are C_4-free. In favorable situations, however, the $(0,1)$-matrix M under consideration reveals an appropriate block matrix structure with square blocks. Let $(\mathcal{G},+)$ be an abelian group of order r. Our approach consists in constructing a $1-1$ correspondence between square $(0,1)$-blocks of M and elements of $\mathcal{G}$ in such a way that checking whether M is C_4-free can be translated into inspecting algebraic equations with coefficients in $\mathcal{G}$.

In $(\mathcal{G},+)$, let $\mathcal{G}=\{z_1=0,z_2,\dots,z_r\}$ be a fixed labeling. Define the matrix $\tau(\mathcal{G})$ as an addition table for $(\mathcal{G},+)$ given by

$$\tau(\mathcal{G})_{i,j} := z_i + z_j\,, \quad \text{for } i,j = 1,\dots,r\,.$$

(similarly to [12, p. 30]). For short, we will write $\tau_{i,j}$ instead of $\tau(\mathcal{G})_{i,j}$ when it is clear what the group $\mathcal{G}$ is.

Definition 2.1 *Let $z\in\mathcal{G}$. We define the $(0,1)$-matrix P_z of order r with*

$$(P_z)_{i,j} \quad := \quad \begin{cases} 1 & \textit{if } \tau(\mathcal{G})_{i,j} = z \\ 0 & \textit{otherwise}\,. \end{cases}$$

Since the element z appears in each row and column of the addition table $(\tau(\mathcal{G})_{i,j})$ precisely once, P_z is a *permutation matrix* of order r.

Definition 2.2 *Let $B=(b_{i,j})$ be an $s\times t$ matrix whose entries are elements of $\mathcal{G}$. We define the* **blow up** *$\overline{B}$ of B* **through the group** *$(\mathcal{G},+)$ in the following way: $\overline{B}$ is the $s\times t$ block matrix having square blocks $\overline{B}_{i,j}$ of order r such that for all $i=1,\dots,s$ and $j=1,\dots,t$ we have*

$$\overline{B}_{i,j} = P_z \quad \textit{if and only if} \quad b_{i,j} = z\,.$$

Hence, $\overline{B}$ is a $(0,1)$-matrix with rs rows and rt columns.

Proposition 2.3 *(Criterion 1) The* $(0,1)$*-matrix* $\overline{B}$ *is* C_4*-free if and only if for each* 2×2 *submatrix* S *of* B*, say*

$$S \quad = \quad \begin{pmatrix} a & b \\ d & c \end{pmatrix}, \quad (a,b,c,d \in \mathcal{G}),$$

we have

$$a-b+c-d \neq 0\,.$$

Proof. To prove sufficiency, assume that $\overline{B}$ has an ordinary submatrix of order 2 all of whose entries are 1. Clearly, these four entries occur in four distinct blocks of $\overline{B}$. Since the entries lie two by two in the same row and the same column, we find entries 1 in positions

$$(i,j) \text{ in } P_a\,, \ \ (i,k) \text{ in } P_b\,, \ \ (l,k) \text{ in } P_c\,, \ \text{ and } (l,j) \text{ in } P_d\,,$$

for some $i,j,k,l \in \{1,\ldots,r\}$. By Definition 2.1, these imply:

$$z_i+z_j = a\,, \ \ z_i+z_k = b\,, \ \ z_l+z_k = c\,, \ \text{ and } \ z_l+z_j = d\,.$$

Subtracting the second and fourth equations from the sum of the first and third, we obtain $0 = a-b+c-d$, a contradiction.

To prove necessity, suppose $S = \left(\begin{smallmatrix} a & b \\ d & c \end{smallmatrix}\right)$ is a submatrix of B such that $a-b+c-d = 0$. Then $\overline{B}$ has a block submatrix $\overline{S} = \left(\begin{smallmatrix} P_a & P_b \\ P_d & P_c \end{smallmatrix}\right)$. In the first row of P_a and P_b there is precisely one entry 1, say in positions $(P_a)_{1,j}$ and $(P_b)_{1,k}$. In the j^{th} column of P_d there is precisely one entry 1, say in position $(P_d)_{l,j}$. Thus, we have: $\tau_{1,j} = a$ whence $\tau_{1,j} = z_1 + z_j = 0 + z_j$ and $z_j = a$. Analogously, $\tau_{1,k} = b$ implies $z_k = b$ and $\tau_{l,j} = d$ whence $\tau_{l,j} = z_l + z_j = z_l + a$ and $z_l = d-a$. Therefore, $\tau_{l,k} = z_l + z_k = d-a+b = c$ implies $(P_c)_{l,k} = 1$. Thus, there is a 2×2 submatrix of $\overline{S}$ all of whose entries are 1. Hence $\overline{B}$ is not C_4-free. □

Note that, if we put $B = \tau(\mathcal{G})$ then blowing up B through $(\mathcal{G},+)$ results in a non C_4-free matrix. In the remainder of this section we construct two types of C_4-free matrices using finite fields.

Let $q = p^m$ be a prime power and $(GF(q),+,\cdot)$ be the finite field of order q. Denote by $GF(q)^* := (GF(q)-\{0\},\cdot)$ the multiplicative group of the non-zero elements of $GF(q)$. This group is well known to be cyclic [5, Ch.XIII, sec. 8]. Therefore, a finite field is made up of two abelian groups, namely the elementary abelian additive group $GF(q)^+ := (GF(q),+)$ and the cyclic multiplicative group $(GF(q)^*,\cdot)$. We define $B_* := \tau(GF(q)^*)$ and $B_+ := \tau(GF(q)^+)$, with blank entries substituting the zero entries.

Remark 2.4 *Since the groups* $GF(q)^+$ *and* $GF(q)^*$ *have almost the same set of elements, we will blow up matrices with elements in one group through the other group. We will only encounter the problem that the element* $0 \in GF(q)^+$ *cannot be blown up through* $GF(q)^*$*, since* $0 \notin GF(q)^*$*. In this case, we substitute the* 0 *entry of* $GF(q)^+$ *by a blank entry and in the blow up the blank entry is substituted by a* *block all of whose entries are zero. Since a block all of whose entries are zero cannot contribute to a 2×2 submatrix all of whose entries are 1, Criterion 1 still holds if we admit blank entries in the matrix B.*

Example 2.5 *Let $GF(4)$ be the finite field of order 4 given by the extension $GF(2)(x)$, where x is a root of the irreducible polynomial X^2+X+1 over $GF(2)$. Here $x+1=x^2$, and we write $x^2=\overline{x}$ for short. Hence, $GF(4)=\{0,1,x,\overline{x}\}$. Then B_* and B_+ are the following:*

$$B_* = \begin{pmatrix} 1 & x & \overline{x} \\ x & \overline{x} & 1 \\ \overline{x} & 1 & x \end{pmatrix} \qquad B_+ = \begin{pmatrix} & 1 & x & \overline{x} \\ 1 & & \overline{x} & x \\ x & \overline{x} & & 1 \\ \overline{x} & x & 1 & \end{pmatrix}$$

The permutation matrices of Definition 2.1 coming from B_* are

$$P_1^* = \begin{pmatrix} 1&0&0\\0&0&1\\0&1&0 \end{pmatrix} \qquad P_x^* = \begin{pmatrix} 0&1&0\\1&0&0\\0&0&1 \end{pmatrix} \qquad P_{\overline{x}}^* = \begin{pmatrix} 0&0&1\\0&1&0\\1&0&0 \end{pmatrix},$$

while the permutation matrices of Definition 2.1 coming from B_+ are

$$P_1^+ = \begin{pmatrix} 0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0 \end{pmatrix} \qquad P_x^+ = \begin{pmatrix} 0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0 \end{pmatrix} \qquad P_{\overline{x}}^+ = \begin{pmatrix} 0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0 \end{pmatrix}.$$

Note Since $GF(q)^*$ is multiplicative, verifying Criterion 1 for a blow up through $GF(q)^*$ is equivalent to checking that $a \cdot b^{-1} \cdot c \cdot d^{-1} \neq 1$.

Proposition 2.6

(i) The blow up $\overline{B_*}$ of B_* through $\mathcal{G}_1 = GF(q)^+$ is C_4-free.

(ii) The blow up $\overline{B_+}$ of B_+ through $\mathcal{G}_2 = GF(q)^*$ is C_4-free.

Proof. (i) Consider an arbitrary 2×2 submatrix $S_1 = \begin{pmatrix} \sigma_{i,j} & \sigma_{i,k} \\ \sigma_{l,j} & \sigma_{l,k} \end{pmatrix}$ of B_*. Note that S_1 comes from the multiplication table of $\tau(GF(q)^*)$, hence there exist elements $x_i, x_l, y_j, y_k \in GF(q)^*$ with $x_i \neq x_l$ and $y_j \neq y_k$ such that

$$\sigma_{i,j} = x_i \cdot y_j,\ \sigma_{i,k} = x_i \cdot y_k,\ \sigma_{l,j} = x_l \cdot y_j,\ \sigma_{l,k} = x_l \cdot y_k\,.$$

Thus

$$\sigma_{i,j} - \sigma_{i,k} + \sigma_{l,k} - \sigma_{l,j} = x_i \cdot y_j - x_i \cdot y_k + x_l \cdot y_k - x_l \cdot y_j = (x_i - x_l) \cdot (y_j - y_k) \neq 0.$$

Hence, by Criterion 1 $\overline{B_*}$ is C_4-free.

(ii) Note that, $GF(q)^*$ is multiplicative, hence Criterion 1 becomes $a \cdot b^{-1} \cdot c \cdot d^{-1} \neq 1$. To apply this criterion consider an arbitrary 2×2 submatrix $S_2 = \begin{pmatrix} \sigma_{i,j} & \sigma_{i,k} \\ \sigma_{l,j} & \sigma_{l,k} \end{pmatrix}$ of B_+. If one or two entries of S_2 are blank we are through. Otherwise, note that S_2 comes from the addition table $\tau(GF(q)^{+})$, thus there exist elements $x_i, x_l, y_j, y_k \in GF(q)$ with $x_i \neq x_l$ and $y_j \neq y_k$ such that

$$\sigma_{i,j} = x_i + y_j\,,\ \sigma_{i,k} = x_i + y_k\,,\ \sigma_{l,j} = x_l + y_j\,,\ \sigma_{l,k} = x_l + y_k\,.$$

Hence

$$\sigma_{i,j} \cdot \sigma_{i,k}^{-1} \cdot \sigma_{l,k} \cdot \sigma_{l,j}^{-1} = \frac{x_i x_l + x_i y_k + x_l y_j + y_j y_k}{x_i x_l + x_i y_j + x_l y_k + y_j y_k} \neq 1$$

if and only if

$$x_i y_k + x_l y_j \neq x_i y_j + x_l y_k\,.$$

This, in turn, holds true if and only if

$$(x_i - x_l)(y_j - y_k) \neq 0\,.$$

Hence, by Criterion 1 $\overline{B_+}$ is C_4-free. □

3 The Class $S(\kappa)$

We construct two classes of $(q-\lambda)$-regular bipartite graphs of girth 6, $G_*(q,\lambda)$ and $G_+(q,\lambda)$, from which we build the class $\mathbf{S}(\kappa)$ of κ-regular bipartite graphs of girth 6, for each integer $\kappa \geq 2$ and $\kappa = q - \lambda$, where $q = p^m$ is a prime power, $q \geq 4$, and $0 \leq \lambda \leq q-3$.

To this purpose, we define two variations of B_* and B_+;

$$B_*(q,0) := \left(\begin{array}{ccc|c} & & & 0 \\ & B_* & & \vdots \\ & & & 0 \\ \hline 0 & \cdots & 0 & 0 \end{array}\right) \qquad B_+(q,0) := \left(\begin{array}{ccc|c} & & & 1 \\ & B_+ & & \vdots \\ & & & 1 \\ \hline 1 & \cdots & 1 & \end{array}\right).$$

having orders q and $q+1$, respectively.

Lemma 3.1

(i) The blow up $\overline{B_*}(q,0)$ of $B_*(q,0)$ through $\mathcal{G}_1 = GF(q)^{+}$ is C_4-free matrix of order q^2.

(ii) The blow up $\overline{B_+}(q,0)$ of $B_+(q,0)$ through $\mathcal{G}_2 = GF(q)^{*}$ is C_4-free matrix of order q^2-1.

Proof. The orders follow from Definition 2.2.

(i) It is enough to prove that $B_*(q,0)$ satisfies Criterion 1. For entries coming from the submatrix B_*, the statement follows from the proof of Proposition 2.6(i). Thus, the only remaining 2×2 submatrices to be examined are of types

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\ ,\ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\ \text{and}\ \begin{pmatrix} a & 0 \\ d & 0 \end{pmatrix}$$

for some $a, b, d \in GF(q)^*$. Since a, b and a, d appear in the same row and the same column of a multiplication table $\tau(GF(q)^*)$, respectively, they cannot be equal. Hence, $a \neq 0$, $a - b \neq 0$ and $a - d \neq 0$, i.e. Criterion 1 is satisfied and $\overline{B_*}(q, 0)$ is C_4-free.

(ii) Analogously to (i) but with Criterion 1 applied multiplicatively as in Proposition 2.6(ii). □

Definition 3.2 *We define*

$$A_*(q,0) := \begin{pmatrix} & B_*(q,0) \\ B_*(q,0)^t & \end{pmatrix}, \qquad \overline{A_*}(q,0) := \begin{pmatrix} O & \overline{B_*}(q,0) \\ \overline{B_*}(q,0)^t & O \end{pmatrix},$$

$$A_+(q,0) := \begin{pmatrix} & B_+(q,0) \\ B_+(q,0)^t & \end{pmatrix}, \qquad \overline{A_+}(q,0) := \begin{pmatrix} O & \overline{B_+}(q,0) \\ \overline{B_+}(q,0)^t & O \end{pmatrix}$$

where $\overline{A_*}(q, 0)$ *and* $\overline{A_+}(q, 0)$ *are the* $(0, 1)$*-matrices obtained as the blow up of* $A_*(q, 0)$ *and* $A_+(q, 0)$ *through* $GF(q)^+$ *and* $GF(q)^*$*, respectively. In both cases* O *is a matrix all of whose entries are* 0*, but in the first case it is of order* q^2 *and in the second it is of order* $q^2 - 1$*. Therefore,* $\overline{A_*}(q, 0)$ *and* $\overline{A_+}(q, 0)$ *have order* $2q^2$ *and* $2(q^2 - 1)$ *respectively.*

Theorem 3.3

(i) The $(0, 1)$*-matrices* $\overline{B_*}(q, 0)$ *and* $\overline{B_+}(q, 0)$ *are incidence matrices of partial planes.*

(ii) The $(0, 1)$*-matrices* $\overline{A_*}(q, 0)$ *and* $\overline{A_+}(q, 0)$ *are adjacency matrices of* q*-regular bipartite graphs of girth* 6*, with the exception of* $\overline{A_*}(2, 0)$ *which is an* 8*-cycle* C_8*.*

Proof. (i) The order of the $(0, 1)$-matrix $\overline{B_*}(q, 0)$ is q^2 from Lemma 3.1, in each row and each column there are q entries 1 and, by Lemma 3.1, it is C_4-free. From Lemma 1.1, $\overline{B_*}(q, 0)$ is an incidence matrix for a partial plane with q^2 points and lines such that each point and each line is incident with q distinct lines and points, respectively.

Similarly, $\overline{B_+}(q, 0)$ is an incidence matrix for a partial plane with $q^2 - 1$ points and lines such that each point and each line is incident with q distinct lines and points, respectively.

(ii) From Remark 1.2, the $(0, 1)$-matrices $\overline{A_*}(q, 0)$ and $\overline{A_+}(q, 0)$ are adjacency matrices of q-regular bipartite graphs. Then, the graph with adjacency matrix $\overline{A_*}(q, 0)$ has $2q^2$ vertices while the graph with adjacency matrix $\overline{A_+}(q, 0)$ has $2(q^2 - 1)$ vertices. The matrices are C_4-free, from Lemma 3.1, thus, the girth of these graphs is at least 6. A k-regular graph of girth 8 must have at least $1 + k + k(k-1) + k(k-1)^2 + (k-1)^3 = 2(k^3 - 2k^2 + 2k)$ vertices, see [4, Ch 23, p.180]. Since the number of vertices of the graphs that we have constructed is strictly less than this bound, except for $\overline{A_*}(2, 0)$ which gives an 8-cycle C_8, they must have girth 6. □

Theorem 3.3(ii) allows us to define $\mathbf{G}_*(\mathbf{q}, \mathbf{0})$ and $\mathbf{G}_+(\mathbf{q}, \mathbf{0})$ as the q-regular bipartite graphs of girth 6 having adjacency matrices $\overline{A_*}(q, 0)$ and $\overline{A_+}(q, 0)$, respectively.

Example 3.4 *Let $GF(4)$ be the finite field of order 4. Then, we have*

$$B_*(4,0) = \begin{pmatrix} 1 & x & \overline{x} & 0 \\ x & \overline{x} & 1 & 0 \\ \overline{x} & 1 & x & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \qquad B_+(4,0) = \begin{pmatrix} & 1 & x & \overline{x} & 1 \\ 1 & & \overline{x} & x & 1 \\ x & \overline{x} & & 1 & 1 \\ \overline{x} & x & 1 & & 1 \\ 1 & 1 & 1 & 1 & \end{pmatrix},$$

$$A_*(4,0) := \begin{pmatrix} & \begin{smallmatrix} 1 & x & \overline{x} & 0 \\ x & \overline{x} & 1 & 0 \\ \overline{x} & 1 & x & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix} \\ \begin{smallmatrix} 1 & x & \overline{x} & 0 \\ x & \overline{x} & 1 & 0 \\ \overline{x} & 1 & x & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix} & \end{pmatrix}, \quad A_+(4,0) := \begin{pmatrix} & \begin{smallmatrix} & 1 & x & \overline{x} & 1 \\ 1 & & \overline{x} & x & 1 \\ x & \overline{x} & & 1 & 1 \\ \overline{x} & x & 1 & & 1 \\ 1 & 1 & 1 & 1 & \end{smallmatrix} \\ \begin{smallmatrix} & 1 & x & \overline{x} & 1 \\ 1 & & \overline{x} & x & 1 \\ x & \overline{x} & & 1 & 1 \\ \overline{x} & x & 1 & & 1 \\ 1 & 1 & 1 & 1 & \end{smallmatrix} & \end{pmatrix}.$$

The adjacency matrices of the graphs $G_*(4,0)$ and $G_+(4,0)$ are obtained by blowing up $A_*(4,0)$ and $A_+(4,0)$ through $GF(4)^+$ and $GF(4)^*$, respectively, using the permutation matrices from Example 2.5.

They are 4-regular bipartite graphs with girth 6, the former with 32 vertices and the latter with 30 vertices. Note that, they both have order greater than the $(4,6)$-cage, namely $\Gamma(PG(2,3))$ on 26 vertices.

CONSTRUCTION. We construct two classes $G_*(q,\lambda)$ and $G_+(q,\lambda)$ from the graphs $G_*(q,0)$ and $G_+(q,0)$ as follows.

(i) Let $B_*(q,\lambda)$ and $B_+(q,\lambda)$, for $\lambda = 0,\dots,q-3$, be the *principal minors* obtained by deleting the last λ rows and columns from $B_*(q,0)$ and $B_+(q,0)$.

The corresponding blow up $\overline{B_*}(q,\lambda)$ and $\overline{B_+}(q,\lambda)$ could be equivalently obtained by deleting the last λ rows and columns of blocks from $\overline{B_*}(q,0)$ and $\overline{B_+}(q,0)$.

(ii) Similarly to Definition 3.2, we define $A_*(q,\lambda) := \begin{pmatrix} & B_*(q,\lambda) \\ B_*(q,\lambda)^t & \end{pmatrix}$, $A_+(q,\lambda)$, $\overline{A_*}(q,\lambda)$ and $\overline{A_+}(q,\lambda)$.

Note that, $\overline{A_*}(q,\lambda)$ and $\overline{A_+}(q,\lambda)$ are adjacency matrices of graphs since they are symmetric and the main diagonal has all entries zero.

Definition 3.5 *We define $G_*(q,\lambda)$ the class of graphs having adjacency matrix $\overline{A_*}(q,\lambda)$ and $G_+(q,\lambda)$ the class of graphs with adjacency matrix $\overline{A_+}(q,\lambda)$, for $\lambda = 0,\dots,q-3$.*

Theorem 3.6 *The graphs of the classes $G_*(q,\lambda)$ and $G_+(q,\lambda)$ are $(q-\lambda)$-regular bipartite of girth 6, for $q \geq 4$ and $\lambda = 0,1,\dots,q-3$.*

Proof. A simple counting of the number of entries 1 in each row and column of $\overline{A_*}(q,\lambda)$ and $\overline{A_+}(q,\lambda)$ proves that the corresponding graphs are $(q-\lambda)$-regular. They are bipartite, by Remark 1.2.

For $q \geq 4$, fix a labeling for the elements of $GF(q)$ as follows:

$$GF(q) = \{z_1 = 0, z_2 = 1, z_3 = x, z_4 = y, \dots, z_q\}.$$

Then, the principal minor of order 3 in $B_+(q,\lambda)$ is $M := \begin{pmatrix} & 1 & x \\ 1 & 1+1 & 1+x \\ x & 1+x & x+x \end{pmatrix}$.

In the blow up $\overline{B}_+(q,\lambda)$ of $B_+(q,\lambda)$ through $GF(q)^*$, M becomes

$$\overline{M} := \begin{pmatrix} O & P_1^* & P_x^* \\ P_1^* & P_{1+1}^* & P_{1+x}^* \\ P_x^* & P_{1+x}^* & P_{x+x}^* \end{pmatrix}.$$

In characteristic two $1+1 = x+x = 0$, thus $P_{1+1}^* = P_{x+x}^* = O$ in $\overline{M}$.
Let i,j,k,l be indices such that $z_i = 1{+}x$, $z_j = x{\cdot}z_i^{-1}$, $z_k = 1{\cdot}z_j^{-1}$ and $z_l = (1{+}x){\cdot}z_k^{-1}$. Then, $z_l = (1+x)\cdot x\cdot(1+x)^{-1} = x$. Thus, $(P_1^*)_{1,1} = (P_{1+x}^*)_{i,1} = (P_x^*)_{i,j} = (P_1^*)_{k,j} = (P_{1+x}^*)_{k,l} = (P_x^*)_{1,l} = 1$. Hence, there is a hexagon in $\overline{A_+}(q,\lambda)$.

Similarly, the principal minor of order 3 in $B_*(q,\lambda)$ is $M' := \begin{pmatrix} 1 & x & y \\ x & x^2 & x{\cdot}y \\ y & x{\cdot}y & y^2 \end{pmatrix}$.

In the blow up $\overline{B}_*(q,\lambda)$ of $B_*(q,\lambda)$ through $GF(q)^+$, M' becomes

$$\overline{M}' := \begin{pmatrix} P_1^+ & P_x^+ & P_y^+ \\ P_x^+ & P_{x^2}^+ & P_{x\cdot y}^+ \\ P_y^+ & P_{x\cdot y}^+ & P_{y^2}^+ \end{pmatrix}.$$

Let i,j,k,l be indices such that $z_i = x{\cdot}y - x$, $z_j = y - z_i$, $z_k = x - z_j$ and $z_l = x{\cdot}y - z_k$. Then, $z_l = x\cdot y - x + y - (x\cdot y) + x = y$. Therefore, $(P_x^+)_{1,3} = (P_{x\cdot y}^+)_{i,3} = (P_y^+)_{i,j} = (P_x^+)_{k,j} = (P_{x\cdot y}^+)_{k,l} = (P_y^+)_{1,l} = 1$, which produces a hexagon in $\overline{A_*}(q,\lambda)$. □

Remark 3.7 *(i) The number of vertices of a graph in the class* $G_*(q,\lambda)$ *is* $2q(q-\lambda) = 2(q^2-\lambda q)$, *while the number of vertices of a graph in the class* $G_+(q,\lambda)$ *is* $2(q+1-\lambda)(q-1) = 2(q^2-\lambda q+\lambda-1)$.

(ii) For $\lambda = 0$, *the number of vertices of a graph in the class* $G_+(q,0)$ *is strictly smaller than the number of vertices of* $G_*(q,0)$. *For* $\lambda = 1$, *they have the same number of vertices and we conjecture that they are isomorphic. For* $\lambda \geq 2$, *the number of vertices of* $G_*(q,0)$ *is strictly smaller than the number of vertices of* $G_+(q,0)$.

Definition 3.8 *Let* κ *be a positive integer and let* $q = p^m$, $m \geq 1$ *and* $q \geq 4$, *be the closest prime power greater or equal to* κ. *Let* $\lambda = q-\kappa$, $\lambda \geq 0$. *We define the class* $\mathbf{S}(\kappa)$ *of* κ*-regular bipartite graphs of girth* 6 *as follows*

$$S(\kappa) := \begin{cases} G_+(q,\lambda) & \text{if} \quad \lambda \leq 1 \\ G_*(q,\lambda) & \text{if} \quad \lambda \geq 2 \end{cases}$$

Remark 3.9 *(i) The two classes* $G_+(q,\lambda)$ *and* $G_*(q,\lambda)$ *are defined for* $\lambda = 0,\dots,q-3$. *Thus, the class* $S(k)$ *is well defined since it is easy to check that* $\lambda \leq \lfloor q/2 \rfloor \leq q-3$.

(ii) The graphs in $S(\kappa)$ *are sometimes* minimal *in the sense that they have the smallest number of vertices known so far among the* κ*-regular graphs of girth* 6. *In particular, the graph* $S(11)$ *is an* 11*-regular graph on* 240 *vertices which has the same order of a graph due to Wong [17], while e.g.* $S(13)$ *yields a new* 13*-regular graph of girth* 6 *on* 336 *vertices.*

(iii) The graphs in $S(\kappa)$ such that $\kappa - 1$ is not a prime power, $14 \leq \kappa \leq 40$ are listed in the following table:

κ	graph	order	κ	graph	order
15	$G_+(16,1)$	480	29	$G_+(29,0)$	1680
16	$G_+(16,0)$	510	31	$G_+(31,0)$	1920
19	$G_+(19,0)$	720	34	$G_*(37,3)$	2516
21	$G_*(23,2)$	966	35	$G_*(37,2)$	2590
22	$G_+(23,1)$	1012	36	$G_+(37,1)$	2664
23	$G_+(23,0)$	1056	37	$G_+(37,0)$	2736
25	$G_+(25,0)$	1248	39	$G_*(41,2)$	3198
27	$G_+(27,0)$	1456	40	$G_+(41,1)$	3280

Note that they are candidates to be $(\kappa, 6)$-cages as described in the table by G. Royle [15]. We consider only those values of κ where $\kappa - 1$ is not a prime power since the incidence graph of the projective plane $PG(2, \kappa - 1)$ is already known to be a $(\kappa, 6)$-cage (cf. Section 1).

4 The Class $S(q^2, \lambda)$

In this section, we construct a 15- and a 16-regular graph of girth 6 with less vertices than $S(15)$ and $S(16)$, respectively. We conjecture that this construction can be extended for all prime powers $\kappa = q^2 = p^{2m}$, p prime and $m \geq 1$.

For each $r \geq 3$, a subset $\Delta = \{z_0, \ldots, z_{\kappa-1}\} \subseteq \mathbb{Z}_r$ is called a **difference set modulo** r if the $\kappa^2 - \kappa$ differences

$$\delta_{i,j} :\equiv s_i - s_j \pmod r$$

are pairwise distinct for $i, j = 0, \ldots, \kappa - 1$ with $i \neq j$. If $r = \kappa^2 - \kappa + 1$, then Δ is called **perfect** [3].

A **circulant matrix** $C =< c_0, \ldots, c_{r-1} >$ of order r is defined as follows:

$$C = \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_{r-2} & c_{r-1} \\ c_{r-1} & c_0 & c_1 & \cdots & c_{r-3} & c_{r-2} \\ c_{r-2} & c_{r-1} & c_0 & \cdots & c_{r-4} & c_{r-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c_2 & c_3 & c_4 & \cdots & c_0 & c_1 \\ c_1 & c_2 & c_3 & \cdots & c_{r-1} & c_0 \end{pmatrix}.$$

In particular, C is a **circulant** $(0,1)$-**matrix** if $c_0, c_1, \ldots, c_{r-1} \in \{0, 1\}$ [7].

There is a 1–1 correspondence between circulant $(0,1)$-matrices of order r and subsets of $\mathbb{Z}_r$ such that

$$C = < c_0, \ldots, c_{r-1} > \longmapsto \Delta_C := \{i \in \{0, \ldots, r-1\} \mid c_i = 1\}.$$

Lemma 4.1 [13] *Let* $C = < c_0, \dots, c_{r-1} >$ *be a circulant* $(0,1)$*-matrix. Then* C *is* C_4*-free if and only if* Δ_C *is a difference set modulo* r.

Instances of perfect difference sets are $\{0,1,3\}$ modulo 7 and $\{0,1,4,6\}$ modulo 13, which represent incidence matrices for $PG(2,2)$ and $PG(2,3)$, respectively. We give a generalization of Definition 2.2 using difference sets as entries of a matrix in analogy to [9].

Definition 4.2 *Fix a labeling of* $\mathbb{Z}_r = \{0,1,\dots,r-1\}$. *Let* $\Delta = \{z_0, \dots, z_{\kappa-1}\}$ *be a difference set modulo* r *and let* $B^{(r)} = (b_{i,j})^{(r)}$ *be a square matrix of order* s *such that*

$$b_{i,j} = \begin{cases} \Delta & \text{if } i = j \\ z \in \mathbb{Z}_r & \text{if } i \neq j \end{cases}$$

for all $i,j = 1,\dots,s$, *where* Δ *is considered as a symbol. We define the* **Delta-blow up** $\overline{B}$ **of** B **through the group** $(\mathbb{Z}_r,+)$ *in the following way:* $\overline{B}$ *is the block matrix of order* s *having square blocks* $\overline{B}_{i,j}$ *of order* r *such that for all* $i,j = 1,\dots,s$, *we have*

$$\overline{B}_{i,j} = \begin{cases} P_z & \text{if } b_{i,j} = z \in \mathbb{Z}_r \\ P_{z_0} + \dots + P_{z_{\kappa-1}} & \text{if } b_{i,i} = \Delta \end{cases}$$

Hence, $\overline{B}$ *is a* $(0,1)$*-matrix of order* rs.

Remark 4.3 *(i) The exponent* (r) *of the matrix* $B^{(r)}$ *in the above definition underlines that the operations are in* $\mathbb{Z}_r$.

(ii) In the Δ*-blow up* $\overline{B}$ *of* B, *the* $(0,1)$*-block* $P_{z_0} + \dots + P_{z_{\kappa-1}}$ *is the circulant matrix associated to the difference set* Δ *in the bijection above.*

(iii) Criterion 1 *still holds true for* $B^{(r)}$ *as has been proved in [9, Theorem 5.5].*

Each finite Desarguesian projective plane $PG(2,q^2)$ can be partitioned into copies of Baer subplanes $PG(2,q)$, for details see e.g. [11]. By a famous result due to J. Singer [16], *any finite projective plane* $PG(2,q)$ *admits a circulant* $(0,1)$*-matrix* $C(q)$ *as its incidence matrix, such that*

$$\Delta_{C(q)} := \{ i \in \{0,\dots,q-1\} \mid c_i = 1 \}$$

is a perfect difference set.

Let $r := q^2+q+1$ and $\theta(q) := \dfrac{q^4+q^2+1}{q^2+q+1} = q^2-q+1$. Then, the incidence matrix of $PG(2,q^2)$ can be written as a $(0,1)$-block matrix $(I^{(q^2)}_{i,j})_{i,j=1,\dots,\theta(q)}$ such that the blocks $I^{(q^2)}_{i,i}$ in the main diagonal are copies of $C(q)$ and the blocks $I^{(q^2)}_{i,j}$, $i \neq j$, off the main diagonal are permutation matrices of order r.

Conjecture 4.4 *There exist elements* $z_{i,j} \in \mathbb{Z}_r$, *for* $i,j = 1,\dots,\theta(q)$, $i \neq j$ *such that the* Δ*-blow up* $\overline{I}(q^2,0)$ *of*

$$I(q^2,0) := \begin{pmatrix} \Delta_{C(q)} & z_{1,2} & \dots & z_{1,\theta(q)} \\ z_{2,1} & \Delta_{C(q)} & \dots & z_{2,\theta(q)} \\ \vdots & \vdots & \ddots & \vdots \\ z_{\theta(q),1} & z_{\theta(q),2} & \dots & \Delta_{C(q)} \end{pmatrix}$$

through the group $(\mathbb{Z}_r,+)$ is an incidence matrix of $PG(2,q^2)$ of the form $(I_{i,j}^{(q^2)})_{i,j=1,\dots,\theta(q)}$ and $z_{i,j}$ must be such that the matrix $I(q^2,\lambda)$ satisfies Criterion 1.

Remark 4.5 *The values for which the conjecture is true allow to construct a new family of graphs $S(q^2,\lambda)$, for $\lambda=0,\dots,\theta(q)-1$, analogously to the construction made in the Section 3. The graphs $G'(q^2,\lambda)$ in $S(q^2,\lambda)$ have adjacency matrix*

$$\overline{J}(q^2,\lambda) \quad = \quad \begin{pmatrix} O & \overline{I}(q^2,\lambda) \\ \overline{I}(q^2,\lambda)^t & O \end{pmatrix},$$

where $\overline{I}(q^2,\lambda)$ is the matrix obtained from $\overline{I}(q^2,0)$ deleting the last λ rows and columns of blocks (i.e. it is the principal minor of order $r(\theta(q)-\lambda)$). Note that, the graph $G'(q^2,0)$ is the incidence graph $\Gamma(PG(2,q^2))$, thus it is (q^2+1)-regular bipartite of girth 6 with $2(q^4+q^2+1)$ vertices [8]. Hence, the graphs $G'(q^2,\lambda)$ are $(q^2+1-\lambda)$-regular bipartite with $2[q^4+q^2+1-\lambda(q^2+q+1)]$. The girth of these graphs is 6 since, for $\lambda=0,\dots,\theta(q)-1$, their adjacency matrix is still C_4-free and, they always contain as a subgraph the incidence graph $\Gamma(PG(2,q))$ which contains a hexagon.

Example 4.6 *The conjecture holds true for $q=2,3,4$. In particular, for $q=4$, $PG(2,4)$ admits a circulant incidence matrix $C(4)$ such that $\Delta_{C(4)}=\{0,1,4,14,16\}$ modulo 21 is a perfect different set. The matrix $I(16,0)=$*

$$\begin{pmatrix}
\Delta_{C(4)} & 3 & 20 & 6 & 12 & 17 & 5 & 5 & 17 & 12 & 6 & 20 & 3 \\
3 & \Delta_{C(4)} & 3 & 20 & 6 & 12 & 17 & 5 & 5 & 17 & 12 & 6 & 20 \\
20 & 3 & \Delta_{C(4)} & 3 & 20 & 6 & 12 & 17 & 5 & 5 & 17 & 12 & 6 \\
6 & 20 & 3 & \Delta_{C(4)} & 3 & 20 & 6 & 12 & 17 & 5 & 5 & 17 & 12 \\
12 & 6 & 20 & 3 & \Delta_{C(4)} & 3 & 20 & 6 & 12 & 17 & 5 & 5 & 17 \\
17 & 12 & 6 & 20 & 3 & \Delta_{C(4)} & 3 & 20 & 6 & 12 & 17 & 5 & 5 \\
5 & 17 & 12 & 6 & 20 & 3 & \Delta_{C(4)} & 3 & 20 & 6 & 12 & 17 & 5 \\
5 & 5 & 17 & 12 & 6 & 20 & 3 & \Delta_{C(4)} & 3 & 20 & 6 & 12 & 17 \\
17 & 5 & 5 & 17 & 12 & 6 & 20 & 3 & \Delta_{C(4)} & 3 & 20 & 6 & 12 \\
12 & 17 & 5 & 5 & 17 & 12 & 6 & 20 & 3 & \Delta_{C(4)} & 3 & 20 & 6 \\
6 & 12 & 17 & 5 & 5 & 17 & 12 & 6 & 20 & 3 & \Delta_{C(4)} & 3 & 20 \\
20 & 6 & 12 & 17 & 5 & 5 & 17 & 12 & 6 & 20 & 3 & \Delta_{C(4)} & 3 \\
3 & 20 & 6 & 12 & 17 & 5 & 5 & 17 & 12 & 6 & 20 & 3 & \Delta_{C(4)}
\end{pmatrix}^{(21)},$$

gives rise to the incidence matrix $\overline{I}(16,0)$ of $PG(2,16)$. Thus, the incidence graph $\Gamma(PG(2,16))$ has adjacency matrix $\overline{J}(16,0)$ (c.f. Remark 4.5).

The graph $G'(16,0)$ is 17-regular bipartite graphs of girth 6 having 546 vertices, i.e. it is the $(17,6)$-cage. The graphs $G'(16,1)$ and $G'(16,2)$ in $S(16,\lambda)$ are a 16- and a 15-regular bipartite graph of girth 6 of order 504 and 462, respectively. In both cases, $G'(16,1)$ and $G'(16,2)$ have smaller order than the graphs $S(16)$ and $S(15)$, respectively.

5 Conclusion

The table below indicates an update state of knowledge on (minimal) κ-regular graphs of girth 6, for $3 \leq \kappa \leq 16$ analogously to G. Royle [15]. For each valency, we have listed κ-regular graphs of girth 6 indicating the corresponding graph or the references where such graphs can be found. The graphs which are also $(\kappa, 6)$-cages have the order preceded by an "=" sign.

κ	order	graph	κ	order	graph
3	= 14	$\Gamma(PG(2,2))$	10	= 182	$\Gamma(PG(2,9))$
4	= 26	$\Gamma(PG(2,3))$	11	240	[17], $\mathbf{G(11,0)}$
5	= 21	$\Gamma(PG(2,4))$	12	= 264	$\Gamma(PG(2,11))$
6	= 62	$\Gamma(PG(2,5))$	13	336	$\mathbf{G(13,0)}$
7	= 90	[1, 2, 14]	14	= 366	$\Gamma(PG(2,13))$
8	= 114	$\Gamma(PG(2,7))$	15	462	$\mathbf{G'(16,2)}$
9	= 146	$\Gamma(PG(2,8))$	16	504	$\mathbf{G'(16,1)}$

The two classes $S(\kappa)$ and $S(q^2, \lambda)$ give new instances for the above table indicated in bold face. Furthermore, for $\kappa \geq 17$ the class $S(\kappa)$ furnishes many more new instances.

Acknowledgement

The authors wish to thank the referees for their valuable suggestions.

References

[1] R.D. Baker, An Elliptic Semiplane, *J. Combin. Theory, Ser. A* 25 (1978), 193–195.

[2] R.D. Baker, Elliptic Semi-planes I : Existence and Classification, in: *Proc. 8th Conf. Combinatorics, Graph Theory and Computing*, Baton Rouge 1977, *Congressus Numer.* 19 (1977), 61–73.

[3] L.D. Baumert, *Cyclic difference sets*, Springer-Verlag, Berlin – Heidelberg – New York, 1971.

[4] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, Cambridge, 1993.

[5] G. Birkhoff and S. Mac Lane, *Algebra (3rd edition)*, AMS Chelsea Publishing, Providence, 1999.

[6] J.A. Bondy and U.S.R. Murty, *Graph Theory with Applications*, Elsevier, North Holland, New York 1976.

[7] P. J. Davis, *Circulant matrices*, Chelsea Publ., New York 1994.

[8] P. Dembowski, *Finite geometries*, Springer, Berlin Heiderlberg New York 1997.

[9] M. Funk, D. Labbate and V. Napolitano, Tactical decompositions of symmetric configurations, (submitted).

[10] M. Hall, Projective Planes, *Trans. Am. Math. Soc.* 54 (1943), 229–277.

[11] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields* (2^{nd} ed.), Clarendon Press, Oxford 1998.

[12] N. Jacobson, *Basic Algebra I (2^{nd} ed.)*, Freeman and Co., New York 1985.

[13] M. J. Lipman, The existence of small tactical configurations, in: *Graphs and Combinatorics*, Springer Lecture Notes in Mathematics 406 (1974), 319–324.

[14] M. O'Keefe and P. K. Wong, The smallest graph of girth 6 and valency 7, *J. Graph Theory* 5 (1981), 79–85.

[15] G. Royle, Cages of Higher Valency, `http://www.csse.uwa.edu.au/~gordon/cages/allcages.html`, last update Feb. 2004.

[16] J. Singer, A Theorem in Finite Projective Geometry and Some Applications to Number Theory, *Trans. Amer. Math. Soc.* 43 (1938), 377–385.

[17] P. K. Wong, A regular graph of girth 6 and valency 11, *Internat. J. Math. Math. Sci.* 9 (1986), 561–565.

(Received 25 Nov 2004)