JOURNAL OF COMBINATORIAL THEORY, Series B 49, 190–194 (1990)

Note on the Girth of Ramanujan Graphs

N. L. BIGGS AND A. G. BOSHIER

London School of Economics, Houghton Street, London WC2A 2AE, England

Communicated by the Editors

Received June 25, 1987

The purpose of this note is to establish an upper bound for the girth of the Ramanujan graphs constructed by Lubozky, Phillips, and Sarnak, thereby determining the asymptotic behaviour of the girth of these graphs.

1. INTRODUCTION

Let G be a finite k-regular graph. Then G is called a Ramanujan graph if all its eigenvalues (other than $\pm k$) have modulus at most $2\sqrt{(k-1)}$. Families of such graphs provide very good enlargers which can be used to construct good expanders and superconcentrators (see [2, 4] for a fuller discussion of these matters). It was therefore of some significance when Lubotzky, Phillips, and Sarnak [3] were able to present an explicit construction of infinite families of Ramanujan graphs. In fact their construction is isomorphic to some cases of a construction already given by Margulis in 1984 (see [5]).

The Ramanujan graphs so constructed are of added interest in that they have large girth. In particular, for infinitely many values of k there is a family of k-regular graphs whose order n and girth g satisfy asymptotically $g \geqslant \frac{4}{3}\log_{k-1} n$, which gives a value of the parameter

$$c = (\log_{k-1} n)/g$$

of at most 3/4. This is smaller than all previous explicit or nonexplicit constructions, with the single exception of the sextet graphs [1, 6] which yield the same bound in the case $k = 3$. The purpose of this note is to show that, in fact, the asymptotic value of c for the LPS graphs is exactly 3/4, by providing a suitable upper bound for the girth.

0095-8956/90 $3.00

2. Construction of the Ramanujan Graphs $X^{p,q}$

Let p be a prime congruent to 1 modulo 4, and let $H(\mathbf{Z})$ denote the integral quaternions

$$H(\mathbf{Z}) = \{\alpha = a_0 + a_1 i + a_2 j + a_3 k \mid a_j \in \mathbf{Z}\}.$$

Let $\bar{\alpha} = a_0 - a_1 i - a_2 j - a_3 k$ and $N(\alpha) = \alpha\bar{\alpha}$. It can be shown that there are precisely $(p+1)/2$ conjugate pairs $\{\alpha, \bar{\alpha}\}$ of elements of $H(\mathbf{Z})$ satisfying $N(\alpha) = p$, $\alpha \equiv 1 \pmod 2$ and $a_0 > 0$. Denote by S the set of all such elements, and define $\Lambda'(2)$ to be the set of all $\alpha \in H(\mathbf{Z})$ with $\alpha \equiv 1 \pmod 2$ and $N(\alpha) = p^v$ for some non-negative $v \in \mathbf{Z}$. If $\Lambda(2)$ is the set of equivalence classes obtained from $\Lambda'(2)$ by identifying $\alpha, \beta \in \Lambda'(2)$ whenever $\pm p^{v_1}\alpha = p^{v_2}\beta$ for some non-negative $v_1, v_2 \in \mathbf{Z}$, then it is shown in [3] that the Cayley graph of $\Lambda(2)$ with respect to S is the infinite $(p+1)$-regular tree.

Now let q be another prime congruent to 1 modulo 4, satisfying $q > \sqrt{p}$ and $(p/q) = -1$. The normal subgroup $\Lambda(2q)$ of $\Lambda(2)$ is defined by

$$\Lambda(2q) = \{[\alpha] \in \Lambda(2) \mid 2q \text{ divides } a_j, j = 1, 2, 3\},$$

where $[\alpha]$ denotes the equivalence class of α. If $X^{p,q}$ is defined to be the Cayley graph of $\Lambda(2)/\Lambda(2q)$ with respect to $S/\Lambda(2q)$, then it is proved in [3] that $X^{p,q}$ is a $(p+1)$-regular bipartite Ramanujan graph of order $q(q^2-1)$ and girth

$$g(X^{p,q}) \geqslant 4 \log_p q - \log_p 4.$$

In the next section we show how to find an upper bound for the quantity $g(X^{p,q})$.

3. An Upper Bound for $g(X^{p,q})$

Since $X^{p,q}$ is a Cayley graph, and hence vertex-transitive, its girth is simply the minimum distance from the identity to a non-trivial element of $\Lambda(2q)$ in the infinite tree on $\Lambda(2)$. (In the future we shall say that an element of $\Lambda(2)$ is at level r if it is at distance r from the identity in the tree on $\Lambda(2)$). Since $(p/q) = -1$ this minimum distance is necessarily even.

Lemma 1. *If $[b] \in \Lambda(2q)$ is at level $2r$ for $r > 0$, then b can be chosen so that*

$$b_0 = \pm(p^r - mq^2),$$

where $m > 0$ is even.

Proof. If such a b exists then $N(b^2) = p^{2r}$ and

$$b = b_0 + 2qb_1 i + 2qb_2 j + 2qb_3 k$$

so that $b_0^2 \equiv p^{2r} \pmod{q^2}$. But the group $(\mathbf{Z}/q^2\mathbf{Z})^*$ is cyclic, so we deduce that

$$b_0 \equiv \pm p^r \qquad (\mathrm{mod}\ q^2).$$

Since $r > 0$ we have $b_0 \neq \pm p^r$ and, mindful of the fact that $|b_0| \leqslant p^r$ and b_0 is odd, we have the required result.

We recall Legendre's theorem on sums of three squares, which states that a positive integer is the sum of three (or fewer) squares if and only if it is not of the form $4^\alpha(8\beta + 7)$, for some non-negative integers α and β. We shall call any positive integer not of this form "good."

LEMMA 2. *There is a* $[b] \in \Lambda(2q)$ *at level* $2r$ *with* $b_0 = p^r - mq^2$ *(where* m *is even and positive) if and only if* $2mp^r - m^2q^2$ *is good. (Note that good entails positive, so the condition ensures that* $2p^r > mq^2$*, that is,* $p^r - mq^2 > -p^r$*, so that* b_0 *is in the correct range.)*

Proof. If such a $[b]$ exists then

$$p^{2r} = (p^r - mq^2)^2 + 4q^2(b_1^2 + b_2^2 + b_3^2)$$

which reduces to

$$2mp^r - m^2q^2 = 4(b_1^2 + b_2^2 + b_3^2)$$

so that $2mp^r - m^2q^2$ is good, as required.

Conversely, if $2mp^r - m^2q^2$ is good then, since m is even, we have $2mp^r - m^2q^2 \equiv 0 \pmod 4$. Consequently $2mp^r - m^2q^2$ is the sum of three even squares, so that we may write

$$2mp^r - m^2q^2 = 4(b_1^2 + b_2^2 + b_3^2)$$

which implies that

$$p^{2r} = (p^r - mq^2)^2 + 4q^2(b_1^2 + b_2^2 + b_3^2).$$

Hence if $b = (p^r - mq^2) + 2qb_1 i + 2qb_2 j + 2bq_3 k$ then $[b] \in \Lambda(2q)$ is at level $2r$, which completes the proof.

THEOREM. *If* $(p/q) = -1$ *then*

$$4\log_p q - \log_p 4 \leqslant g(X^{p,q}) < 4\log_p q + \log_p 4 + 2.$$

Proof. We show first that at least one of the integers $2mp^r - m^2q^2$ ($m = 2, 4$) is good, provided that they are both positive. Suppose that the case $m = 2$ is bad, that is, $4(p^r - q^2)$, and hence $p^r - q^2$, is bad (that is, not good). Then $p^r - q^2 = 4^\alpha(8\beta + 7)$ so that the $m = 4$ case gives $8p^r - 16q^2$ with

$$\begin{aligned} 8p^r - 16q^2 &= 8(p^r - q^2) - 8q^2 \\ &= 8(4^\alpha(8\beta + 7) - q^2). \end{aligned}$$

Since $\alpha \geqslant 1$ (because $p^r, q^2 \equiv 1 \pmod 4$), it follows that the term inside the outer brackets is odd, so that $8p^r - 16q^2$ is certainly good.

So let r_0 be the least integer r for which $p^r > 2q^2$ (note that $4p^r - 4q^2$ and $8p^r - 16q^2$ are then both positive). Then

$$p^{r_0 - 1} < 2q^2 \Rightarrow r_0 < 2 \log_p q + \log_p 2 + 1.$$

By the above, there exists $[b] \in \Lambda(2q)$ at level $2r_0$, so that

$$g(X^{p,q}) \leqslant 2r_0 < 4 \log_p q + \log_p 4 + 2$$

as required. The lower bound for $g(X^{p,q})$ is established in [3]. This completes the proof.

COROLLARY. *Let $p, q \equiv 1 \pmod 4$ be unequal primes satisfying $q > \sqrt{p}$ and $(p/q) = -1$. Then the asymptotic value of $c_{p,q} = (\log_p q(q^2 - 1))/g(X^{p,q})$ as $q \to \infty$ is* 3/4.

Proof. Immediate from the Theorem.

The result of the Theorem establishes the value of $g(X^{p,q})$ almost exactly for all practical purposes, since $g(X^{p,q})$ must be an even integer lying in the interval

$$[4 \log_p q - \log_p 4, 4 \log_p q + \log_p 4 + 2)$$

whose length is $2 + \log_p 16$. For $p \geqslant 5$ this interval contains at most two even numbers, and in most cases only one, thus determining $g(X^{p,q})$ exactly.

In fact, a minor reformulation of the analysis, based on Lemma 2, yields the following exact result, where $x(q) = \lceil 2 \log_p q \rceil$. If $p^{x(q)} - q^2$ is good, then $g(X^{p,q}) = 2x(q)$; otherwise $g(X^{p,q}) = 2\lceil 2 \log_p q + \log_p 2 \rceil$. The authors are grateful to one of the referees for pointing out this formulation, and for drawing attention to the fact that Margulis (May 1987) has also obtained an exact formula for his more general construction.

REFERENCES

1. N. L. BIGGS AND M. J. HOARE, The sextet construction for cubic graphs, *Combinatorica* **3** (1983), 153–165.
2. O. GABBER AND Z. GALIL, Explicit constructions of linear-sized superconcentrators, *J. Comput. System Sci.* **22** (1981), 407–420.
3. A. LUBOTZKY, R. PHILLIPS, AND P. SARNAK, Ramanujan graphs, *Combinatorica* **8** (1988), 261–277.
4. A. LUBOTZKY, R. PHILLIPS, AND P. SARNAK, Ramanujan conjecture and explicit construction of expanders, *Proc. STOC* **86** (1986), 240–246.
5. G. A. MARGULIS, Arithmetic groups and graphs without short cycles. *Problems Inform. Transmission*, in press.
6. A. WEISS, Girths of bipartite sextet graphs, *Combinatorica* **4**, Nos. 2–3 (1984), 241–245.