On the spectrum of projective norm-graphs

Tibor Szabó [*]

Abstract

We show that the projective norm-graphs of [4] are pseudorandom in the sense that their second eigenvalue is as small as the square root of the degree. Our approach is simple, it only uses the evaluation of Gaussian sums and determines the complete spectrum exactly.

Keywords: pseudorandom graph, projective norm-graph, Gaussian sum

1 Introduction

Ever since randomness was introduced in Theoretical Computer Science, great efforts have also been made for its elimination. Whenever a random graph is utilized to perform an algorithmic task efficiently, but random bits are expensive or a deterministic answer would simply be more desirable, the need for a replacement arises. This demand is one of the main motivations behind the interest in explicit constructions of families of *pseudorandom graphs.* Pseudorandom graphs possess certain random-like properties and can, in some cases, serve as substitutes of truly random graphs.

There are several different ways to understand and define the pseudorandomness of a graph. Here we consider the one through the second eigenvalue, which is linked strongly to the graph's *edge distribution* and *expansion properties*; both crucial concepts for applications in Computer Science (see [6, Chapter 9] for more details). Given a graph G, let $\lambda_1 \geq \lambda_2 \geq \dots \lambda_n$ be the eigenvalues of its adjacency matrix. The *second eigenvalue* of G is defined to be $\lambda = \lambda(G) = \max\{\lambda_2, |\lambda_n|\}$. It is easy to see that for d-regular graphs $\lambda_1 = d$. Graphs whose second eigenvalue is smaller order than the largest one possess some properties of random graphs with appropriate edge probability. The larger this "spectral gap" is the more randomness the graph has [6]. As the second eigenvalue of any graph (of maximum degree at most $n/2$) is at least the square root of the degree up to a constant factor, graphs with $\lambda(G) = \Theta(\sqrt{\lambda_1})$ are of particular interest.

The projective norm-graphs [4] and their predecessors, the norm-graphs [9] were introduced to provide tight bounds (up to a constant factor) for the Zarankiewicz problem, i.e. for the

[*] Department of Computer Science, ETH Zürich, 8092 Switzerland. Email address: szabo@inf.ethz.ch. Research supported in part by NSF grant DMS 99-70270 and by the joint Berlin/Zurich graduate program Combinatorics, Geometry, Computation, financed by the German Science Foundation (DFG) and ETH Zürich.

maximum number of edges in a $K_{t,s}$-free graph. Recently they appeared in several other explicit constructions for a wide variety of Turán- and Ramsey-type problems [3, 5, 7, 10]. They also found application in Theoretical Computer Science providing superpolynomial lower bounds for monotone span programs [8].

In this short note we determine the spectrum of projective norm-graphs. We notice that all eigenvalues are (possibly signed) Gaussian sums, hence can be calculated precisely. We find that the second eigenvalue is asymptotically the square root of the degree, thus the projective norm-graphs are as pseudorandom as it gets. In Corollary 1 we obtain the multiplicities of all eigenvalues. Estimation of the eigenvalues of algebraically defined graphs is often hard or applies deep theorems of Algebra or Algebraic Geometry. Besides, these techniques rarely give the precise answer. Our treatment is elementary, uses only basic facts about groups and fields while providing the exact values.

Our result has already got an application in Ramsey-theory. Alon and Rödl [5] obtained Theorem 1 independently and used the second eigenvalue to bound the number of independent sets in projective norm-graphs. Through this they provide surprisingly precise answers about asymmetric multicolor Ramsey numbers of complete bipartite graphs.

2 The eigenvalues

Let q be the power of an odd prime, $t > 1$ be an arbitrary integer and denote by $GF(q)$ the finite field with q elements. The projective norm-graph $G = G_{q,t}$ is defined as follows. The vertex set $V(G)$ is the direct product $GF(q^{t-1}) \times GF(q)^*$, where $GF(q)^* = GF(q) \setminus \{0\}$ refers to the multiplicative group of $GF(q)$. A vertex (A, a) is adjacent to (B, b) if and only if $N(A + B) = ab$, where $N : GF(q^{t-1}) \longrightarrow GF(q)$ is the usual norm function, i.e. $N(X) = X^{(q^{t-1}-1)/(q-1)}$.

$G_{q,t}$ has $n := q^{t-1}(q-1)$ vertices. For any fixed $(A, a) \in V(G_{q,t})$ and any $B \in GF(q^{t-1})$, $B \neq -A$, there is a unique $b \in GF(q)^*$ such that (A, a) is adjacent to (B, b) in $G_{q,t}$. Hence $G_{q,t}$ is $q^{t-1} - 1 \approx n^{1-1/t}$-regular. Based on some tools from algebraic geometry [9] it was shown in [4] that $G_{q,t}$ is $K_{t,(t-1)!+1}$-free.

Theorem 1 *The largest eigenvalue of $G_{q,t}$ is $q^{t-1} - 1$. All other eigenvalues are $\pm q^{(t-1)/2}, \pm 1$ or 0.*

Proof. Let M be the adjacency matrix of $G_{q,t}$. Let χ be an arbitrary additive character of $GF(q^{t-1})$ and ϕ be an arbitrary multiplicative character of $GF(q)^*$. Let (χ, ϕ) denote the column vector whose coordinates are labeled by the elements of $V(G)$, and whose entry at the coordinate (A, a) is $\chi(A)\phi(a)$.

Then the entry of the vector $M(\chi, \phi)$ at the coordinate (A, a) is

$$\sum_{\substack{B \in GF(q^{t-1}) \\ b \in GF(q)^* \\ N(A+B)=ab}} \chi(B)\phi(b) = \sum_{\substack{B \in GF(q^{t-1}) \\ B \neq -A}} \chi(B)\phi\left(\frac{N(A+B)}{a}\right) = \sum_{\substack{C \in GF(q^{t-1}) \\ C \neq 0}} \chi(C-A)\phi\left(\frac{N(C)}{a}\right) =$$

$$= \sum_{\substack{C \in GF(q^{t-1}) \\ C \neq 0}} \chi(C)\phi(N(C))\overline{\chi(A)\phi(a)}$$

So

$$M(\chi, \phi) = \sum_{\substack{C \in GF(q^{t-1}) \\ C \neq 0}} \chi(C)\phi(N(C))(\overline{\chi}, \overline{\phi}). \tag{1}$$

Applying M once more we obtain that (χ, ϕ) is an eigenvector of M^2. Moreover all eigenvectors are of this form as they are orthogonal and the number of characters of a group is equal to its order. So all eigenvalues of M^2 are of the form

$$|\sum_{\substack{C \in GF(q^{t-1}) \\ C \neq 0}} \chi(C)\phi(N(C))|^2.$$

The eigenvalues of M^2 are the squares of the eigenvalues of M. These are reals, as M is symmetric. So all eigenvalues of M are of the form

$$\pm|\sum_{\substack{C \in GF(q^{t-1}) \\ C \neq 0}} \chi(C)\phi(N(C))|.$$

When $\chi = \chi_0$ and $\phi = \phi_0$ are the principal characters of their respective groups, then the corresponding eigenvalue is $q^{t-1} - 1$. (No surprise, as this is the degree of G.)

When $\chi = \chi_0$, but $\phi \neq \phi_0$, then the corresponding eigenvalues are

$$\pm|\sum_{\substack{C \in GF(q^{t-1}) \\ C \neq 0}} \phi(N(C))| = \pm|\frac{q^{t-1}-1}{q-1} \sum_{c \in GF(q)^*} \phi(c)| = 0.$$

When $\chi \neq \chi_0$, but $\phi = \phi_0$, then the corresponding eigenvalues are

$$\pm|\sum_{\substack{C \in GF(q^{t-1}) \\ C \neq 0}} \chi(C)| = \pm 1.$$

When neither χ nor ϕ is a principal character, then we can apply the well-known estimates on Gaussian sums (see for example [11, Theorem 3A, page 47]). For this, we just need to observe that ϕN is a multiplicative character of $GF(q^{t-1})$.

$$|\sum_{\substack{C \in GF(q^{t-1}) \\ C \neq 0}} \chi(C)\phi(N(C))| = q^{(t-1)/2}.$$

□

In an earlier version of this note the multiplicities of the eigenvalues were determined for even t and non-square q using the trace of M and the irrationality of $q^{(t-1)/2}$. Dhruv Mubayi pointed out that the multiplicities can be determined for *all* values of the parameters if, instead of the irrationality argument, one observes that the eigenvectors of M corresponding to eigenvalues $+1$ and -1 are of the form $(\chi, \phi_0) - (\overline{\chi}, \phi_0)$ and $(\chi, \phi_0) + (\overline{\chi}, \phi_0)$, respectively.

Corollary 1 *Assume that q is the power of an odd prime. Then the eigenvalues of $G_{q,t}$ have the following multiplicities: $q^{t-1}-1$ is of multiplicity 1, 0 is of multiplicity $q-2$, 1 and -1 are both of multiplicity $(q^{t-1}-1)/2$, while $q^{(t-1)/2}$ and $-q^{(t-1)/2}$ are both of multiplicity $(q^{t-1}-1)(q-2)/2$.*

Proof. It follows easily from (1) that $(\chi, \phi_0) - (\overline{\chi}, \phi_0)$ is an eigenvector of M with eigenvalue $+1$ and $(\chi, \phi_0) + (\overline{\chi}, \phi_0)$ is an eigenvector with eigenvalue -1 for any character $\chi \neq \chi_0$. This immediately implies that the multiplicities of both eigenvalues $+1$ and -1 are $(q^{t-1}-1)/2$. The multiplicity m of eigenvalue $q^{(t-1)/2}$ can then be obtained by calculating the trace of M.

By definition, the projective norm-graph has a loop at vertex (A, a) iff $N(2A) = a^2$. Since exactly $(q-1)/2$ elements of $GF(q)^*$ are squares and the equation $N(X) = y$ has $(q^{t-1}-1)/(q-1)$ solutions in X for each $y \in GF(q)^*$, there are $(q^{t-1}-1)/2$ elements $A \in GF(q^{t-1})$ with $N(2A)$ being a square. Once $N(2A)$ is a square, there are two distinct elements $a, a' \in GF(q)^*$ with $N(2A) = a^2 = a'^2$. Thus $G_{q,t}$ contains $q^{t-1}-1$ loops, so the trace of M is $q^{t-1}-1$. Hence

$$q^{t-1}-1 = TrM = \sum_{i=1}^{q^{t-1}(q-1)} \lambda_i = q^{t-1}-1 + \frac{q^{t-1}-1}{2} - \frac{q^{t-1}-1}{2} + q^{(t-1)/2}(2m - (q^{t-1}-1)(q-2)),$$

which implies that the multiplicity m is $(q^{t-1}-1)(q-2)/2$.

□

Remark. Alon [1] proved that the C_4-free Erdős-Rényi graphs on n vertices have independence number at most $2n^{3/4}$ (which can actually be improved to $n^{3/4}(1+o(1))$; [2]). This represents the best known *constructive* lower bound for the Ramsey number $r(C_4, K_n)$. A referee pointed out that via Theorem 1 the projective norm-graphs provide an *alternative* construction with similar parameters.

Acknowledgment. I would like to thank the referees for their insightful comments. I am grateful to Dhruv Mubayi who extended the statement of Corollary 1 for all values of the parameters.

References

[1] N. Alon, Eigenvalues, geometric expanders, sorting in rounds, and Ramsey theory, *Combinatorica* **6** (1986), 207-219.

[2] N. Alon, M. Krivelevich, Constructive bounds for a Ramsey-type problem *Graphs and Combinatorics* **13** (1997), 217-225.

[3] N. Alon, P. Pudlák, Constructive lower bounds for off-diagonal Ramsey numbers, *Israel J. Math.* **122** (2001), 243-251.

[4] N. Alon, L. Rónyai, T. Szabó, Norm-graphs: variations and applications, *J. Combinatorial Theory, Ser. B* 76 (1999), 280-290.

[5] N. Alon, V. Rödl, Asymptotically tight bounds for some multicolored Ramsey numbers, *submitted*

[6] N. Alon, J.H. Spencer, *The Probabilistic Method,* Wiley, 1992.

[7] M. Axenovich, Z. Füredi, D. Mubayi, On generalized Ramsey theory: the bipartite case, *J. Combin. Theory (Ser. B)* **79** (2000), no. 1, 66–86.

[8] L. Babai, A. Gál, J. Kollár, L. Rónyai, T. Szabó, A. Wigderson, Extremal Bipartite Graphs and Superpolynomial Lower Bounds for Monotone Span Programs *Proc. of the twenty-eighth Annual ACM Symposium on the Theory of Computing (STOC)*, (1996), 603-611.

[9] J. Kollár, L. Rónyai, T. Szabó, Norm-graphs and bipartite Turán numbers, *Combinatorica* **16** (1996), 399-406.

[10] D. Mubayi, Some exact results and new asymptotics for hypergraph Turán numbers, *Combin. Probab. Comput.* **11** (2002), no.3, 299-309.

[11] W.G. Schmidt, *Equations over Finite Fields, An Elementary Approach,* Springer LNM 536, 1976.