Computers and Mathematics with Applications 62 (2011) 2472–2479

Contents lists available at SciVerse ScienceDirect

Computers and Mathematics with Applications

journal homepage: www.elsevier.com/locate/camwa

New graphs related to $(p, 6)$ and $(p, 8)$-cages

Alain Bretto [a,*], Alain Faisant [b], Luc Gillibert [a]

[a] Université de Caen, GREYC CNRS UMR-6072, Campus 2, Bd Marechal Juin BP 5186, 14032 Caen cedex, France

[b] Université Jean Monnet LAMUSE 23 rue Paul Michelon, 42023 Saint-Etienne cedex 2, France

ARTICLE INFO

Article history:
Received 21 February 2011
Received in revised form 14 July 2011
Accepted 14 July 2011

Keywords:
Algorithms
Algebraic computation
Computational group theory
Cage graph problem

ABSTRACT

Constructing regular graphs with a given girth, a given degree and the fewest possible vertices is hard. This problem is called the cage graph problem and has some links with the error code theory. G-graphs can be used in many applications: symmetric and semi-symmetric graph constructions, (Bretto and Gillibert (2008) [12]), hamiltonicity of Cayley graphs, and so on. In this paper, we show that G-graphs can be a good tool to construct some upper bounds for the cage problem. For p odd prime we construct $(p, 6)$-graphs which are G-graphs with orders $2p^2$ and $2p^2 - 2$, when the Sauer bound is equal to $4(p-1)^3$. We construct also $(p, 8)$-G-graphs with orders $2p^3$ and $2p^3 - 2p$, while the Sauer upper bound is equal to $4(p-1)^5$.

1. Preliminaries

The problem of cages has been introduced by Tutte in 1947 [1]. It is an important part of both extremal graph theory and algebraic graph theory. So this topic has been widely studied and some interesting applications to computer science have been developed, [2–9]. There exist both an upper bound (Sauer bound) and a lower bound (Moore bound) for the problem of cages but these bounds are actually rarely reached. Consequently there is no general method to construct arbitrary cages. In this paper, we construct several infinite families of G-graphs with a girth of 6 or 8 and regular of degree p, for any odd prime number p. For families the best upper bound known so far is given for both the $(p, 6)$-cage problem and the $(p, 8)$-cage problem. Some other families give us a best new upper bound.

Let $\Gamma = (V; E)$ be a simple graph, (without loop or multiple edge). A chain is a sequence $(\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{k-1}, v_k\})$.

A cycle C is a chain such that $v_1 = v_k$ and all edges are distinct.

An elementary cycle is a chain such that $v_1 = v_k$ and all vertices are distinct except the first one and the last one.

So any cycle contains an elementary cycle.

The G-graphs have been introduced in [10] to study the isomorphism problem. Their properties have been studied in [11,12]. Some applications of these graphs to symmetric and semi-symmetric graph-construction have been developed in [13]. Here we reminded the reader the construction of this type of graph. We denote by (G, S) a finite group G with a subset S. For any $s \in S$, we consider the right action of G on the right cosets Hx of the subgroup $H = \langle s \rangle$.

Thus we have a partition $G = \bigsqcup_{x \in T_s} \langle s \rangle x$, where T_s is a right transversal of $\langle s \rangle$. The cardinality of $\langle s \rangle$ is $o(s)$, the order of the element s. Let us consider the cycles $(s)x = (x, sx, s^2x, \ldots, s^{o(s)-1}x)$ of the permutation $g_s : x \longmapsto sx$. Notice that $\langle s \rangle x$ is the support of the cycle $(s)x$. We now define a graph denoted by $\Phi(G; S) = (V; E)$ as follows:

- The vertices of $\Phi(G; S)$ are the cycles of g_s, $s \in S$: $V = \sqcup_{s \in S} V_s$ with $V_s = \{(s)x, x \in T_s\}$.
- For $(s)x$, $(t)y \in V$, $\{(s)x, (t)y\}$ is an n-edge if $|\langle s \rangle x \cap \langle t \rangle y| = n,\ n \geq 1$.

* Corresponding author.
E-mail addresses: alain.bretto@info.unicaen.fr (A. Bretto), faisant@univ-st-etienne.fr (A. Faisant), luc.gillibert@info.unicaen.fr (L. Gillibert).

0898-1221/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2011.07.033

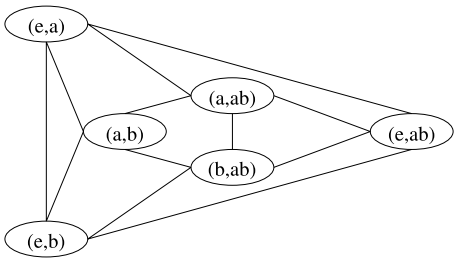


Fig. 1. The octahedral graph.

Thus, $\Phi(G;S)$ is a k-partite graph and any vertex has an $o(s)$-loop. We denote by $\widetilde{\Phi}(G;S)$ the graph $\Phi(G;S)$ without loops and multi-edges.

Both graphs $\Phi(G;S)$ and $\widetilde{\Phi}(G;S)$ are called *G-graphs*, and we say that the graph is *associated* by the group $(G;S)$.

An example of a G-graph construction is given below.

Let G be the KLEIN group, the product of two cyclic groups of order 2. So $G=\{e,a,b,ab\}$ with $o(a)=2$, $o(b)=2$ and $ab=ba$. The set $S=\{a,b,ab\}$ is a family of generators of G. Let us compute the graph $\widetilde{\Phi}(G;S)$.

The cycles of the permutation g_a are:

$$(a)e=(e,ae)=(e,a)$$
$$(a)b=(b,ab).$$

The cycles of the permutation g_b are:

$$(b)e=(e,be)=(e,b)$$
$$(b)a=(a,ba)=(a,ab).$$

The cycles of the permutation g_{ab} are:

$$(ab)e=(e,abe)=(e,ab)$$
$$(ab)a=(a,aba)=(a,b).$$

The graph $\widetilde{\Phi}(G;S)$ is isomorphic to the octahedral graph (see Fig. 1). The octahedral graph is a 3-partite symmetric quartic graph.

2. Properties of G-graphs

The two following results can be found in [11,12].

Proposition 2.1. *If $\langle s_1\rangle\cap\langle s_2\rangle=1$, then the G-graph $\Phi(G;\{s_1,s_2\})$ has just loops as multi-edges.*

Proposition 2.2. *Let $\Phi(G;S)=(V;E)$ be a G-graph. This graph is connected if and only if S is a set of generators of G.*

Proposition 2.3. *Let $(G;\{s_1,s_2\})$ be a group with $\langle s_1\rangle\cap\langle s_2\rangle=1$ and let $\widetilde{\Phi}(G;\{s_1,s_2\})$ be its associated simple G-graph. Each elementary cycle of length $2n$ in $\widetilde{\Phi}(G;\{s_1,s_2\})$ stands for a relation*

$$s_2^{l_n}s_1^{k_n}\dots s_2^{l_1}s_1^{k_1}=1 \tag{1}$$

with $0<k_1,k_2,\dots,k_n<o(s_1)$ and $0<l_1,l_2,\dots,l_n<o(s_2)$.

Proof. We first fix two right transversals T_{s_1} and T_{s_2} of $\langle s_1\rangle$ and $\langle s_2\rangle$ and reminded the reader that every $g\in G$ can be written in a unique way: $g=s_1^ix,\ 0\le i<o(s_1),\ x\in T_{s_1}$ and in a unique way: $g=s_2^jx,\ 0\le j<o(s_2),\ x\in T_{s_2}$.

(a) Let us consider an elementary cycle $C=(\{v_1,v_2\},\{v_2,v_3\},\dots,\{v_{2n},v_1\})$ of length $2n$ (the graph is bipartite). We can suppose $v_1\in V_{g_{s_1}}$ and so $v_2\in V_{g_{s_2}}$. There is an element which is both in $\langle s_1\rangle x_1$ and in $\langle s_2\rangle x_2$ ($x_1\in T_{s_1}$, $x_2\in T_{s_2}$). So there are h and j_2 such that

$$s_2^{j_2}x_2=s_1^hx_1.$$

There is also an element which is both in $\langle s_2\rangle x_2$ and in $\langle s_1\rangle x_3$, $(x_3\in T_{s_1})$ with $x_1\ne x_3$ because $v_3\ne v_1$ by hypothesis.

$$s_1^{j_3}x_3=s_2^{i_2}x_2=s_2^{i_2-j_2}s_2^{j_2}x_2=s_2^{i_2-j_2}s_1^hx_1=:s_2^{l_1}s_1^hx_1.$$

If $l_1\equiv 0 \bmod o(s_2)$, then $s_1^{j_3}x_3=s_1^hx_1$, $x_1=x_3$ and $v_1=v_3$. So $l_1\not\equiv 0 \bmod o(s_2)$.
There exist i_3,j_4 such that

$$s_2^{j_4}x_4=s_1^{i_3}x_3=s_1^{i_3-j_3}s_1^{j_3}x_3=s_1^{i_3-j_3}s_2^{l_1}s_1^hx_1=:s_1^{k_2}s_2^{l_1}s_1^hx_1.$$

We have $k_2 \not\equiv 0 \bmod o(s_1)$ (otherwise, we would have $s_2^{j_4}x_4 = s_2^{l_1}s_1^h x_1 = s_2^{l_1}s_2^{j_2}x_2$, which implies $x_4 = x_2$ and $v_4 = v_2$). We continue the process up to:

$$s_1^{j_{2n+1}}x_{2n+1} = s_2^{i_2 n}x_{2n} = s_2^{l_n}s_1^{k_n}\ldots s_2^{l_1}s_1^h x_1$$

with $l_n \not\equiv 0 \bmod o(s_2)$; $x_{2n+1} = x_1$ implies:

$$s_2^{l_n}s_1^{k_n}\ldots s_2^{l_1}s_1^{h-j_{2n+1}} = 1.$$

Finally we have $k_1 := h - j_{2n+1} \not\equiv 0 \bmod o(s_1)$. Assume that this is not the case: $s_2^{j_2}x_2 = s_1^h x_1 = s_1^{j_{2n+1}}x_{2n+1} = s_2^{i_{2n}}x_{2n}$. If $x_{2n} \neq x_2$, then there is an edge between $(s_2)x_2$ and $(s_2)x_{2n}$, which is impossible by construction. So $x_{2n} = x_2$, which leads to $v_{2n} = (s_2)x_{2n} = (s_2)x_2 = v_2$. But by hypothesis the cycle is elementary, a contradiction. □

3. The cage graph problem

The results of this section can be found in [2,14,3,5,15,7,16,17,9]. The *girth* is the length of the shortest graph cycle in a simple graph. Acyclic graphs are considered to have infinite girth. A (k, g)-*graph*, with $g \geq 3$, is a k-regular graph of girth g. The graph $\Gamma = (V; E)$ is a (k, g)-*cage* if Γ is a (k, g)-graph with $|V|$ minimum; we denote this minimum by $\mathrm{cage}(k, g)$. There are two problems.

1. calculation of the $\mathrm{cage}(k, g)$,
2. determination of all the (k, g)-cages.

There are special cases.

- $\mathrm{cage}(k, 3) = k + 1$, and the $(k, 3)$-cage are the complete graphs K_{k+1}.
- $\mathrm{cage}(k, 4) = 2k$, and the $(k, 4)$-cage are the complete bipartite graphs $K_{k,k}$.

The best lower bounds known for $\mathrm{cage}(v, g)$ are the *Moore bounds*.

$$\mathrm{cage}(k, g) \geq \mathrm{Moore}(k, g) = \begin{cases} 1 + k \displaystyle\sum_{0 \leq i \leq \frac{g-3}{2}} (k-1)^i & \text{if } g \text{ is odd} \\ 1 + k \displaystyle\sum_{0 \leq i \leq \frac{g-4}{2}} (k-1)^i + (k-1)^{\frac{g-2}{2}} & \text{if } g \text{ is even.} \end{cases}$$

A (k, g)-graph $\Gamma = (V; E)$ is a *Moore-graph* if $|V| = \mathrm{Moore}(k, g)$; if it exists, we have $\mathrm{cage}(k, g) = \mathrm{Moore}(k, g)$.

- For $g = 5$, a (k, g)-Moore-graph exists only if $k = 3, 7$ or 57.
  - The Petersen graph is a $(3, 5)$-Moore-graph: $\mathrm{cage}(3, 5) = 10$.
  - The Hoffman–Singleton graph is a $(7, 5)$-Moore-graph: $\mathrm{cage}(7, 5) = 50$.
  - No example of $(57, 5)$-Moore-graph is known.
- For $g = 6$,
  - The incidence graph of $PG(2, p^n)$ (which is a finite projective plane with p prime and $n \geq 1$) is a $(p^n + 1, 6)$-Moore-graph; so for $k = p^n + 1$, we have $\mathrm{cage}(k, 6) = \mathrm{Moore}(k, 6) = 2k^2 - 2k + 2$.
  - The Heawood graph is a $(3, 6)$-Moore-graph: $\mathrm{cage}(3, 6) = 14$. It is the incidence graph of $PG(2, 2)$.
  - The Wong graph is a $(4, 6)$-Moore-graph: $\mathrm{cage}(4, 6) = 26$. It is the incidence graph of $PG(2, 3)$.
  - What happens when $k - 1$ is not a prime power is not known.
- For $g = 7$, there exists no $(k, 7)$-Moore-graph. Hence $\mathrm{cage}(k, 7) > \mathrm{Moore}(k, 7)$.
- For $g = 8$, the generalized quadrangle is a $(p^n + 1, 8)$-Moore-graph; for $k = p^n + 1$, p prime, we have $\mathrm{cage}(k, 8) = \mathrm{Moore}(k, 8) = 2k^3 - 4k^2 + 4k$.
  - What happens when $k - 1$ is not a prime power is not known.

The best upper bounds known for $\mathrm{cage}(k, g)$ are the Sauer bounds [16].

$$\mathrm{cage}(k, g) \leq \mathrm{Sauer}(k, g) = \begin{cases} 2(k-2)^{g-2} & \text{if } g \text{ is odd} \\ 4(k-1)^{g-3} & \text{if } g \text{ is even.} \end{cases}$$

Hence we have

$$\mathrm{Moore}(k, 6) = 2k^2 - 2k + 2 \leq \mathrm{cage}(k, 6) \leq 4(k-2)^3 = \mathrm{Sauer}(k, 6)$$

and

$$\mathrm{Moore}(k, 8) = 2k^3 - 4k^2 + 4k \leq \mathrm{cage}(k, 8) \leq 4(k-2)^5 = \mathrm{Sauer}(k, 8).$$

We present a construction for a new graph, regular of degree p, p odd prime number, with a girth equal to 6, and $2p^2$ vertices.

$$\mathrm{Moore}(p, 6) = 2p^2 - 2p + 2 \leq \mathrm{cage}(p, 6) \leq 2p^2 < \mathrm{Sauer}(p, 6) = 4(p-1)^3.$$

Thus we improve the upper bound for the order of a $(p, 6)$-cage.

Then we present a new graph, regular of degree p, odd prime, with a girth equal to 8, and $2p^3$ vertices.

$$\text{Moore}(p, 8) = 2p^3 - 4p^2 + 4p \leq \text{cage}(p, 8) \leq 2p^3 < \text{Sauer}(p, 8) = 4(p-1)^5$$

improving the upper bound.

4. Construction of the $(p, 6)$-graph

Let p be a prime odd number, the group $\text{Aut}(\mathbb{Z}/p\mathbb{Z})^2$ can be identified as the group $GL_2(\mathbb{Z}/p\mathbb{Z})$ of invertible 2×2-matrices with coefficients in $\mathbb{Z}/p\mathbb{Z}$. The matrix

$$M = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

is of order p, and gives rise to a morphism $\lambda : \mathbb{Z}/p\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/p\mathbb{Z})^2$ by the rule $\lambda(m) = M^m$. Let $G = (\mathbb{Z}/p\mathbb{Z})^2 \rtimes_\lambda \mathbb{Z}/p\mathbb{Z}$ be the semi-direct product. For the convenience, we use the following.

Multiplicative notations: $G' = (\langle a, b\rangle) \rtimes_\lambda \langle c\rangle$, with $ab = ba$, $a^p = b^p = c^p = 1$. The map θ: $G = (\mathbb{Z}/p\mathbb{Z})^2 \rtimes_\lambda \mathbb{Z}/p\mathbb{Z} \longrightarrow (\langle a, b\rangle) \rtimes_\lambda \langle c\rangle$ defined by $\theta(k, l, m) = (a^k b^l, c^m)$ with k, l, m integers modulo p is an isomorphism between these two groups. According to this identification we have $\lambda(c^m)(a) = ab^m$, $\lambda(c^m)(b) = b$ and so the product in G is:

$$(a^k b^l, c^m).(a^{k'} b^{l'}, c^{m'}) = (a^{k+k'} b^{l+l'+mk'}, c^{m+m'}).$$

Let $s_1 = (a, 1)$, $s_2 = (1, c)$, because $s_1^t = (a^t, 1)$, $s_2^t = (1, c^t)$, the order of both s_1 and s_2 are p in G.

Proposition 4.1. *If $S = \{s_1, s_2\}$ then S is a set of generators of G.*

Proof. Since $G = \langle (a, 1), (b, 1), (1, c)\rangle$, it is sufficient to obtain $(b, 1)$ with s_1 and s_2. We can notice that $s_1^k s_2^l = (a^k, 1)(1, c^l) = (a^k, c^l)$ and

$$s_1^k s_2^l s_1^{k'} s_2^{l'} = (a^{k+k'} b^{lk'}, c^{l+l'}) \tag{I}$$

so $(b, 1) = s_1^{-1} s_2 s_1 s_2^{-1}$. □

Let us consider the G-graph $\widetilde{\Phi}(G; S)$. Since $\langle s_1\rangle \cap \langle s_2\rangle = 1$, this is a simple,connected, and regular graph of degree p.

Theorem 4.2. *The girth of the graph $\widetilde{\Phi}(G; S)$ is equal to* 6.

Proof. The G-graph $\Gamma = \widetilde{\Phi}(G; S)$ is bipartite because $|S| = 2$ and so its girth is even. The graph Γ is simple, so its girth is greater than or equal to 4. We have to prove that there is no cycle of length 4 in the graph. If there is such a cycle, there is a relation of type $s_1^k s_2^l s_1^{k'} s_2^{l'} = 1$, $0 < k, k', l, l' < p$ in G, (the other form, beginning with s_2 is equivalent to this one); applying (I) we obtain the system:

- $k + k' \equiv 0 \mod p$
- $lk' \equiv 0 \mod p$
- $l + l' \equiv 0 \mod p$

p being prime, the second equation implies $l \equiv 0 \mod p$ or $k' \equiv 0 \mod p$, which is impossible.
There is at least one cycle of length 6 in the graph, otherwise $\widetilde{\Phi}(G; S)$ would be a $(p, 8)$-graph with $2p^2$ vertices, contrary to the Moore-bound $2p^3 - 4p^2 + 4p$. One can find such a relation in the following way: there exist two nonabelian groups of order p^3; our group G is the extra-special $M(p)$ (see for example [18]), whose presentation is

$$M(p) = \langle x, y, z : x^p = y^p = z^p = 1, xy = yx, yz = zy, xzx^{-1}z^{-1} = y\rangle$$

the correspondance is $x = (a^{-1}, 1)$, $y = (b, 1)$, $z = (1, c)$. If we denote by $\varphi_g : t \longmapsto gtg^{-1}$ the inner automorphism associated to g, $xzx^{-1}z^{-1} = y$ can be read $\varphi_x(z) = yz$. Since $\varphi_x(y) = y$, we have $\varphi_{x^2}(z) = \varphi_x(yz) = y^2 z = (yz)^2 z^{-1} = \varphi_x(z)^2 z^{-1}$ $(zy = yz)$, so $\varphi_x(z)^{-2}\varphi_{x^2}(z)z = 1$ (y is eliminated). Hence $xz^{-2}xzx^{-2}z = 1$ and $s_1 = x^{-1}$, $s_2 = z$ give

$$s_1^{-1} s_2^{-2} s_1^{-1} s_2 s_1^2 s_2 = 1. \quad \square$$

The number of vertices of $\widetilde{\Phi}(G; S)$ is $2p^2$, so:

Corollary 1. *For p odd prime one has the following:*

$$\text{Moore}(p, 6) = 2p^2 - 2p + 2 \leq \text{cage}(p, 6) \leq 2p^2 < \text{Sauer}(p, 6) = 4(p-1)^3$$

improving the Sauer bound.

Remark. For the case where $k - 1$ is not equal to a prime power, there are two bounds manually computed. We have $\text{cage}(7, 6) = 90$ [17,7] (our graph for $p = 7$ is of order 98). The best known upper bound for the $(11, 6)$-cage is a graph of order 240 described in [19]; our graph for $p = 11$ is of order 242. In Section 7 we will see that, thanks to G-graph we can find a best known upper bound for both the $(11, 6)$-cage and $(13, 6)$-cage.

5. Construction of the $(p, 8)$-graph

Let p be an odd prime number, the group $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})^3$ can be identified as the group $GL_3(\mathbb{Z}/p\mathbb{Z})$. The matrix

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \in GL_3(\mathbb{Z}/p\mathbb{Z})$$

verifies

$$M^n = \begin{pmatrix} 1 & 0 & 0 \\ n & 1 & 0 \\ \dfrac{n(n-1)}{2} & n & 1 \end{pmatrix}$$

so M is of order p in $GL_3(\mathbb{Z}/p\mathbb{Z})$ and gives rise to a morphism $\lambda : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})^3$ by the rule $\lambda(n) = M^n$. Let G be the semi-direct product $G = (\mathbb{Z}/p\mathbb{Z})^3 \rtimes_\lambda \mathbb{Z}/p\mathbb{Z}$. For convenience, we use the following.

Multiplicative notations: Let $G' = (\langle a, b, c\rangle) \rtimes_\lambda \langle d\rangle$, with $\langle a, b, c\rangle$ abelian, and $a^p = b^p = c^p = d^p = 1$. The map θ: $G = (\mathbb{Z}/p\mathbb{Z})^3 \rtimes_\lambda \mathbb{Z}/p\mathbb{Z} \longrightarrow (\langle a, b, c\rangle) \rtimes_\lambda \langle d\rangle$, defined by $\theta(k, l, m, n) = (a^k b^l c^m, d^n)$ with k, l, m, n integers modulo p is an isomorphism between these two groups. According to these identifications we have $\lambda(d^n)(a) = ab^n c^{\frac{n(n-1)}{2}}$, $\lambda(d^n)(b) = bc^n$ and $\lambda(d^n)(c) = c$. So the product in G is:

$$\begin{aligned}(a^k b^l c^m, d^n).(a^{k'} b^{l'} c^{m'}, d^{n'}) &= (a^k b^l c^m \lambda(d^n)(a^{k'} b^{l'} c^{m'}), d^n d^{n'}) \\ &= \left(a^{k+k'} b^{l+l'+nk'} c^{m+m'+\frac{n(n-1)}{2}k'}, d^{n+n'}\right).\end{aligned}$$

Let $s_1 = (a, 1) \in G$, $s_2 = (1, d) \in G$. Clearly s_1 and s_2 are of order p. Let $S = \{s_1, s_2\}$. The G-graph $\widetilde{\Phi}(G; S)$ is simple ($\langle s_1\rangle \cap \langle s_2\rangle = 1$) and regular of degree p; $|G| = p^4$ and $|S| = 2$, so the number of edges of $\widetilde{\Phi}(G; S)$ is equal to p^4. Therefore the order of $\widetilde{\Phi}(G; S)$ is $2p^3$.

Proposition 5.1. *S is a set of generators of G.*

Proof. Since $G = \langle (a, 1), (b, 1), (c, 1), (1, d)\rangle$, it is sufficient to obtain $(b, 1)$ and $(c, 1)$ with s_1 and s_2. Notice that $s_1^k s_2^l = (a^k, 1)(1, d^l) = (a^k, d^l)$ and

$$s_1^k s_2^l s_1^{k'} s_2^{l'} = \left(a^{k+k'} b^{lk'} c^{\frac{l(l-1)}{2}k'}, d^{l+l'}\right) \tag{II}$$

so $(b, 1) = s_1^{-1} s_2 s_1 s_2^{-1}$, and

$$\begin{aligned}s_1^k s_2^l s_1^{k'} s_2^{l'} s_1^{k''} s_2^{l''} &= (a^{k+k'} b^{lk'} c^{\frac{l(l-1)}{2}k'}, d^{l+l'}).(a^{k''}, d^{l''}) \\ &= \left(a^{k+k'+k''} b^{lk'+(l+l')k''} c^{\frac{l(l-1)}{2}k' + \frac{(l+l')(l+l'-1)}{2}k''}, d^{l+l'+l''}\right).\end{aligned} \tag{III}$$

To obtain $(c, 1)$ we have, by [3], to solve:

- $k + k' + k'' \equiv 0 \bmod p$
- $lk' + (l + l')k'' \equiv 0 \bmod p$
- $\frac{l(l-1)}{2}k' + \frac{(l+l')(l+l'-1)}{2}k'' \equiv 1 \bmod p$
- $l + l' + l'' \equiv 0 \bmod p$.

A solution is $k = -2, k' = 1, k'' = 1, l = 1, l' = -2, l'' = 1$. Hence $(c, 1) = s_1^{-2} s_2 s_1 s_2^{-2} s_1 s_2$. □

Theorem 5.2. *The girth of the graph $\widetilde{\Phi}(G; S)$ is equal to* 8.

Proof. The G-graph $\Gamma = \widetilde{\Phi}(G; S)$ is bipartite because $|S| = 2$, so its girth is even. The graph Γ is simple, so its girth is greater than or equal to 4. We have to prove that there is no cycle of length 4 or 6 in the graph.

If there is a cycle of length 4, there is a relation $s_1^k s_2^l s_1^{k'} s_2^{l'} = 1$ in G with $0 < k, l, k', l' < p$. By Eq. (II) it implies $lk' \equiv 0 \bmod p$, where p being prime, $l \equiv 0 \bmod p$ or $k' \equiv 0 \bmod p$. There is a contradiction because we need $0 < l, k' < p$. So there is no cycle of length 4 in the graph $\widetilde{\Phi}(G; S)$.

If there is a cycle of length 6, there is a relation $s_1^k s_2^l s_1^{k'} s_2^{l'} s_1^{k''} s_2^{l''} = 1$ in G with $0 < k, l, k', l', k'', l'' < p$. By (III) we have:

- $k + k' + k'' \equiv 0 \bmod p$
- $lk' + (l + l')k'' \equiv 0 \bmod p$
- $\frac{l(l-1)}{2}k' + \frac{(l+l')(l+l'-1)}{2}k'' \equiv 0 \bmod p$
- $l + l' + l'' \equiv 0 \bmod p$.

The third equation implies $k'l(l-1)+k''(l+l')(l+l'-1) \equiv 0 \bmod p$, or $l(l-1)k'+l''(l''+1)k'' \equiv 0 \bmod p (l+l' = -l'')$; therefore the second equation can be written $lk' - l''k'' \equiv 0 \bmod p$.
By using the third equation, $l''k''(l-1)+k''l''(l''+1) \equiv 0 \bmod p$, i.e. $l''k''(-l') \equiv 0 \bmod p$. Now p being prime, this implies $l'' = 0$, or $k'' = 0$, or $l = 0$ which is impossible. So there is no cycle of length 6 in the graph $\widetilde{\Phi}(G; S)$.

If there is no cycle of length 8 in Γ, then we would have a graph of girth at least 10 with an order equal to $2p^3$, contradicting the fact that the Moore-bound $2p^4 - 6p^3 + 8p^2 - 4p + 2$. So the girth of Γ is equal to 8.

It is easy to find a relation between s_1 and s_2. Indeed in the proof of Proposition 4.1 we have seen that $(b, 1) = s_1^{-1}s_2s_1s_2^{-1}$; but $s_1 = (a, 1)$ commute with $(b, 1)$, so $s_1(b, 1) = (b, 1)s_1$ and

$$s_1^{-1}s_2s_1^{-1}s_2^{-1}s_1s_2s_1s_2^{-1} = 1. \quad \square$$

Corollary 2. *If p is an odd prime then:*

$$\text{Moore}(p, 8) = 2p^3 - 4p^2 + 4p \leq \text{cage}(p, 8) \leq 2p^3 < \text{Sauer}(p, 8) = 4(p-1)^5$$

improving the Sauer bound.

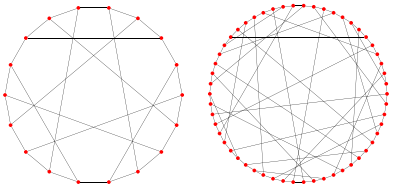
Finally this work gives rise to the following.

Conjecture 3. *For p prime and g even:*

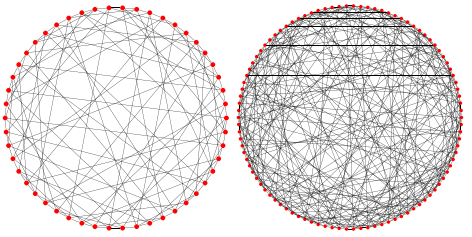
$$\text{cage}(p, g) \leq 2p^{\frac{g}{2}-1}.$$

6. Examples

The (3, 6)-graph shown in the figure below is well known, and is usually called the Pappus graph; the graph on the right is our (3, 8)-graph.



Our (5, 6)-graph and our (7, 6)-graph.



7. Improvements of the bounds

7.1. Construction of another $(p, 6)$-graph

We are going to use the following result.

Proposition 7.1. *Let $\Phi(G; S)$, where S is not a generator set. Let $(C_\alpha)_{\alpha\in\{1,2,\ldots,r\}}$, $r \geq 2$ be the set of connected components of $\Phi(G; S)$. Then $C_\alpha \simeq C_\beta$, for all $\alpha, \beta \in \{1, 2, \ldots, r\}$.*

Proof. Let $S = \{s_1, s_2, s_3, \ldots, s_k\}$ be a nongenerator subset of G. We know that $\Phi(G; S)$ is not connected.

- Let C be a connected component of $\Phi(G; S)$. Assume that C contains the vertex $(s_i)x_i$. Let $x := x_i$. For every j, $1 \leq j \leq k$, x must be in a cycle of g_{s_j}, say $(s_j)x_j$. Consequently C contains at least one vertex in each "layer", ("stratum") $(s)\square$ of each permutation.
- For every $g \in G$, consider the automorphism $\delta_g : V \longrightarrow V$, defined by $\delta_g((s)x) = (s)xg^{-1}$, and $\delta_g^{\#} : E \longrightarrow E$ associating to the n-edge $\{(s)x, (t)y\}$ and the n-edge $\{(s)xg^{-1}, (t)yg^{-1}\}$. It is easy to see that $\delta : g \longmapsto \delta_g$ is a morphism from G to $\text{Aut}(\Phi(G; S))$.

- Let C_α and C_β be two connected components of $\Phi(G; S)$ and $(s_1)x_\alpha \in C_\alpha, (s_1)x_\beta \in C_\beta$. The element $g = x_\beta^{-1}x_\alpha$ verifies $\delta_g((s_1)x_\alpha) = (s_1)x_\beta$. Hence $\delta_g(C_\alpha) \subset C_\beta$; we have also $\delta_{g^{-1}}((s_1)x_\beta) = (s_1)x_\alpha$, so that $\delta_{g^{-1}}(C_\beta) \subseteq C_\alpha$, therefore $C_\beta \subseteq \delta_g(C_\alpha)$, and finally $\delta_g(C_\alpha) = C_\beta$. □

Let $SL(2, p)$, where p is prime and $p \geq 3$, be the special linear group of 2×2 matrices over $\mathbb{F}_p$. We have $|SL(2, p)| = p(p-1)(p+1)$.

Let $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $\widetilde{\Phi}(SL(2, p); S)$ be the simple G-graph associated with $SL(2, p)$, $S = \{a, b\}$.

Easy calculations give $a^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, and $b^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$ for $n \in \frac{\mathbb{Z}}{p.\mathbb{Z}}$.

Theorem 7.2. *The girth of $\widetilde{\Phi}(SL(2, p); \{a, b\})$ is 6.*

Proof. Assume that $\widetilde{\Phi}(SL(2, p); \{a, b\})$ contains a 4-cycle. This one is of the form:
$a^{k_1}b^{l_1}a^{k_2}b^{l_2} = id$, with $0 < k_1, l_1, k_2, l_2 < p$. In this case:

$$a^{k_1}b^{l_1}a^{k_2}b^{l_2} = \begin{pmatrix} (l_1k_1+1)(l_2k_2+1)k_1l_2 & k_2(l_1k_1+1)+k_1 \\ l_1(l_2k_2+1)+l_2 & l_1k_2+1 \end{pmatrix}.$$

So $l_1k_2 + 1 \equiv 1 \bmod p$ implying $l_1k_2 \equiv 0 \bmod p$. Hence $\frac{l_1}{p}$ or $\frac{k_2}{p}$, so $l_1 \equiv 0 \bmod p$ or $k_2 \equiv 0 \bmod p$. But, by hypothesis, $0 < l_1 < p$ and $0 < k_2 < p$, a contradiction. Hence $\widetilde{\Phi}(SL(2, p); \{a, b\})$ does not contain any 4-cycle.

The graph $\widetilde{\Phi}(SL(2, p); \{a, b\})$ has $p(p-1)(p+1)$ edges and is bipartite. Because $o(a) = o(b) = p$, the degree of any vertex is p. So $\widetilde{\Phi}(SL(2, p); \{a, b\})$ has $\frac{2p(p-1)(p+1)}{p} = 2p^2 - 2$ vertices.

Suppose now that there is no 6-cycle in $\widetilde{\Phi}(SL(2, p); \{a, b\})$. So the girth is 8 at least, it leads to $\text{Moore}(p, 8) = 2p^3 - 4p^2 + 4p < 2p^2 - 2$ which is false. □

Corollary 4. *If p is an odd prime we have,*

$$\text{Moore}(p, 6) = 2p^2 - 2p + 2 \leq \text{cage}(p, 6) \leq 2p^2 - 2 < 2p^2 < \text{Sauer}(p, 6) = 4(p-1)^3.$$

Corollary 5. *Let $S = \{a, b\}$ be a subset of $SL(2, p)$, where p is prime and $p \geq 3$, and such that $o(a) = o(b) = p$. We have, $\widetilde{\Phi}(SL(2, p); \{a, b\})$ has a girth equal to 6 then $S = \{a, b\}$ is a generator set of $SL(2, p)$.*

Proof. Assume that $S = \{a, b\}$ is not a generator set. Then $\widetilde{\Phi}(SL(2, p); \{a, b\})$ is not connected, and by Proposition 7.1, each connected component C_α of $\widetilde{\Phi}(SL(2, p); \{a, b\})$ has the same vertex number, say $\frac{2p^2-2}{n}$, $n \in \mathbb{N}$, $n \geq 2$, and a girth 6. So $\text{Moore}(p, 6) = 2p^2 - 2p + 2 \leq \frac{2p^2-2}{n}$, which is impossible. □

7.2. Construction of another $(p, 8)$-graph

Let $G = \frac{\mathbb{Z}}{p.\mathbb{Z}} \times SL(2, p)$, where p is prime and $p \geq 3$. Now let $S = \{a, b\}$ with $a = \left(1_{\frac{\mathbb{Z}}{p.\mathbb{Z}}}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)$ and $b = \left(0_{\frac{\mathbb{Z}}{p.\mathbb{Z}}}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right)$. Like above we have, $a^n = \left(1_{\frac{\mathbb{Z}}{p.\mathbb{Z}}}, \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\right)$, $b^n = \left(0_{\frac{\mathbb{Z}}{p.\mathbb{Z}}}, \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}\right)$ $n \in \frac{\mathbb{Z}}{p.\mathbb{Z}}$.

For convenience, we note $X_i = 1 + k_il_i$. Hence,

$$a^{k_1}b^{l_1}a^{k_2}b^{l_2} = \left(k_1 + k_2, \begin{pmatrix} X_1X_2 + k_1l_2 & X_1k_2 + k_1 \\ l_1 + l_2 + k_2l_1l_2 & 1 + k_2l_1 \end{pmatrix}\right)$$

where every expression read modulo p.

If $a^{k_1}b^{l_1}a^{k_2}b^{l_2} = 1$, then the last equation implies $1 + l_1k_2 = 1$. Therefore $l_1k_2 = 0$, which is impossible.

Now the graph $\widetilde{\Phi}(G; \{a, b\})$ does not contain any 6-cycle; otherwise,

$$1 = a^{k_1}b^{l_1}a^{k_2}b^{l_2}a^{k_3}b^{l_3} = \left(k_1 + k_2 + k_3, \begin{pmatrix} \text{I} & \text{II} \\ \text{III} & \text{IV} \end{pmatrix}\right)$$

by brute calculation the three first equations are:

- $k_1 + k_2 + k_3 = 0$.
- $X_1X_2X_3k_3 + k_1l_2X_3 + X_1k_2l_3 + k_1l_3 = 1$ (I).
- $X_1X_2k_3 + k_1l_2k_3 + X_1k_2 + k_1 = 0$ (II).

Now (I)–(II) $\times\, l_3$ gives $X_1X_2 + k_1l_2 = 1$, i.e. $X_1X_2 = 1 - k_1l_2$. We bring this in (I):

$(1 - k_1l_2)X_3 + k_1l_2X_3 + k_2l_3X_1 + k_1l_3 = 1$, or $X_3 + k_2l_3X_1 + k_1l_3 = 1$, and $k_3l_3 + k_2l_3X_1 + k_1l_3 = 0$; since $l_3 \neq 0$ we have $k_3 + k_2X_1 + k_1 = 0$, and so $X_1 = -\frac{k_1+k_3}{k_2} = 1 - \frac{k_1+k_2+k_3}{k_2} = 1$ $(k_1 + k_2 + k_3 = 0)$; this implies $k_1l_1 = 0$ which is impossible.

The girth cannot be greater than 8, since $\text{Moore}(p, 10) = 2p^4 - 6p^3 + 8p^2 - 4p + 2$ cannot be majored by $2p^3 - 2p$.

We have shown that:

Theorem 7.3. *The girth of* $\widetilde{\Phi}\left(\frac{\mathbb{Z}}{p.\mathbb{Z}} \times SL(2,p); \{a,b\}\right)$ *is* 8.

Corollary 6. *For p odd prime one has the following:*

$$\text{Moore}(p,8) = 2p^3 - 4p^2 + 4p \leq \text{cage}(p,8) \leq 2p^3 - 2p < 2p^3 < \text{Sauer}(p,6) = 4(p-1)^5.$$

Corollary 7. *The set* $S = \{a, b\}$ *is a generator set of* $\frac{\mathbb{Z}}{p.\mathbb{Z}} \times SL(2,p)$*, where p is prime and* $p \geq 3$*.*

Proof. The argument is the same as in Corollary 4: $2p^3 - 4p^2 + 4p \leq \frac{2p^3-2p}{n}$ is impossible for $n \geq 2$. □

References

[1] W.T. Tutte, A family of cubical graphs, Proceedings of the Cambridge Philosophical Society (1947) 459–474.
[2] N. Biggs, Cubic graphs with large girth, in: Combinatorial Mathematics: Proceedings of the Third International Conference, 1989, pp. 56–62.
[3] N. Biggs, Construction for cubic graphs with large girth, The Electronic Journal of Combinatorics 5 (1998).
[4] G. Exoo, Voltage graph, group presentations and cages, The Electronic Journal of Combinatorics 11 (2004).
[5] G. Exoo, R. Jajcay, Dynamic cage survey, The Electronic Journal of Combinatorics 15 (2008).
[6] G. Malema, M. Liebelt, Low complexity regular LDPC codes for magnetic storage devices, in: Proceedings of the International Enformatika Conference, IEC'05, Enformatika, Çanakkale, Turkey, 2005, pp. 269–271.
[7] G. Royle, Higher valency cages. http://people.csse.uwa.edu.au/gordon/cages/allcages.html.
[8] H. Song, J. Liu, B.V.K. Vijaya Kumar, Large girth cycle codes for partial response channels, IEEE Transactions on Magnetics 40 (4, Part 2) (2004) 3084–3086.
[9] P. Wong, Cages a survey, Journal of Graph Theory 3 (1982) 1–22.
[10] A. Bretto, A. Faisant, A new way for associating a graph to a group, Mathematica Slovaca 55 (1) (2005) 1–8.
[11] A. Bretto, A. Faisant, L. Gillibert, *G*-graphs: a new representation of groups, Journal of Symbolic Computation 42 (5) (2007) 549–560.
[12] A. Bretto, L. Gillibert, *G*-graphs: an efficient tool for constructing symmetric and semi-symmetric graphs, Discrete Applied Mathematics 156 (14) (2008) 2719–2739.
[13] A. Bretto, L. Gillibert, *G*-graphs for the cage problem: a new upper bound, in: ISSAC, 2007, pp. 49–53.
[14] N.L. Biggs, Algebraic Graph Theory, 2nd ed., Cambridge University Press, Cambridge, England, 1993 (Chapter 23).
[15] C.D. Godsil, G.F. Royle, Algebraic Graph Theory, 1st ed., Springer Verlag, New York, 2001.
[16] N. Sauer, Extremaleigneschaften regularer Graphen gegebener Taillenweite, I und II, Osterreich Akad. Wiss. Math. Natur. Kl. S.-B. II 176 (1967) 9–25, und 28–43.
[17] E.W. Weisstein, Cage Graph. From MathWorld, A Wolfram Web Resource. http://mathworld.wolfram.com/CageGraph.html.
[18] D. Gorenstein, Finite Groups, Harper and Row, 1968.
[19] P.K. Wong, A regular graph of girth 6 and valency 11, International Journal of Mathematics and Mathematical Sciences 9 (1986) 561–565.