Discrete Mathematics 339 (2016) 2384–2392

Contents lists available at ScienceDirect

Discrete Mathematics

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

On the conjecture for the girth of the bipartite graph $D(k, q)$[☆]

Xiaoyan Cheng, Wenbing Chen, Yuansheng Tang[*]

School of Mathematical Sciences, Yangzhou University, Yangzhou, Jiangsu, 225002, PR China

ARTICLE INFO

Article history:
Received 9 August 2015
Received in revised form 17 March 2016
Accepted 21 March 2016
Available online 10 May 2016

Keywords:
Bipartite graph
Non-recurrent walk
Non-recurrent circuit
Girth cycle
Edge-transitive
Binomial coefficient

ABSTRACT

For integer $k \geq 2$ and prime power q, Lazebnik and Ustimenko (1995) proposed an algebraic bipartite graph $D(k, q)$ which is q-regular, edge-transitive and of large girth. Füredi et al. (1995) conjectured that $D(k, q)$ has girth $k + 5$ for all odd k and all $q \geq 4$ and, shown that this conjecture is true for the case that $(k+5)/2$ divides $q-1$. Cheng et al. (2014) shown that this conjecture is true for the case that $(k + 5)/2$ is an arbitrary power of the characteristic of $\mathbb{F}_q$. In this paper, we propose a generalization for the binomial coefficients and show that this conjecture is true when $(k + 5)/2$ is the product of an arbitrary factor of $q - 1$ and an arbitrary power of the characteristic of $\mathbb{F}_q$.

1. Introduction

The graphs we consider in this paper are simple, i.e. undirected, without loops and multiple edges. For a graph G, its vertex set and edge set are denoted by $V(G)$ and $E(G)$, respectively. The degree (or valency) of a vertex $v \in G$ is the number of the vertices that are adjacent to it. A graph is said to be r-regular if the degree of any vertex is equal to r. An automorphism of graph G is a bijection ϕ from $V(G)$ to itself such that $\{\phi(v), \phi(v')\}$ is an edge iff $\{v, v'\}$ is. Graph G is said to be vertex-transitive if for any two vertices v_1, v_2 there is an automorphism ϕ of G such that $\phi(v_1) = v_2$. Graph G is said to be edge-transitive if for any two edges $\{v_1, v_1'\}, \{v_2, v_2'\}$ there is an automorphism ϕ of G such that $\phi(\{v_1, v_1'\}) = \{v_2, v_2'\}$. A sequence $v_1 v_2 \cdots v_n$ of vertices of G is called a non-recurrent walk of length n if $\{v_i, v_{i+1}\} \in E(G)$ for $i = 1, 2, \ldots, n-1$ and $v_j \neq v_{j+2}$ for $j = 1, 2, \ldots, n-2$. A non-recurrent walk $v_1 v_2 \cdots v_n$ is called a non-recurrent circuit further if its length n is not smaller than 3 and $v_3 v_4 \cdots v_n v_1 v_2$ is still a non-recurrent walk. If graph G contains at least one non-recurrent circuit, then the girth of G, denoted by $g(G)$, is the length of a shortest non-recurrent circuit in G. Clearly, in graph G the non-recurrent circuits of length $g(G)$ are just the girth cycles of G.

In literature, graphs with large girth and a high degree of symmetry have been applied to variant problems in extremal graph theory, finite geometry, coding theory, cryptography, communication networks and quantum computations (c.f. [1] to [19]). For example, one of the most attractive progresses in coding theory is the study on the low-density parity-check (LDPC) codes. Many of the LDPC codes with low-complexity decoding and near Shannon limit performance are constructed by using bipartite graphs of large girth. Indeed, the girth of the Tanner graph of an LDPC code has been widely trusted to be the main parameter affecting its error performance, such as the error floor. Large girth usually leads fast convergence for iterative decoding of LDPC codes.

☆ This work was supported by the Natural Science Foundation of China (No. 61379004), the Key Project of Chinese Ministry of Education (No. 208045) and the open Foundation of NCRL of Southeast University (W200819).

* Corresponding author.
E-mail addresses: cxy_nt@hotmail.com (X. Cheng), chenwenbing007@163.com (W. Chen), ystang@yzu.edu.cn (Y. Tang).

http://dx.doi.org/10.1016/j.disc.2016.03.018
0012-365X/

For integer $k \geq 2$ and prime power q, in [6] Lazebnik and Ustimenko proposed a bipartite graph, denoted by $D(k, q)$, which is q-regular, edge-transitive and of large girth. $D(k, q)$ has been investigated quite well (cf. [1] to [17]). The girth of $D(k, q)$ is at least $k + 4$ for $k \geq 3$. The connected components of $D(k, q)$ provide the best-known asymptotic lower bound for the greatest number of edges in graphs of their order and girth, with the exceptions of $k = 7, 8$.

It is of interest to know whether $D(k, q)$ has larger girth than the lower bound. Since the length of any non-recurrent circuit in a bipartite graph is even, the girth of $D(k, q)$ is at least $k + 5$ for odd k. The following conjecture was proposed in [3]:

Conjecture A. *$D(k, q)$ has girth $k + 5$ for all odd k and all $q \geq 4$.*

Conjecture A has been proved in [3] for the case that $(k + 5)/2$ divides $q - 1$ and in [1] for the case that $(k + 5)/2$ is a power of the characteristic of $\mathbb{F}_q$, respectively. We will show in this paper that Conjecture A is valid when $(k + 5)/2$ is the product of an arbitrary factor of $q - 1$ and an arbitrary power of the characteristic of the finite field $\mathbb{F}_q$.

This paper is arranged as follows. To show the main result, we introduce a generalization for the binomial coefficients in Section 2 at first. Then, by using this generalization and the closed-form expression of the non-recurrent walks given in [1], we show the main result of this paper in Section 3.

2. A generalization of the binomial coefficients

In this section, we consider to generalize the binomial coefficient $\binom{k+s}{k} = \frac{(k+s)!}{k!s!}$.

Let $\mathbb{F}_q$ be the finite field of q elements. Let $b \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ be a fixed element of order h, where h is the smallest positive integer such that $b^h = 1$. For nonnegative integers k and s, in $\mathbb{F}_q$ we define

$$\theta(k, s) = \binom{\lfloor k/h \rfloor + \lfloor s/h \rfloor}{\lfloor k/h \rfloor} \prod_{j=1}^{s \bmod h} \frac{b^{k+j} - 1}{b^j - 1}, \tag{1}$$

where $s \bmod h$ is the smallest nonnegative integer such that h divides $s - s \bmod h$ and, we define $\prod_{j=1}^{0} \frac{b^{k+j}-1}{b^j-1} = 1$ as the unit of the finite field $\mathbb{F}_q$ by convention. Furthermore, we define $\theta(k, s) = 0$ if $k < 0$ or $s < 0$.

Since for any nonnegative integers k and s we have

$$\prod_{j=1}^{k \bmod h} \frac{b^{s+j} - 1}{b^j - 1} = \prod_{j=1}^{s \bmod h} \frac{b^{k+j} - 1}{b^j - 1},$$

we see that $\theta(k, s)$ is symmetric with respect to parameters k and s, namely,

$$\theta(k, s) = \theta(s, k). \tag{2}$$

From the definition of $\theta(k, s)$, we also see easily that

$$\theta(k, s) = 0 \quad \text{if } k \bmod h + s \bmod h \geq h, \tag{3}$$

$$\theta(k, s) = \binom{\lfloor k/h \rfloor + \lfloor s/h \rfloor}{\lfloor k/h \rfloor} \quad \text{if } h|k \text{ or } h|s, \tag{4}$$

where the binomial coefficient is treated as an element of the finite field $\mathbb{F}_q$. We note that $\theta(k, s)$ can be seen as a generalization of the binomial coefficient $\binom{k+s}{s}$ in finite fields, since

$$\binom{k+s}{k} = \frac{(k+s)!}{k!s!} = \lim_{x \to 1} \prod_{j=1}^{s} \frac{x^{k+j} - 1}{x^j - 1}.$$

Below we present several properties of $\theta(k, s)$ which will be used in Section 3.

Lemma 1. *For any integers k, s with $|k| + |s| \neq 0$,*

$$\theta(k, s) = b^k \theta(k, s - 1) + \theta(k - 1, s), \tag{5}$$

$$\theta(k, s) = \theta(k, s - 1) + b^s \theta(k - 1, s). \tag{6}$$

Proof. We only prove the equality (5). The equality (6) can be proved simply from (5) and the symmetry of $\theta(k, s)$.

If $k < 0$ or $s < 0$, then $\theta(k, s) = \theta(k, s-1) = \theta(k-1, s) = 0$ and thus (5) follows. If $k = 0$, then $s \neq 0$ and thus (5) follows from $b^k = 1$, $\theta(k, s) = \theta(k, s - 1)$ and $\theta(k - 1, s) = 0$. If $s = 0$, then $k \neq 0$ and thus (5) follows from $\theta(k, s) = \theta(k - 1, s)$ and $\theta(k, s - 1) = 0$.