数理解析研究所講究録
第1811巻 2012年 130-134

New constructions of graphs with large girth obtained from "classical" ones

Xavier Dahan*
Faculty of mathematics, Kyûshû university, Japan
dahan@math.kyushu-u.ac.jp

Abstract

This short note surveys some new and not so new constructions of infinite families of constant degree regular graphs with large girth. Many of these families are constructed as follows: interpret algebraically the infinite d-regular tree as a Cayley graph on a relevant free group defined over $\mathbb{Z}$. Take finite quotients of this tree realized as Cayley graphs on groups defined by taking projections $\mathbb{Z} \to \mathbb{F}_q$ of this free group, for an infinite set of primes q. For these families, the finite quotients are Cayley graphs over $GL_2(\mathbb{F}_q)$, $SL_2(\mathbb{F}_q)$ or $PGL_2(\mathbb{F}_q)$, $PSL_2(\mathbb{F}_q)$. We highlight the use of quaternion groups, allowing to obtain new constructions of regular graphs displaying a girth larger than what were able to achieve some "classical" constructions.

1 Introduction

The *girth* of a graph is the length of one of its shortest cycle. For large graphs, it is difficult to compute, and a natural question raises: how large the girth of a graph with N vertices can be ? This very general question is not trivial as soon as there are some vertices of degree of regularity greater than 2 (otherwise it is a cycle graph which have girth equal to N). If one restricts the kind of graphs to *regular graphs*, this question has a more precise signification, due to an upper bound found out by Moore. This "Moore bound" is a simple counting observation that can be summed up as follows. In a regular graph of girth $g := \mathrm{girth}(G)$, the set of vertices at distance less than t from a given vertex (the root) is a regular tree, assuming that $t \leq \lfloor \frac{g}{2} \rfloor$ (g is odd) or $t < \frac{g}{2}$ (g is even). It follows that:

$$g \leq \begin{cases} 2\log_{d-1}|G| + 1 & \text{if } g \text{ is } \textit{odd}, \\ 2\log_{d-1}|G| + 2 - 2\log_{d-1} 2 & \text{if } g \text{ is } \textit{even}. \end{cases} \tag{1}$$

This implies that for $d \geq 5$,

$$g \leq (2 + \frac{2}{\log_{d-1}|G|}) \log_{d-1}|G| = (2 + o(1)) \log_{d-1}|G| \tag{2}$$

Consequently given a family of d-regular graphs $(G_n)_{n\in\mathbb{N}}$,

$$\liminf_{n\to\infty} \frac{\mathrm{girth}(G_n)}{\log_{d-1}|G_n|} \leq 2.$$

*Supported by the GCOE project "Maths-for-Industry" of Kyûshû university

This motivates the following definition due to Biggs [1]. A family of d-regular graphs is said to be of *large girth* if $\liminf_{n\to\infty} \frac{\text{girth}(G_n)}{\log_{d-1}|G_n|} \geq \epsilon$ for some $\epsilon > 0$.

Application. The property of large girth, besides its own theoretical interest, finds an application in error-correcting codes theory, and more precisely for "Low Density Parity Check" (LDPC) codes. This approach was pioneered by Margulis in [10], where he gave the first constructive example of a family of LDPC codes of unbounded minimum distance by providing explicit families of regular graphs of large girth. Such a property is quite useful in this context for several reasons:
(i) Tanner gave in [14] a construction of codes based on graphs together with a lower bound on the code minimum distance growing exponentially with the girth;
(ii) these LDPC codes are decoded with the help of iterative decoding algorithms working on a certain graph associated to the code construction and the performance of such algorithms is known to deteriorate in the presence of small cycles. This phenomenon is related to the fact that these iterative decoding algorithms compute symbol probabilities conditioned on an exponentially large (in the number of iterations) number of received symbols as long as the number of iterations is smaller than half the girth [5], but that does not hold anymore for a larger number of iterations.

This motivates the construction of graphs with the largest girth possible. Define:

$$\gamma(\{G_n\}) := \liminf_{n\to\infty} \frac{\text{girth}(G_n)}{\log_{d-1}|G_n|}. \tag{3}$$

We wish to determine for each integer $d \geq 3$ the constant

$$\gamma_d := \sup_{\{G_n\}_{n\in\mathbb{N}} \text{ family of } d\text{-regular graphs}} \gamma(\{G_n\}).$$

The Moore bound (2) implies that $\gamma_d \leq 2$ for all $d \geq 3$. Lower bounds can be found in several works. Here is a non exhaustive list, written in chronological order:

	authors	degree d	$\gamma_d \geq$	explicit ?
1	Erdös & Sachs [4]	≥ 3	1	no
2	Margulis [10]	≥ 3, even	4/9	yes
		4	8/9	yes
3	Weiss [15]	3	4/3	yes
4	Imrich [7]	any	0.48	yes
5	LPS [9]	$p+1$, $p \equiv 1 \bmod 4$ prime	4/3	yes
6	Margulis [10]	$p+1$, p any odd prime	4/3	yes
7	Chiu [2]	3	4/3	yes
8	Morgenstern [12]	p^k+1, p odd prime $k \in \mathbb{N}^\star$	4/3	yes
		2^k+1 ,$k \in \mathbb{N}^\star$	2/3	yes
9	Lazeb.& Ustim. [8]	p^k+1, p prime, $k \in \mathbb{N}^\star$	4/3	yes
10	see [3]	see Table 2	see Table 2	yes

Table 1: Old and new results about graphs with large girth

Except the graphs in [15, 8] all these families of graphs are defined as *Cayley graphs* on the groups $GL_2(\mathbb{F}_q)$, $SL_2(\mathbb{F}_q)$ or their projective counterparts $PGL_2(\mathbb{F}_q)$ or $PSL_2(\mathbb{F}_q)$. In this survey, we will focus on the constructions in [9, 11] and especially on how to modify these to obtain the graphs in [3] that display a larger girth than what previously known for many special cases.

2 The LPS-Margulis construction

These are the famous *Ramanujan graphs* that are optimal expanders [6] with respect to the eigenvalue bound. These can be defined using quaternions due to a well-known isomorphism between the "Hamilton" quaternion algebra $\mathbb{H}(\mathbb{F}_q)$ over the finite field with q elements,

$$\mathbb{H}(\mathbb{F}_q) := \{x_0 + x_1\mathsf{i} + x_2\mathsf{j} + x_3\mathsf{k},\ x_i \in \mathbb{F}_q\},\ \text{where}\ \mathsf{i}^2 = \mathsf{j}^2 = -1,\ \mathsf{ij} = \mathsf{k}$$

and the 2x2 matrix algebra over $\mathbb{F}_q$. In particular, denoting $\mathbb{H}^1(\mathbb{F}_q) := \{x = x_0+x_1\mathsf{i}+x_2\mathsf{j}+x_3\mathsf{k} \in \mathbb{H}(\mathbb{F}_q) \mid N(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1\}$, and $\mathcal{Z} := \{x = \overline{x} := 2x_0 - x,\ x \in \mathbb{H}(\mathbb{F}_q)^\times\}$ the center group of $\mathbb{H}(\mathbb{F}_q)^\times$, holds:

$$\mathbb{H}(\mathbb{F}_q)^\times/\mathcal{Z} \simeq PGL_2(\mathbb{F}_q) \qquad \text{and} \qquad \mathbb{H}^1(\mathbb{F}_q)/\{\pm 1\} \simeq PSL_2(\mathbb{F}_q).$$

Following a famous theorem of Jacobi, every prime integer p can be written in $8(p+1)$ different ways as the sum of the squares of 4 integers. Consequently there are in $\mathbb{H}(\mathbb{Z})$ $8(p+1)$ quaternions of norm p. The group of invertible quaternions $\mathbb{H}(\mathbb{Z})^\times$ over $\mathbb{Z}$ has exactly 8 elements, and this group acts naturally on the set of quaternions of norm p. If we isolate one quaternion per orbit under this action, this defines a special set $\mathscr{P}(p)$ of $p+1$ quaternions of norm p, and a quite natural way to achieve this is the following:

$$\mathscr{P}(p) = \{\pi \in \mathbb{H}(\mathbb{Z}) \text{ primitive}:\ N(\pi) = p,\ \pi_0 > 0,\ \pi - 1 \in 2\mathbb{H}(\mathbb{Z})\} \qquad \text{if } p \equiv 1 \mod 4, \quad (4)$$

$$\mathscr{P}(p) = \{\pi \in \mathbb{H}(\mathbb{Z}) \text{ primitive}:\ N(\pi) = p,\ \pi_0 > 0 \text{ if } \pi_0 \neq 0, \quad \text{or} \quad \pi_1 > 0 \text{ if } \pi_0 = 0, \quad \text{and} \quad \pi - \mathsf{i} - \mathsf{j} - \mathsf{k} \in 2\mathbb{H}(\mathbb{Z})\} \qquad \text{if } p \equiv 3 \mod 4 \quad (5)$$

For each prime $q > p$, define $\mathscr{S}_{p,q}$ the image of $\mathscr{P}(p) \subset \mathbb{H}(\mathbb{Z})$ in $\mathbb{H}(\mathbb{F}_q)^\star/\mathcal{Z}$ and let $X_{p,q} := \mathscr{C}ay(\mathbb{H}^1(\mathbb{F}_q)/\{\pm 1\}, \mathscr{S}_{p,q})$ if $\left(\frac{p}{q}\right) = 1$ or $X_{p,q} := \mathscr{C}ay(\mathbb{H}(\mathbb{F}_q)^\times/\mathcal{Z}, \mathscr{S}_{p,q})$ if $\left(\frac{p}{q}\right) = -1$. These are the Ramanujan graphs of [9, 11]. They are $p+1$-regular, connected graphs, bipartite if $\left(\frac{p}{q}\right) = -1$ and not bipartite otherwise, and have the following remarkable property: let $\lambda(X_{p,q})$ be the second largest eigenvalue of the adjacency matrix of $X_{p,q}$. It verifies $\lambda(X_{p,q}) \leq 2\sqrt{p}$, which for large graphs is essentially the lowest possible. The construction of this kind of graphs reaching the optimal lower bound was quite a breakthrough in graph theory. Besides this "spectral" property, these graphs also have large girth, with the result mentioned in Table 1.

3 Modification of the construction

The LPS graphs and its later generalization by Morgenstern yields $\gamma_d \geq 4/3$ for $d = p^k + 1$ and $\gamma_{2^k+1} \geq 2/3$, for $k \in \mathbb{N}^\star$. For other values of d the best lower bounds for γ_d are due to Imrich [7] (following a work of previous work of Margulis [10]). In this section we show a modification of the LPS construction as done in [3] that allows to get the improvements in the last columns of Table 1.

The idea is to consider a "symmetric" subset $\mathscr{D}(d)$ of $\mathscr{P}(p)$ of size $d+1 < p+1$. If $d+1$ is even, such a set exists if and only if $p \equiv 3 \bmod 8$. Consider $\mathscr{D}_{p,q}$ the image of $\mathscr{D}(d)$ in $\mathbb{H}(\mathbb{F}_q)^\times/\mathcal{Z}$. Again, if $\left(\frac{p}{q}\right) = 1$, then this image is contained in $\mathbb{H}^1(\mathbb{F}_p)/\{\pm 1\}$. Take the Cayley graphs $G_{d,p,q} := \mathscr{C}ay(\mathbb{H}^1(\mathbb{F}_q)/\{\pm 1\}, \mathscr{D}_{p,q})$ if $\left(\frac{p}{q}\right) = 1$ or $G_{d,p,q} := \mathscr{C}ay(\mathbb{H}(\mathbb{F}_q)^\times/\mathcal{Z}, \mathscr{D}_{p,q})$ if $\left(\frac{p}{q}\right) = -1$. It is then not very difficult to prove that $\text{girth}(G_{d,p,q}) \geq 4\log_p q - 2\log_p 2$ if $\left(\frac{p}{q}\right) = -1$ or $\text{girth}(G_{d,p,q}) \geq 2\log_p q$ if $\left(\frac{p}{q}\right) = 1$.

It is more complicated to prove that these graphs are connected, and actually this can be proved only if $q > p^8$. This is due to some properties of subgroups of $PSL_2(\mathbb{F}_q)$ (see [3, § 2.3]). Therefore the families (indexed by q; p and d are fixed) of non-bipartite graphs $\mathscr{X}_{d,p} := \{G_{d,p,q}\}_{q>p^8,\left(\frac{p}{q}\right)=1}$ and the families (indexed by q; p and d are fixed) of bipartite graphs $\mathscr{X}^{\text{bip}}_{d,p} := \{G_{d,p,q}\}_{q>p^8,\left(\frac{p}{q}\right)=-1}$ are all connected and it comes that:

$$\text{girth}(G_{d,p,q}) \geq \begin{cases} \frac{2}{3\log_d(p)} \log_d |G_{d,p,q}| & \text{if } \left(\frac{p}{q}\right) = 1 \\ \frac{4}{3\log_d(p)} \log_d |G_{d,p,q}| - 4\log_p 4 & \text{if } \left(\frac{p}{q}\right) = -1 \end{cases} \tag{6}$$

These lower bounds on the girth are maximized when $\log_d(p)$ is minimal, or equivalently when p is the lowest above d. There exists some bounds on the smallest next prime or smallest next prime equal to 3 modulo 8 to a given number d. Let $\kappa := \log_d \min\{p \geq d \mid p \text{ prime}\}$ if d is odd, and $\kappa := \log_d \min\{p \geq d \mid p \text{ prime} \equiv 3 \bmod 8\}$ if d is even. By using the results in [13] one gets the following:

d odd	$\frac{4}{3\kappa} \leq \gamma(\mathscr{X}^{\text{bip}}_{d,p})$
$15 \leq d \leq 31$	1.27
$35 \leq d \leq 1333$	1.3
$1335 \leq d$	1.33

Table 2: $d+1$ is even

d even	$\frac{4}{3\kappa} \leq \gamma(\mathscr{X}^{\text{bip}}_{d,p})$
$22 \leq d \leq 42$	1.1
$44 \leq d \leq 182$	1.25
$184 \leq d \leq 4824$	1.3
$d \geq 4826$	1.33

$d+1$ is odd

Considering Equality (3), it follows that $\gamma_{d+1} \geq \frac{4}{3\kappa}$ with the values taken from the two tables above. When d is not the power of an odd prime, these lower bounds surpass the 0.48 of [7]. When d is not equal to a power of 2, this surpass the previous best lower bound of 2/3 found in [12].

References

[1] N. L. Biggs. Graphs with large girth. *Ars Combin.*, 25(C):73–80, 1988. Eleventh British Combinatorial Conference (London, 1987).

[2] P. Chiu. Cubic Ramanujan graphs. *Combinatorica*, 12(3):275–285, 1992.

[3] X. Dahan. Arbitrary degree regular graphs of large girth. Preprint, arXiv:1110.????, October 2011.

[4] P. Erdös and H. Sachs. Reguläre Graphen gegebener Tailenweite mit minimaler Knollenzahh. *Wiss. Z. Univ. Halle-Willenberg Math. Nat.*, 12:251–258, 1963.

[5] R. G. Gallager. *Low density parity check codes.* M.I.T. Press, 1963. Monograph.

[6] S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc. (N.S.)*, 43(4):439–561 (electronic), 2006.

[7] W. Imrich. Explicit construction of regular graphs without small cycles. *Combinatorica*, 4(1):53–59, 1984.

[8] F. Lazebnik and V. A. Ustimenko. Explicit construction of graphs with an arbitrary large girth and of large size. *Discrete Appl. Math.*, 60(1-3):275–284, 1995. ARIDAM VI and VII (New Brunswick, NJ, 1991/1992).

[9] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[10] G. A. Margulis. Explicit constructions of graphs without short cycles and low density codes. *Combinatorica*, 2(1):71–78, 1982.

[11] G. A. Margulis. Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators. *Problemy Peredachi Informatsii*, 24(1):51–60, 1988.

[12] M. Morgenstern. Existence and explicit constructions of $q + 1$-regular Ramanujan graphs for every prime power q. *J. Combin. Theory Ser. B*, 62(1):44–62, 1994.

[13] O. Ramaré and R. Rumely. Primes in arithmetic progressions. *Mathematics of Computation*, 65(213):397–425, 1996.

[14] R. M. Tanner. A recursive approach to low complexity codes. *IEEE Trans. on Inform. Theory*, 27(5):533–547, 1981.

[15] A. Weiss. Girths of bipartite sextet graphs. *Combinatorica*, 4(2-3), 1984.