University of Ljubljana
Institute of Mathematics, Physics and Mechanics
Department of Mathematics
Jadranska 19, 1111 Ljubljana, Slovenia

Preprint series, Vol. 41 (2003), 880

RIGIDITY AND SEPARATION INDICES OF PALEY GRAPHS

Gašper Fijavž   Bojan Mohar

ISSN 1318-4865

May 29, 2003

Ljubljana, May 29, 2003

Rigidity and separation indices of Paley graphs

Gašper Fijavž [a,1] Bojan Mohar [b,1]

[a] *Faculty of Computer and Information Science, University of Ljubljana, SI-1000 Ljubljana, Slovenia*
email: `gasper.fijavz@fri.uni-lj.si`

[b] *Department of Mathematics, University of Ljubljana, SI-1000 Ljubljana, Slovenia*
email: `bojan.mohar@uni-lj.si`

Abstract

It is shown that the ratio between separation and rigidity indices of graphs may be arbitrarily large. Paley graphs are such examples.

Key words: rigidity index; separation index; Paley graph

1 Introduction

Let G be a (simple) graph. Let Γ be its (full) automorphism group with its natural action on $V(G)$, and let $\Gamma_v \leq \Gamma$ be the stabilizer of a vertex $v \in V(G)$. We say that a vertex set $S \subseteq V(G)$ *fixes* G if

$$\bigcap_{v \in S} \Gamma_v = \{\mathrm{id}\}. \tag{1}$$

If the automorphism group of G is trivial, then the empty set fixes G. The *rigidity index* of the graph G, denoted by $\mathrm{rig}(G)$, is the minimum cardinality of a vertex set fixing G.

For example, $\mathrm{rig}(K_n) = n-1$, $\mathrm{rig}(K_{m,n}) = m+n-2$, and $\mathrm{rig}(G) = \mathrm{rig}(\overline{G})$. If G is a 3-connected planar graph, then a set of three vertices lying consecutively

[1] Supported in part by the Ministry of Science and Technology of Slovenia, Research Project J1-0502-0101-00.

along a face fixes G. This implies that $\text{rig}(G) \leq 3$ for every 3-connected planar graph. It is proved in [3] that $\text{rig}(G)$ is bounded on the class of 4-connected projective planar graphs, and also, that for every surface Σ there exists an integer q_Σ, so that $\text{rig}(G) \leq q_\Sigma$ if G is 5-connected and admits an embedding in Σ.

Suppose we are given a set of automorphisms of G which generate Γ. We can compute Γ using the Schreier-Sims algorithm, and a set of vertices S fixing G is called a *base* of Γ [2, p. 18].

Let P_v denote the orbit partition of vertices of G induced by the action of Γ_v on $V(G)$. We say that a vertex set S *separates* G if

$$\bigwedge_{v \in S} P_v = 0, \tag{2}$$

where $\wedge$ denotes the *meet* operation in the lattice of all partitions of vertices of G and 0 is the partition into singletons. The *separation index* of a graph G, denoted by $\text{sep}(G)$, is the minimum cardinality of a set separating G. Similarly as above, $\text{sep}(G) = 0$ if the automorphism group of G is trivial.

Let S be a vertex set that separates G. Clearly, S also fixes G. Hence, $\text{rig}(G) \leq \text{sep}(G)$.

The separation index was first defined by Vince in [5], where he used a geometric argument to prove that $\text{sep}(G) \leq 3$ for 3-connected planar graphs.

It is easy to see that $\text{sep}(G) = 1$ is equivalent to $\text{rig}(G) = 1$. Vince mentioned in [5] that rigidity and separation indices are not the same on every graph, but no examples were provided. In this paper we show that for every integer k there exists a graph G with $\text{rig}(G) = 2$ and $\text{sep}(G) \geq k$. It is shown that Paley graphs give rise of such examples.

2 Results

Our main result is the following

Theorem 1 *For every integer k there exists a vertex-transitive graph G with* $\text{rig}(G) = 2$ *and* $\text{sep}(G) \geq k$.

The proof of Theorem 1 is a simple consequence of Proposition 2 and Theorem 3 stated below.

Choose a prime number $p = 4k + 1$. Denote by $\mathbb{Z}_p$ the set of integers modulo p and let $\mathbb{Q}_p = \{x^2 \mid 0 \neq x \in \mathbb{Z}_p\}$ be the set of all quadratic residues modulo

p. For notational clarity we also set $\overline{\mathbb{Q}_p} = \mathbb{Z}_p \setminus \mathbb{Q}_p \setminus \{0\}$. It is easy to see that $\mathbb{Q}_p$ is closed under multiplication and it is well known that $-1 \in \mathbb{Q}_p$.

The vertex set of the *Paley graph* G_p is $\mathbb{Z}_p$ in which vertices u and v are adjacent if $u - v \in \mathbb{Q}_p$. It is easy to see that automorphisms of G_p include multiplications by quadratic residues and translations. Muzychuk [4] proved that *every* automorphism of G_p is of the form $x \mapsto ax+b$ where $a \in \mathbb{Q}_p$ and $b \in \mathbb{Z}_p$. This implies that any automorphism π fixing 0 is merely a multiplication with a quadratic residue, and if also $\pi(1) = 1$, then $\pi = \mathrm{id}$. Therefore $\Gamma_0 \cap \Gamma_1 = \{\mathrm{id}\}$ and hence we have:

Proposition 2 *Rigidity index of the Paley graph G_p is equal to 2.*

Next we shall estimate the separation index of a Paley graph.

Theorem 3 *The following inequalities hold for the separation index of G_p:*

$$\lfloor \log_2 p \rfloor \leq \mathrm{sep}(G_p) \leq \lfloor 2 \log_2 p \rfloor.$$

Proof. It follows from the above discussion that $P_i = \{\{i\}, i + \mathbb{Q}_p, i + \overline{\mathbb{Q}_p}\}$ for every $i \in V(G_p)$. If U is a nonempty vertex subset of G_p then let P_U be the vertex partition defined as

$$P_U = \bigwedge_{v \in U} P_v.$$

Further, let m_r denote the maximum possible number of blocks in a partition P_U, taken over all vertex sets U of cardinality r. We will inductively show that

$$m_r \leq 2^{r+1} - 1. \tag{3}$$

This is obviously true if $r = 1$. For the induction step choose an arbitrary vertex set U' of cardinality $r+1$, and let $U = U' \setminus \{v\}$ be a proper subset of U'. Clearly, $\{v\}$ is a block of the partition $P_{U'} = P_U \wedge P_v$. By intersecting a typical element of P_U with $v + \mathbb{Q}_p$ and $v + \overline{\mathbb{Q}_p}$ we obtain at most *two* nonempty subsets which belong to $P_{U'}$. Hence, the numbers m_r satisfy the following recursion:

$$m_{r+1} \leq 2m_r + 1. \tag{4}$$

By applying the induction hypothesis we conclude that $m_{r+1} \leq 2^{r+2} - 1$. This completes the proof of (3).

Now, if a set U of cardinality k separates G_p, then $|P_U| \geq p$. Combining this fact with (3) gives the condition $2^{k+1} - 1 \geq p$. This implies that $k \geq \lceil \log_2(p+1) \rceil - 1$. Since $p \equiv 1 \pmod 4$, we conclude that $\log_2(p+1)$ is not an integer, hence $\lceil \log_2(p+1) \rceil - 1 = \lfloor \log_2 p \rfloor$. This completes the proof of the lower bound.

We prove the upper bound using the probabilistic method [1].

Let u and v be distinct vertices of G_p. We say that $s \in V(G_p)$ separates $\{u, v\}$ if u and v lie in different blocks of P_s. Obviously enough, both u and v separate $\{u, v\}$. A vertex $s \in V(G_p) \setminus \{u, v\}$ does not separate $\{u, v\}$ if and only if u and v are either both adjacent to s or both nonadjacent to s. This occurs if and only if

$$\frac{u-s}{v-s} = \frac{v-s-v+s+u-s}{v-s} = 1 + \frac{u-v}{v-s} \tag{5}$$

is a member of $\mathbb{Q}_p$ (all operations are considered in $\mathbb{Z}_p$). If s runs over all elements of $\mathbb{Z}_p \setminus \{u, v\}$, the expression in (5) runs over all elements of $\mathbb{Z}_p \setminus \{0, 1\}$, and exactly $(p-3)/2$ of these belong to $\mathbb{Q}_p$. Hence:

(1) *Let u and v be distinct vertices of G_p. Then exactly $\frac{p-3}{2}$ vertices of G_p do not separate u and v.*

Let $K = \lfloor 2 \log_2 p \rfloor$. Let $S = (s_1, s_2, \ldots, s_K)$ be a random vertex sequence of length K i.e., the vertex s_i is chosen randomly with uniform distribution, and independently from other choices, out of the set of all vertices of G_p. We say that the sequence S *separates* a vertex set U if the set $\{s_1, s_2, \ldots, s_K\}$ (which may have less than K elements) separates U.

Let $X_{u,v}$ $(u < v)$ be the random indicator variable of the event that a randomly chosen sequence S of length K does not separate $\{u, v\}$. By (1) we have

(2) $\Pr\Big[S \textit{ does not separate } \{u, v\}\Big] = E(X_{u,v}) = \left(\frac{p-3}{2p}\right)^K < \frac{1}{2^K}.$

Finally, let X denote the random variable which counts the number of (unordered) pairs of distinct vertices which are not separated by a random vertex-sequence S. By linearity of expectation we have

(3) $E(X) = \sum_{u<v} E(X_{u,v}) < p^2 \frac{1}{2^{K+1}}.$

Now $K+1 \geq 2 \log_2 p$ implies that $E(X) < 1$. Therefore there exists a sequence of length K (and a set of cardinality at most K) separating G. This completes the proof. □

3 Open problems

Problem 4 *Is it true that already powers of 2 separate Paley graphs? In other words, does the set $\{1, 2, 2^2, \ldots, 2^{\lfloor \log_2 p \rfloor}\}$ separate G_p?*

It is reasonable to expect that Paley graphs attain the maximum possible ratio between separation and rigidity indices. In fact, we propose the following:

Conjecture 5 *Let G be a graph of order n such that* $\text{rig}(G) > 0$. *Then*

$$\text{sep}(G) \,/\, \text{rig}(G) = O(\log n).$$

Let us observe that the difference $\text{sep}(G) - \text{rig}(G)$ can be much larger. Its order can be proportional to n. Such examples are obtained by taking many copies of a fixed graph G_0 whose separation and rigidity indices are different (and then taking the complement if we want the resulting graph to be connected).

Acknowledgement

G. F.'s research was conducted while visiting University of Hannover under sponsorship of Alexander von Humboldt Foundation. Both hospitality of the university and help of the foundation are greatly acknowledged.

References

[1] N. Alon, J. H. Spencer, P. Erdős, *The Probabilistic Method*, Wiley Interscience, New York, 1992.

[2] P. J. Cameron, *Permutation Groups*, Cambridge University Press, Cambridge, 1999.

[3] G. Fijavž, B. Mohar, *Separation and rigidity index of graphs on surfaces*, in preparation.

[4] M. E. Muzychuk, *Automorphism group of a Paley graph* (in Russian), Vopr. Teor. Grupp Gomologicheskoj Algebry **7** (1987), 64–69.

[5] A. Vince, *Separation index of a graph*, J. Graph Theory **41** (2002), 53–61.