On the spectrum of Wenger graphs

Sebastian M. Cioabă, Felix Lazebnik, Weiqiang Li

Department of Mathematical Sciences, University of Delaware, Newark, DE 19707-2553, USA

 ARTICLE INFO

Article history:
Received 14 April 2013
Available online 5 March 2014

Keywords:
Eigenvalues of graphs
Graph spectrum
Expander
Edge-transitive graphs
Vertex-transitive graphs
Extremal graph theory
Algebraically defined graphs

 ABSTRACT

Let $q = p^e$, where $p$ is a prime and $e \geq 1$ is an integer. For $m \geq 1$, let $P$ and $L$ be two copies of the $(m + 1)$-dimensional vector spaces over the finite field $\mathbb{F}_q$. Consider the bipartite graph $W_m(q)$ with partite sets $P$ and $L$ defined as follows: a point $p = (p_1, p_2, \ldots, p_{m+1}) \in P$ is adjacent to a line $[l] = [l_1, l_2, \ldots, l_{m+1}] \in L$ if and only if the following $m$ equalities hold: $l_{i+1} + p_{i+1} = l_ip_i$ for $i = 1, \ldots, m$. We call the graphs $W_m(q)$ Wenger graphs. In this paper, we determine all distinct eigenvalues of the adjacency matrix of $W_m(q)$ and their multiplicities. We also survey results on Wenger graphs. © 2014 Elsevier Inc. All rights reserved.

1. Introduction

All graph theory notions can be found in Bollobás [2]. Let $q = p^e$, where $p$ is a prime and $e \geq 1$ is an integer. For $m \geq 1$, let $P$ and $L$ be two copies of the $(m + 1)$-dimensional vector spaces over the finite field $\mathbb{F}_q$. We call the elements of $P$ points and the elements of $L$ lines. If $a \in \mathbb{F}_q^{m+1}$, then we write $(a) \in P$ and $[a] \in L$. Consider the bipartite graph $W_m(q)$ with partite sets $P$ and $L$ defined as follows: a point $p = (p_1, p_2, \ldots, p_{m+1}) \in P$ is adjacent to a line $[l] = [l_1, l_2, \ldots, l_{m+1}] \in L$ if and only if the following $m$ equalities hold:

$$l_2 + p_2 = l_1p_1,$$
$$l_3 + p_3 = l_2p_1.$$

http://dx.doi.org/10.1016/j.jctb.2014.02.008
0095-8956/© 2014 Elsevier Inc. All rights reserved.
\[
l_{m+1} + p_{m+1} = l_mp_1.
\]

The graph \( W_m(q) \) has \( 2q^{m+1} \) vertices, is \( q \)-regular and has \( q^{m+2} \) edges.

In [25], Wenger introduced a family of \( p \)-regular bipartite graphs \( H_k(p) \) as follows. For every \( k \geq 2 \), and every prime \( p \), the partite sets of \( H_k(p) \) are two copies of integer sequences \( \{0, 1, \ldots, p-1\}^k \), with vertices \( a = (a_0, a_1, \ldots, a_{k-1}) \) and \( b = (b_0, b_1, \ldots, b_{k-1}) \) forming an edge if
\[
b_j \equiv a_j + a_{j+1}b_{k-1} \pmod{p} \quad \text{for all } j = 0, \ldots, k-2.
\]

The introduction and study of these graphs were motivated by an extremal graph theory problem of determining the largest number of edges in a graph of order \( n \) containing no cycle of length \( 2k \). This parameter also known as the Turán number of the cycle \( C_{2k} \), is denoted by \( \text{ex}(n, C_{2k}) \). Bondy and Simonovits [3] showed that \( \text{ex}(n, C_{2k}) = O(n^{1+1/k}) \), \( n \to \infty \). Lower bounds of magnitude \( n^{1+1/k} \) were known (and still are) for \( k = 2, 3, 5 \) only, and the graphs \( H_k(p) \), \( k = 2, 3, 5 \), provided new and simpler examples of such magnitude extremal graphs. For many results on \( \text{ex}(n, C_{2k}) \), see Verstraëte [21], Pikhurko [19] and references therein.

In [9], Lazebnik and Ustimenko, using a construction based on a certain Lie algebra, arrived at a family of bipartite graphs \( H'_n(q) \), \( n \geq 3 \), \( q \) is a prime power, whose partite sets were two copies of \( \mathbb{F}_q^{n-1} \), with vertices \( (p) = (p_2, p_3, \ldots, p_n) \) and \([l] = [l_1, l_3, \ldots, l_n]\) forming an edge if
\[
l_k - p_k = l_1p_{k-1} \quad \text{for all } k = 3, \ldots, n.
\]

It is easy to see that for all \( k \geq 2 \) and prime \( p \), graphs \( H_k(p) \) and \( H'_{k+1}(p) \) are isomorphic, and the map
\[
\phi : (a_0, a_1, \ldots, a_{k-1}) \mapsto (a_{k-1}, a_{k-2}, \ldots, a_0),
\]
\[
(b_0, b_1, \ldots, b_{k-1}) \mapsto [b_{k-1}, b_{k-2}, \ldots, b_0],
\]
provides an isomorphism from \( H_k(p) \) to \( H'_{k+1}(p) \). Hence, graphs \( H'_n(q) \) can be viewed as generalizations of graphs \( H_k(p) \). It is also easy to show that graphs \( H'_{m+2}(q) \) and \( W_m(q) \) are isomorphic: the function
\[
\psi : (p_2, p_3, \ldots, p_{m+2}) \mapsto [p_2, p_3, \ldots, p_{m+2}],
\]
\[
[l_1, l_3, \ldots, l_{m+2}] \mapsto (-l_1, -l_3, \ldots, -l_{m+1}),
\]
mapping points to lines and lines to points, is an isomorphism of \( H'_{m+2}(q) \) to \( W_m(q) \). Combining this isomorphism with the results in [9], we obtain that the graph \( W_1(q) \)
is isomorphic to an induced subgraph of the point-line incidence graph of the projective plane $PG(2,q)$, the graph $W_2(q)$ is isomorphic to an induced subgraph of the point-line incidence graph of the generalized quadrangle $Q(4,q)$, and $W_3(q)$ is a homomorphic image of an induced subgraph of the point-line incidence graph of the generalized hexagon $H(q)$.

We call the graphs $W_m(q)$ Wenger graphs. The representation of Wenger graphs as $W_m(q)$ graphs first appeared in Lazebnik and Viglione [11]. These authors suggested another useful representation of these graphs, where the right-hand sides of equations are represented as monomials of $p_1$ and $l_1$ only, see [22]. For this, define a bipartite graph $W'_m(q)$ with the same partite sets as $W_m(q)$, where $(p) = (p_1,p_2,\ldots,p_{m+1})$ and $[l] = [l_1,l_2,\ldots,l_{m+1}]$ are adjacent if

$$l_k + p_k = l_1p_1^{k-1} \quad \text{for all } k = 2,\ldots,m+1. \tag{1}$$

The map

$$\omega: (p) \mapsto (p_1,p_2,p_1',\ldots,p_m'), \quad \text{where } p_k' = p_k + \sum_{i=2}^{k-1} p_i p_1^{k-i}, \quad k = 3,\ldots,m+1,$$

$$[l] \mapsto [l_1,l_2,\ldots,l_{m+1}],$$

defines an isomorphism from $W_m(q)$ and $W'_m(q)$.

It was shown in [9] that the automorphism group of $W_m(q)$ acts transitively on each of $P$ and $L$, and on the set of edges of $W_m(q)$. In other words, the graphs $W_m(q)$ are point-, line-, and edge-transitive. A more detailed study, see [11], also showed that $W_1(q)$ is vertex-transitive for all $q$, and that $W_2(q)$ is vertex-transitive for even $q$. For all $m \geq 3$ and $q \geq 3$, and for $m = 2$ and all odd $q$, the graphs $W_m(q)$ are not vertex-transitive. Another result of [11] is that $W_m(q)$ is connected when $1 \leq m \leq q-1$, and disconnected when $m \geq q$, in which case it has $q^{m-q+1}$ components, each isomorphic to $W_{q-1}(q)$. In [23], Viglione proved that when $1 \leq m \leq q-1$, the diameter of $W_m(q)$ is $2m+2$.

We wish to note that the statement about the number of components of $W_m(q)$ becomes apparent from the representation (1). Indeed, as $l_1p_1^i = l_1p_1^{i+q-1}$, all points and lines in a component have the property that their coordinates $i$ and $j$, where $i \equiv j \mod (q-1)$, are equal. Hence, points $(p)$, having $p_1 = \cdots = p_q = 0$, and at least one distinct coordinate $p_i$, $q+1 \leq i \leq m+1$, belong to different components. This shows that the number of components is at least $q^{m-q+1}$. As $W_{q-1}(q)$ is connected and $W_m(q)$ is edge-transitive, all components are isomorphic to $W_{q-1}(q)$. Hence, there are exactly $q^{m-q+1}$ of them. A result of Mader [16] also obtained independently by Watkins [24], and the edge-transitivity of $W_m(q)$ imply that the vertex connectivity (and consequently the edge connectivity) of $W_m(q)$ equals the degree of regularity $q$, for any $1 \leq m \leq q-1$.

Shao, He and Shan [20] proved that in $W_m(q)$, $q = p^e$, $p$ prime, for $m \geq 2$, for any integer $l \neq 5, 4 \leq l \leq 2p$ and any vertex $v$, there is a cycle of length $2l$ passing through the vertex $v$. We wish to remark that the edge-transitivity of $W_m(q)$ implies
the existence of a $2l$ cycle through any edge, a stronger statement. Li and Lih [12] used the Wenger graphs to determine the asymptotic behavior of the Ramsey number $r_n(C_{2k}) = \Theta(n^{k/(k-1)})$ when $k \in \{2, 3, 5\}$ and $n \to \infty$; the Ramsey number $r_n(G)$ equals the minimum integer $N$ such that in any edge-coloring of the complete graph $K_N$ with $n$ colors, there is a monochromatic $G$. Representation (1) points to a relation of Wenger graphs with the moment curve $t \mapsto (1, t, t^2, t^3, \ldots, t^m)$, and, hence, with the Vandermonde’s determinant, which was explicitly used in [25]. This is also in the background of some geometric constructions by Mellinger and Mubayi [17] of magnitude extremal graphs without short even cycles.

In Section 2, we determine the spectrum of the graphs $W_m(q)$, defined as the multiset of the eigenvalues of the adjacency matrix of $W_m(q)$. Futorny and Ustimenko [6] considered applications of Wenger graphs in cryptography and coding theory, as well as some generalizations. They also conjectured that the second largest eigenvalue $\lambda_2$ of the adjacency matrix of Wenger graphs $W_m(q)$ is bounded from above by $2\sqrt{q}$. The results of this paper confirm the conjecture for $m = 1$ and 2, or $m = 3$ and $q \geq 4$, and refute it in other cases. We wish to point out that for $m = 1$ and 2, or $m = 3$ and $q \geq 4$, the upper bound $2\sqrt{q}$ also follows from the known values of $\lambda_2$ for the point-line $(q + 1)$-regular incidence graphs of the generalized polygons $PG(2, q)$, $Q(4, q)$ and $H(q)$ and eigenvalue interlacing (see Brouwer, Cohen and Neumaier [4]). In [13], Li, Lu and Wang showed that the graphs $W_m(q)$, $m = 1, 2$, are Ramanujan, by computing the eigenvalues of another family of graph described by systems of linear equations in [10], $D(k, q)$, for $k = 2, 3$. Their result follows from the fact that $W_1(q) \simeq D(2, q)$, and $W_2(q) \simeq D(3, q)$. For more on Ramanujan graphs, see Lubotzky, Phillips and Sarnak [15], or Murty [18]. Our results also imply that for fixed $m$ and large $q$, the Wenger graph $W_m(q)$ are expanders. For more details on expanders and their applications, see Hoory, Linial and Wigderson [7], and references therein.

2. Main results

**Theorem 2.1.** For all prime power $q$ and $1 \leq m \leq q - 1$, the distinct eigenvalues of $W_m(q)$ are

$$\pm q, \pm \sqrt{mq}, \pm \sqrt{(m - 1)q}, \ldots, \pm \sqrt{2q}, \pm \sqrt{q}, 0.$$  \hspace{1cm} (2)

The multiplicity of the eigenvalue $\pm \sqrt{iq}$ of $W_m(q)$, $0 \leq i \leq m$, is

$$(q - 1) \binom{q}{i} \sum_{d=i}^{m} \sum_{k=0}^{d-i} (-1)^k \binom{q - i}{k} q^{d-i-k}.$$  \hspace{1cm} (3)

**Proof.** As the graph $W_m(q)$ is bipartite with partitions $L$ and $P$, we can arrange the rows and the columns of an adjacency matrix $A$ of $W_m(q)$ such that $A$ has the following form:
\[ A = L \begin{pmatrix} L & P \\ 0 & N^T \end{pmatrix} \]  

which implies that
\[ A^2 = \begin{pmatrix} N^T N & 0 \\ 0 & N N^T \end{pmatrix}. \]

As the matrices \( N^T N \) and \( N N^T \) have the same spectrum, we just need to compute the spectrum for one of these matrices. To determine the spectrum of \( N^T N \), let \( H \) denote the point-graph of \( W_m(q) \) on \( L \). This means that the vertex set of \( H \) is \( L \), and two distinct lines \([l]\) and \([l']\) of \( W_m(q) \) are adjacent in \( H \) if there exists a point \((p)\) ∈ \( P \), such that \([l] \sim (p) \sim [l']\) in \( W_m(q) \). More precisely, \([l]\) and \([l']\) are adjacent in \( H \), if there exists \( p_1 \in \mathbb{F}_q \) such that for all \( i = 1, \ldots, m \), we have
\[
l_1 \neq l_1' \quad \text{and} \quad l_{i+1} - l_{i+1}' = p_1 (l_i - l'_i) \quad \Leftrightarrow \quad l_1 \neq l_1' \quad \text{and} \quad l_{i+1} - l_{i+1}' = p'_1 (l_1 - l'_1). \]

This implies that \( H \) is actually the Cayley graph of the additive group of the vector space \( \mathbb{F}_q^{m+1} \) with a generating set
\[
S = \{(t, tu, \ldots, tu^m) \mid t \in \mathbb{F}_q^*, u \in \mathbb{F}_q \}. \]

Let \( \omega \) be a complex \( p \)-th root of unity. For \( x \in \mathbb{F}_q \), the trace of \( x \) is defined as \( \text{tr}(x) = \sum_{i=0}^{p-1} x^i \). The eigenvalues of \( H \) are indexed after the \((m+1)\)-tuples \((w_1, \ldots, w_{m+1}) \in \mathbb{F}_q^{m+1} \), and can be represented in the following form (see Babai [1] and Lovász [14] for more details):
\[
\lambda_{(w_1,\ldots,w_{m+1})} = \sum_{(t, tu, \ldots, tu^m) \in S} \omega^\text{tr}(tw_1) \cdot \omega^\text{tr}(tw_2) \cdot \ldots \cdot \omega^\text{tr}(tu^m w_{m+1}) \\
= \sum_{t \in \mathbb{F}_q^*, u \in \mathbb{F}_q} \omega^\text{tr}(tw_1 + tw_2 + \ldots + tu^m w_{m+1}) \\
= \sum_{t \in \mathbb{F}_q^*, u \in \mathbb{F}_q} \omega^\text{tr}(t(f(u))) \quad \text{(where } f(u) := w_1 + w_2 u + \ldots + w_{m+1} u^m) \)
\[
= \sum_{t \in \mathbb{F}_q^*, f(u) = 0} \omega^\text{tr}(t(f(u))) + \sum_{t \in \mathbb{F}_q^*, f(u) \neq 0} \omega^\text{tr}(t(f(u))).
\]

As \( \sum_{t \in \mathbb{F}_q^*} \omega^\text{tr}(tx) = q - 1 \) for \( x = 0 \), and \( \sum_{t \in \mathbb{F}_q^*} \omega^\text{tr}(tx) = -1 \) for every \( x \in \mathbb{F}_q^* \), we obtain that
\[
\lambda_{(w_1,\ldots,w_{m+1})} = \left| \left\{ u \in \mathbb{F}_q \mid f(u) = 0 \right\} \right| (q-1) - \left| \left\{ u \in \mathbb{F}_q \mid f(u) \neq 0 \right\} \right|. \]
Let $B$ be the adjacency matrix of $H$. Then $N^T N = B + qI$; this fact can be seen easily by examining the on- and off-diagonal entries of both sides of the equation. Therefore, the eigenvalues of $W_m(q)$ can be written in the form

$$\pm \sqrt{\lambda(w_1, \ldots, w_{m+1}) + q},$$

where $(w_1, \ldots, w_{m+1}) \in \mathbb{F}^{m+1}$. Let $f(X) = w_1 + w_2 X + \cdots + w_{m+1} X^m \in \mathbb{F}_q[X]$. We consider two cases.

1. $f = 0$. In this case, $|\{u \in \mathbb{F}_q \mid f(u) = 0\}| = q$, and $\lambda(w_1, \ldots, w_{m+1}) = q(q-1)$. Thus, $W_m(q)$ has $\pm q$ as its eigenvalues.

2. $f \neq 0$. In this case, let $i = |\{u \in \mathbb{F}_q \mid f(u) = 0\}| \leq m$ as $1 \leq m \leq q-1$. This shows that $\lambda(w_1, \ldots, w_{m+1}) = i(q-1) - (q-i) = iq - q$ and implies that $\pm \sqrt{\lambda(w_1, \ldots, w_{m+1}) + q} = \pm \sqrt{iq}$ are eigenvalues of $W_m(q)$. Note that for any $0 \leq i \leq m$, there exists a polynomial $f$ over $\mathbb{F}_q$ of degree at most $m \leq q-1$, which has exactly $i$ distinct roots in $\mathbb{F}_q$. For such $f$, $|\{u \in \mathbb{F}_q \mid f(u) = 0\}| = i$, and, hence, there exists $(w_1, \ldots, w_{m+1}) \in \mathbb{F}_q^{m+1}$, such that $\lambda(w_1, \ldots, w_{m+1}) = iq - q$. Thus, $W_m(q)$ has $\pm \sqrt{iq}$ as its eigenvalues, for any $0 \leq i \leq m$, and the first statement of the theorem is proven.

The arguments above imply that the multiplicity of the eigenvalue $\pm \sqrt{iq}$ of $W_m(q)$ equals the number of polynomials of degree at most $m$ (not necessarily monic) having exactly $i$ distinct roots in $\mathbb{F}_q$. To calculate these multiplicities, we need the following lemma. Particular cases of the lemma were considered in Zsigmondy [26], and in Cohen [5]. The complete result appears in A. Knopfmacher and J. Knopfmacher [8].

**Lemma 2.2.** (See [8].) Let $q$ be a prime power, and let $d$ and $i$ be integers such that $0 \leq i \leq d \leq q-1$. Then the number $b(q, d, i)$ of monic polynomials in $\mathbb{F}_q[X]$ of degree $d$, having exactly $i$ distinct roots in $\mathbb{F}_q$ is given by

$$b(q, d, i) = \binom{q}{i} \sum_{k=0}^{d-i} (-1)^k \binom{q-i}{k} q^{d-i-k}.$$  \hspace{1cm} (8)

By **Lemma 2.2**, the number of polynomials of degree at most $m$ in $\mathbb{F}_q[X]$ (not necessarily monic) having exactly $i$ distinct roots in $\mathbb{F}_q$ is

$$\sum_{d=i}^{m} (q-1) b(q, d, i) = (q-1) \binom{q}{i} \sum_{d=i}^{m} \sum_{k=0}^{d-i} (-1)^k \binom{q-i}{k} q^{d-i-k}.$$  \hspace{1cm} (9)

This concludes the proof the theorem. \hspace{1cm} $\square$

The previous result shows that $W_m(q)$ is connected and has $2m+3$ distinct eigenvalues, for any $1 \leq m \leq q-1$. As the diameter of a graph is strictly less than the number of
distinct eigenvalues (see [4, Section 4.1] for example), this implies that the diameter of Wenger graph is less or equal to $2m + 2$. This is actually the exact value of the diameter of the Wenger graph as shown by Viglione [23].

Since the sum of multiplicities of all eigenvalues of the graph $W_m(q)$ is equal to its order, and remembering that the multiplicity of $\pm q$ is one when $1 \leq m \leq q - 1$, we have a combinatorial proof of the following identity.

**Corollary 2.3.** For every prime power $q$, and every $m$, $1 \leq m \leq q - 1$,

$$
\sum_{i=0}^{m} \binom{q}{i} \sum_{d=i}^{m} \sum_{k=0}^{d-i} (-1)^k \binom{q - i}{k} q^{d-i-k} = \frac{q^{m+1} - 1}{q - 1}.
$$

The identity (10) seems to hold for all integers $q \geq 3$, so a direct proof is desirable. Other identities can be obtained by taking the higher moments of the eigenvalues of $W_m(q)$.

As we discussed in the introduction, for $m \geq q$, the graph $W_m(q)$ has $q^{m-q+1}$ components, each isomorphic to $W_{q-1}(q)$. This, together with Theorem 2.1, immediately implies the following.

**Proposition 2.4.** For $m \geq q$, the distinct eigenvalues of $W_m(q)$ are

$$
\pm q, \pm \sqrt{(q - 1)q}, \pm \sqrt{(q - 2)q}, \ldots, \pm \sqrt{2q}, \pm \sqrt{q}, 0,
$$

and the multiplicity of the eigenvalue $\pm \sqrt{iq}$, $0 \leq i \leq q - 1$, is

$$(q - 1)q^{m+1-q} \binom{q}{i} \sum_{d=i}^{q} \sum_{k=0}^{d-i} (-1)^k \binom{q - i}{k} q^{d-i-k}.$$
NSF grant DMS-1106938-002. The authors thank Chris Godsil for some useful comments regarding the paper.

References