Algebra and Discrete Mathematics RESEARCH ARTICLE
Number 2. **(2008).** pp. 83 – 88

Exact values of girth for some graphs $D(k,q)$ and upper bounds of the order of cages

Piotr Pikuta

Communicated by V. V. Kirichenko

Abstract. Let q be a prime power and $k \in \{5,7,9,11\}$. In this paper it is shown that the girth of a graph $D(k,q)$ is equal to $k+5$. As a consequence, explicit examples of graphs which provide the best known upper bounds of the order of (r,g)-cages, $r \geq 5$, $g \in \{10,14,16\}$, are given.

1. Introduction

The objective of this paper is to show that the girth of a graph $D(k,q)$, where q is a prime power and $k \in \{5,7,9,11\}$, is equal to $k+5$. Since the proof is constructive (an explicit cycle is shown), we are ensured that graphs $D(k,q)$ are the real examples of the best known upper bounds of the order of (r,g)-cages, $r \geq 5$, $g \in \{10,14,16\}$.

In Section 2 the graphs $D(k,q)$ are introduced and the main theorem is proven. Connections to upper bounds of the order of cages are presented in Section 3.

2. Graphs $D(k,q)$

Let q be a prime power and let $k \geq 2$ be an integer. Let P and L be two k-dimensional subspaces of $(k+1)$-dimensional vector space over the Galois field $GF(q)$, the second and third coordinates of elements $(p_0,p_1,\ldots,p_k) \in P$ and $[l_0,l_1,\ldots,l_k] \in L$ are equal: $p_1 = p_2$, $l_1 = l_2$. Define $V = P \cup L$ to be a set of vertices of a graph $D(k,q)$. (Note

2000 Mathematics Subject Classification: *05C35, 05C38.*
Key words and phrases: *Girth, Cages, Extremal.*

that even though $p \in P$ and $l \in L$ may have the same coordinates they are always considered as distinct elements of V. Parenthesis and square brackets will be used to distinguish between the elements of P and L.) The relation $E \subset P \times L$, given by the following system of linear equations:

$$l_i - p_i = p_0 l_{i-2} \pmod{p}, \quad i \equiv 2 \text{ or } 3 \pmod{4}, \tag{1}$$
$$l_i - p_i = l_0 p_{i-2} \pmod{p}, \quad i \equiv 0 \text{ or } 1 \pmod{4}, \tag{2}$$

where $i = 2, 3, 4, \ldots, k$, $(p_0, p_1, \ldots p_k) \in P$ and $[l_0, l_1, \ldots, l_k] \in L$, defines the set of edges of the graph $D(k, q)$. It is easy to see that the graphs $D(k, q)$ are k-regular and bipartite.

Given nonempty subsets R and S of $GF(q)$. Let $D(k, q, R, S) = (P_R \cup L_S, E)$ be a subgraph of $D(k, q)$, where

$$\begin{aligned} P_R &= \{p \in P : p_0 \in R\}, \\ L_S &= \{l \in L : l_0 \in S\}. \end{aligned}$$

Connected components of $D(k, q)$ and $D(k, q, R, S)$ are extremely important because they provide many examples in the extremal graph theory.

The graphs $D(k, q)$ were introduced by Lazebnik and Ustimenko in [6] and [10], where the authors showed that the girth (length of the smallest cycle) of $D(k, q)$, where $k \geq 3$ odd, is greater than or equal to $k + 5$. More information about these graphs, including their properties (number of vertices and edges, components, transitivity, girth, etc.), connections with Chevalley groups and examples of their applications in extremal graph theory can be found in [3, 4, 5, 6, 7, 9, 8, 12].

Determining the girth $g(D(k, q))$ of $D(k, q)$ is not easy and only lower bounds are known for all pairs of (k, q):

$$g(D(k, q)) \geq \begin{cases} k + 4, & \text{if } k \text{ is even}, \\ k + 5, & \text{if } k \text{ is odd}. \end{cases}$$

In [3] the following conjecture has been formulated

Conjecture 2.1. *If $k \geq 3$ is odd and $q \geq 5$ is a prime power then the girth*

$$g(D(k, q)) = k + 5.$$

Also in [3], it was proved there that if $k \geq 3$ is odd and q is a prime power such that $q \equiv 1 \left(\bmod \frac{k+5}{2}\right)$ then $g(D(k, q)) = k + 5$. On the other hand, we already know that $g(D(3, q)) = 8$ for every prime power q. The main result of this section is

Theorem 2.2. *If $k \in \{5, 7, 9, 11\}$ and $q = p^m$ is a power of a prime $p > 3$ then $g(D(k, q)) = k + 5$.*

Proof. The proof will be finished if we find cycles of length $k+5$. Such cycles are obtained in the following way. Let $P_0 = \left(p_0^0, p_1^0, \ldots, p_k^0\right) \in P$ be a vertex of $D\left(k,q\right)$ and let $l_0^1 = x_1 \in GF\left(q\right)$. Using (1) and (2) one calculates $L_1 = \left[l_0^1, l_1^1, \ldots, l_k^1\right]$, so that P_0 and L_1 are connected with an edge. Given L_{2s-1}, $2 \leq 2s \leq k+5$, put $p_0^{2s} = p_0^{2s-2} + x_{2s}$, $x_{2s} \in GF\left(q\right)$, and calculate $P_{2s} = \left(p_0^{2s}, p_1^{2s}, \ldots, p_k^{2s}\right)$ by (1) and (2), so that P_{2s_2} and L_{2s-1} are connected with an edge. Analogously, for given P_{2s-2}, calculate L_{2s-1}, $1 < s \leq \frac{k+5}{2}$. All coordinates of P_{2s} and L_{2s-1} depend on $p_0^0, p_1^0, \ldots, p_k^0$ and $x_1, x_2, \ldots, x_{k+5}$. By comparing P_0 and P_{k+5} a system of equations is obtained, then simplified and investigated for a solution such that $x_i \neq 0$, $i \in \{2, 3, \ldots, k+5\}$. All equations (after simplifications) are linear with respect to any single variable and do not contain $p_0^0, p_1^0, \ldots, p_k^0$ or x_1, which corresponds to the transitivity properties of the graphs, see [6].

A cycle of length 10 of the graph $D\left(5,q\right)$, ($q = p^m$, $p > 3$ is prime) has the following vertices (all numbers should be reduced $\bmod p$ if necessary):

```
0: (0, 0, 0, 0, 0, 0)
1: [2, 0, 0, 0, 0, 0]
2: (1, p-2, p-2, 0, 4, 0)
3: [p-1, p-3, p-3, p-3, 6, 0]
4: (p-1, p-4, p-4, p-6, 2, p-6)
5: [0, p-4, p-4, p-2, 2, p-6]
6: (2, p-4, p-4, 6, 2, p-6)
7: [1, p-2, p-2, 2, p-2, 0]
8: (p-1, p-1, p-1, 0, p-1, 0)
9: [p-1, 0, 0, 0, 0, 0]
10: (0, 0, 0, 0, 0, 0)
```

A cycle of length 12 of the graph $D\left(7,q\right)$, ($q = p^m$, $p \geq 3$ is prime) has the following vertices (all numbers should be reduced $\bmod p$ if necessary):

```
 0: (0, 0, 0, 0, 0, 0, 0, 0)
 1: [0, 0, 0, 0, 0, 0, 0, 0]
 2: (1, 0, 0, 0, 0, 0, 0, 0)
 3: [1, 1, 1, 1, 0, 0, 0, 0]
 4: (0, 1, 1, 1, p-1, p-1, 0, 0)
 5: [2, 1, 1, 1, 1, 1, 0, 0]
 6: (1, p-1, p-1, 0, 3, 1, p-1, p-1)
 7: [0, p-1, p-1, p-1, 3, 1, 2, 0]
 8: (0, p-1, p-1, p-1, 3, 1, 2, 0)
 9: [1, p-1, p-1, p-1, 2, 0, 2, 0]
10: (1, p-2, p-2, 0, 4, 0, 0, 0)
```

```
11: [2, 0, 0, 0, 0, 0, 0, 0]
12: (0, 0, 0, 0, 0, 0, 0, 0)
```

A cycle of length 14 of the graph $D\,(9, q)$, ($q = p^m$, $p > 3$ is prime) has the following vertices (all numbers should be reduced mod p if necessary):

```
 0: (0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
 1: [0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
 2: (1, 0, 0, 0, 0, 0, 0, 0, 0, 0)
 3: [1, 1, 1, 1, 0, 0, 0, 0, 0, 0]
 4: (0, 1, 1, 1, p-1, p-1, 0, 0, 0, 0)
 5: [0, 1, 1, 1, p-1, p-1, 0, 0, 0, 0]
 6: (p-3, 1, 1, 4, p-1, p-1, p-3, p-3, 0, 0)
 7: [p-2, 7, 7, p-17, p-3, p-9, 6, 24, 6, 6]
 8: (p-2, 3, 3, p-3, 3, p-15, 0, 6, 6, 18)
 9: [p-3, 9, 9, p-21, p-6, p-6, 12, 18, 6, 0]
10: (p-3, 0, 0, 6, p-6, 12, p-6, 0, p-12, 0)
11: [p-2, 6, 6, p-12, p-6, 0, 12, 0, 0, 0]
12: (p-2, 2, 2, 0, p-2, 0, 0, 0, 0, 0)
13: [1, 0, 0, 0, 0, 0, 0, 0, 0, 0]
14: (0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
```

A cycle of length 16 of the graph $D\,(11, q)$, ($q = p^m$, $p > 3$ is prime) has the following vertices (all numbers should be reduced mod p if necessary):

```
0: (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
1: [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
2: (1, p-1, p-1, 0, 1, 0, 0, 0, 0, 0, 0, 0)
3: [p-2, p-3, p-3, p-3, 3, 0, 3, 0, 0, 0, 0, 0]
4: (0, p-3, p-3, p-3, p-3, p-6, 3, 0, 6, 0, 0, 0)
5: [p-1, p-3, p-3, p-3, 0, p-3, 3, 0, 3, 0, 0, 0]
6: (1, p-2, p-2, 0, p-2, p-3, 3, 3, 6, 3, p-3, 0)
7: [0, p-2, p-2, p-2, p-2, p-3, 1, 0, 6, 3, 3, 3]
8: (0, p-2, p-2, p-2, p-2, p-3, 1, 0, 6, 3, 3, 3)
9: [p-2, p-2, p-2, p-2, 2, 1, 1, 0, 4, 3, 3, 3]
10: (1, 0, 0, 0, 2, 1, p-1, p-1, 2, 1, p-1, 0)
11: [1, 1, 1, 1, 2, 1, 1, 0, 1, 0, 0, 0]
12: (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)
13: [0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0]
14: (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)
15: [p-1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
16: (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
```

The cycles given here are easily verified using (1) and (2). □

Remark 2.3. *Notice that if $k = 7$ the cycle given in the proof shows that we can take $p \geq 3$ and therefore $g\left(D\left(7, 3^m\right)\right) = 12$, where m is a positive integer. Analogous conclusions cannot be drawn for $k \in \{5, 9, 11\}$.*

3. Cages

Let $r \geq 2$ and $g \geq 3$ be integers. A (r, g)-graph is a r-regular graph with girth equal to g. A (r, g)-graph of minimum order (i.e. having the fewest possible number of vertices) is called a (r, g)-cage. Let $\nu(r, g)$ be the order of a (r, g)-cage. The problem of determining the values of $\nu(r, g)$ is still open for most pairs of (r, g).

By counting the number of vertices spreading from a given edge (for even values of g) or a given vertex (if g is odd) in a k-regular graph of girth g, the following lower bounds are easy to obtain

$$\nu(k, g) \geq 2 \sum_{j=0}^{\frac{g}{2}-1} (r-1)^i = \frac{2(r-1)^{g/2} - 2}{r-2}, \qquad \text{if } g \text{ is even,}$$

and

$$\nu(k, g) \geq 1 + \sum_{j=1}^{\frac{g-1}{2}} r(r-1)^i = \frac{r(r-1)^{(g-1)/2} - 2}{r-2}, \qquad \text{if } g \text{ is odd.}$$

Upper bounds have been established by Lazebnik, Ustimenko and Woldar [9]

$$\nu(r, g) \leq 2rq^{\frac{3}{4}g - a}, \tag{3}$$

where $r \geq 5$ and $g \geq 5$ are integers, q is the smallest odd prime power satisfying $r \leq q$ and $a = \frac{16}{4}, \frac{11}{4}, \frac{14}{4}, \frac{13}{4}$, for $g \equiv 0, 1, 2, 3 \bmod 4$, respectively, and recently, by Araujo-Pardo, González, Montellano-Ballesteros and Serra [1] for $g \in \{11, 12\}$, $\nu(r, 11) \leq \nu(r, 12) \leq 2rq^4$, where q is the smallest prime power greater than or equal to $r \geq 3$. More information on cages and bounds of $\nu(k, g)$ can be found in the article of Wong [13] and on the website of Royle [11], see also [7] and [9].

Upper bounds (3) in [9] were obtained in a nonconstructive way. However, the constructive proof of Theorem 2.2 enables us to give examples of r-regular graphs with girth $g \in \{10, 14, 16\}$ and order equal to the right-hand side of (3). Let q be a power of a prime $p > 3$. Define $R_k \subset GF(q)$, $k \in \{5, 9, 11\}$, in such a way that it has exactly $r \geq 5$ elements and

$$\begin{aligned} R_5 &\supset \{0, 1, 2, p-1\}, \\ R_7 &\supset \{0, 1, 2\}, \\ R_9 &\supset \{0, 1, p-3, p-2\}, \\ R_{11} &\supset \{0, 1, p-2, p-1\}. \end{aligned}$$

Every connected component of $D(k, q, R_k, R_k)$ is a r-regular graph of order $2rq^{\frac{3}{4}g-a}$ (see [4] or [9]) with girth $g = k+5$ (see Theorem 2.2), where $a = 4$ or $\frac{7}{2}$, for $g \equiv 0$ or $2 \pmod 4$, respectively.

References

[1] G. Araujo-Pardo, D. González, J. J. Montellano-Ballesteros and O. Serra. On upper bounds and connectivity of cages. *Electronic Notes in Discrete Mathematics* 26:1-7, 2006.

[2] B. Bollobás. *Extremal graph theory*, Academic Press, London, 1978.

[3] Z. Füredi, Á. Seress, V. A. Ustimenko, and A. J. Woldar. Graphs of Prescribed Girth and Bi–Degree. *Journal of Combinatorial Theory. Series B*, 64(2):228–239, 1995.

[4] F. Lazebnik, V. A. Ustimenko and A. J. Woldar. A Characterization of the components of the graphs $D(k, q)$. *Discrete Mathematics*, 157:271–283, 1996.

[5] F. Lazebnik, V. A. Ustimenko and A. J. Woldar. A New Series of Dense Graphs of High Girth, *American Mathematical Society. Bulletin. New Series*, 32(1):73–79, 1995.

[6] F. Lazebnik and V. A. Ustimenko. Explicit construction of graphs with an arbitrary large girth and of large size. *Discrete Applied Mathematics*, 60(1-3):275-284, 1995.

[7] F. Lazebnik and A. J. Woldar. General properties of some families of graphs defined by systems of equations. *Journal of Graph Theory*, 38(2): 65–86, 2001.

[8] F. Lazebnik and V. A. Ustimenko. New examples of graphs without small cycles and of large size. *European Journal of Combinatorics*, 14(5):445–460, 1993.

[9] F. Lazebnik, V. A. Ustimenko and A. J. Woldar. New upper bounds on the order of cages. *Electronic Journal of Combinatorics*, 4(2):R13, 1997.

[10] F. Lazebnik and V. A. Ustimenko. Some Algebraic Constructions of Dense Graphs of Large Girth and of Large Size. *Expanding graphs (Princeton, NJ, 1992)*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Volume 10, 75–93, Providence, RI, 1993.

[11] G. Royle. *Cages of higher valency.* http://www.csse.uwa.edu.au/~gordon/cages/allcages.html

[12] V. A. Ustimenko and A. J. Woldar. Extremal properties of regular and affine generalized m-gons as tactical configurations. *European Journal of Combinatorics*, 24:99–111, 2003.

[13] P. K. Wong. Cages–A Survey. *Journal of Graph Theory*, 6(1):1-22, 1982.

Contact information

P. Pikuta Institute of Mathematics, Maria Curie-Skłodowska University, pl. Marii Curie-Skłodowskiej 1, 20-031 Lublin, Poland

Received by the editors: 09.06.2008
and in final form 09.06.2008.