COMBINATORICA 4 (1) (1984) 53—59

EXPLICIT CONSTRUCTION OF REGULAR GRAPHS WITHOUT SMALL CYCLES

Wilfried IMRICH

Dedicated to Paul Erdős on his seventieth birthday

Received 23 April 1983

For every integer $d>2$ we give an explicit construction of infinitely many Cayley graphs X of degree d with $n(X)$ vertices and girth $>0.4801\ldots(\log n(X))/\log(d-1)-2$. This improves a result of Margulis.

1. Introduction

Margulis [5] has given an explicit construction of Cayley graphs with large girth. In particular, he showed how to find infinitely many values k_i for any given $\varepsilon>0$ and infinitely many Cayley graphs X_{ij} of degree $2k_i$ whose girths $c(X_{ij})$ satisfy the inequality

$$c(X_{ij}) > \left(\frac{4}{9}-\varepsilon\right)(\log n(X_{ij}))/\log k_i,$$

$n(X_{ij})$ denoting the number of vertices of X_{ij}. This compares with a non-constructive bound of Erdős and Sachs [1] for regular graphs of degree d which implies the asymptotic lower bound

$$(\log n(X))/\log(d-1)+2$$

for $c(X)$. For degree 4 Margulis [5] also derived the bound

$$c(X) > 0.83\ \ldots\ (\log n(X))/\log 3-3.$$

We shall prove the following theorem:

Theorem. *For every integer $d>2$ one can effectively construct infinitely many Cayley graphs X of degree d whose girth $c(X)$ satisfies the inequality*

$$c(X) > 0.4801\ \ldots\ (\log n(X))/\log(d-1)-2,$$

AMS subject classification (1980): 05 C 35, 05 C 38, 05 C 25, 20 E 05

where $n(X)$ denotes the number of vertices of X. For $d=3$ we further have

$$c(X) > 0.9602 \dots (\log n(X))/\log 2-5.$$

As Margulis [5] we shall use Cayley graphs of factor groups of certain subgroups of the modular group.

2. Preliminaries

Let $SL_2(K)$ denotet he group of unimodular two-by-two matrices over a commutative ring K with identity and let Z and Z_p denote the ring of integers and the field of residues mod p for any prime p. The *modular group* L is the factor group of $SL_2(Z)$ with respect to its center, i.e. with respect to the group consisting of the identity matrix I and $-I$. It is well known that L is the free product of a cyclic group of order 2 with one of order 3 (see [4]). In particular, L is the free product of the groups of order 2 and 3 generated by

$$S=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad R=\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

(Note that S and R have orders 4 and 6 in $SL_2(Z)$ but orders 2 and 3 in L.)

The group $SL_2(Z_p)/\pm I$ will be denoted by G_p. It has $p(p^2-1)/2$ elements and there is a homomorphism f_p of L onto G_p which associates with each matrix A in L the matrix $f_p(A)$ obtained by reducing each element of A modulo p.

The elements A of L are endowed with the usual matrix norm

$$\|A\| = \sup_{x\neq 0} \|Ax\|/\|x\|,$$

where $\|x\|$ is the Euclidean length of the vector x. This norm is submultiplicative. As noted in [5] the norm of A can be computed as the square root of the largest eigenvalue of A^*A, where A^* is the conjugate transpose of A.

It will be our main problem to find certain subgroups of L generated by elements with small norms. To this end we shall use directed Cayley graphs of L. The graphs without short cycles we wish to construct, however, will be f_p-images of undirected Cayley graphs of these subgroups of L.

3. Cayley graphs

The directed Cayley graph $C(G, H)$ of a group with respect to a subset H of G is defined on the vertex set G with the edge set $G\times H$. The initial vertex $o(g, h)$ of an edge (g, h) is g and the terminal one gh. If we assume that $H^{-1}=H$ there exists an edge (gh, h^{-1}) to every edge (g, h) in $C(G, H)$. By identifying these edges we obtain the so-called undirected Cayley graph $X(G, H)$.

For example, consider $C(L, \{R, S\})$. Every vertex of $C_L=C(L, \{R, S\})$ is adjacent to exactly one two-cycle and one triangle, but there are no other cycles in C_L. We color all edges of type (g, R) red and the others blue. Thus C_L is a Husimi tree of red triangles and blue two-cycles.

As another example, consider a free group F with a set $\{g_1, \ldots, g_k\}$ of free generators. Then $X(F, \{g_1^{\pm 1}, \ldots, g_k^{\pm 1}\})$ is a tree of degree $2k$. Furthermore, if G is the free product of F with the two-element group $\langle a | a^2 = 1\rangle$, then $X(G, \{a, g_1^{\pm 1}, \ldots$ $\ldots, g_k^{\pm 1}\})$ is a tree of degree $2k+1$.

We note that every subgroup U of G acts on $C(G, H)$ by left multiplication, i.e. for every u in U the mapping $g \mapsto ug$, $(g, h) \mapsto (ug, h)$ is an automorphism of C. Furthermore, the quotient graph $C(G, H)/U$ is a so-called coset graph of G. Its vertices are the right cosets Ug of U and its edges the pairs (Ug, h). The mapping $g \mapsto Ug$, $(g, h) \mapsto (Ug, h)$ is a local isomorphism. Finally, we observe that $C(G, H)$ is a coset graph with respect to the trivial subgroup.

To describe walks in directed graphs we wish to indicate whether an edge e is traversed from its origin to its terminus or vice-versa. In the first case we simply write e or e^{+1}, in the second e^{-1}. Then the mapping ψ defined on the edges of $C(G, H)/U$ by

$$\psi(Ug, h) = h \quad \text{and} \quad \psi(Ug, h)^{-1} = h^{-1}$$

readily extends to a homomorphism of the groupoid of walks in $C(G, H)/U$ into the group G.

If T is a fixed spanning tree in $C(G, H)/U$ and e an edge of $C(G, H)/U$ let $w(e)$ consist of the unique walk in T from U to $o(e)$, the edge e and the unique walk in T from $t(e)$ to U. Then the set of elements $\psi w(e)$, where e is an edge of $C(G, H)/U$ but not of T, generates U. Sometimes one can make due with considerably fewer generators though, as is examplified by the basic construction in the proof of the Kurosh subgroup theorem in [2] and [3]. We shall use this construction in the next section.

4. Subgroups of L

By the Kurosh subgroup theorem every subgroup U of a free product $A * B$ is the free product of a free group with the intersection of U with conjugates of the factors A or B. Thus every subgroup of L is the free product of a free group with groups of order 2 or 3. With the methods of [2] or [3] it is easy to obtain the decomposition of every subgroup U of L into a free product by inspection of the quotient graph $C_{L,U} = C(L, \{R, S\})/U$. We proceed as follows:

$C_{L,U}$ consists of red triangles, blue two cycles and red or blue loops. Choose a spanning tree T of $C_{L,U}$ such that the intersection of T with every red triangle contains two edges, i.e. spans the triangle. Further, consider the set D consisting of one edge in every blue two-cycle and the set M of all loops. Then the set

$$\{\psi w(e) | e \in D\}$$

is a set of free generators for a free group F, every $\psi w(e)$, $e \in M$, generates a group G_e of order 2 or 3 and

$$U = F * \prod_{e \in M}{}^{*} G_e.$$

For example, let $C_{L,U}$ be the graph of Figure 1; red edges indicated by broken arrows. Let T consist of the red edges adjacent to U and let D consist of the edge (UR, S). Of course, $M = \{(U, S)\}$. Then U is the free product of the free group generated by RSR with the group of order 2 generated by S. Let $\alpha=\|RSR\|$. We note that

$$\alpha = 1+\sqrt{2} = 2.4142135 \ldots.$$

For the quotient graph $C_{L,V}$ of Figure 2, let T consist of the edge (V, S) and of the red edges adjacent to V and VS. Then V is a free group and the elements

$$RSRS = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad R^{-1}SR^{-1}S = -\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

freely generate V. (This generating set is used by Margulis [5].)

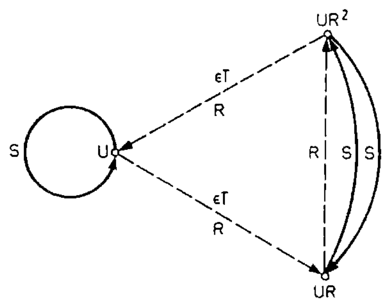

Fig. 1

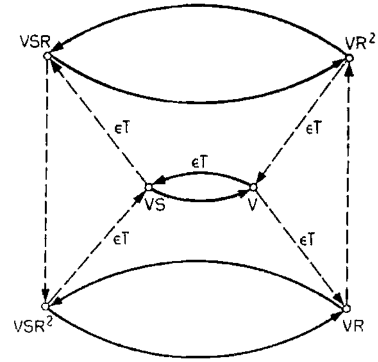

Fig. 2

We shall use the following construction: Let H_m be the graph formed from $C_L=C(L, \{R, S\})$ by deletion of all vertices of distance $\geqq 2m$ from the blue two-cycle with the endpoints I and S. We also delete all edges incident with the removed vertices. Then every triangle of distance $2m-2$ from $\{I, S\}$ contains one vertex of distance $2m-2$ from $\{I, S\}$ and two vertices of distance $2m-1$. These two vertices are not incident with blue edges in H_m. We connect every pair of such vertices with a blue two-cycle such as the vertices UR and UR^2 in Figure 1 are connected by a blue two-cycle. The resulting graph is a quotient graph of C_L with respect to a free subgroup V_m of L. We can immediately read off a set B_m of free generators for V_m. For example, we can take all elements of the form

$$S^{\varepsilon_0}(R^{\varepsilon_1}S) \ldots (R^{\varepsilon_{m-1}}S)RSR(SR^{-\varepsilon_{m-1}}) \ldots (SR^{-\varepsilon_1})S^{\varepsilon_0},$$

where $\varepsilon_0 \in \{0, 1\}$ and $\varepsilon_i \in \{1, -1\}$ for $i \geqq 1$. We also observe that the rank of V_m is 2^m.

If we replace the generator

$$(RS)^{m-1}RSR(SR^{-1})^{m-1},$$

of V_m by

$$(RS)^{m-2}RSR^{-1}(SR^{-1})^{m-2},$$

which is of order two, we obtain a generating set A_m of a subgroup U_m of L which is a free product of a cyclic group of order two by a free group of rank 2^m-1.

Setting β for the norm of R,

$$\beta = \sqrt{(3+\sqrt{5})/2} = 1.6180339 \ldots,$$

we observe that $\beta^{2m-2}\alpha < \beta^{2m}$ is an upper bound for the norm of the generators of V_m and U_m.

5. Proof of the theorem

Let A_m be the generating set of U_m and B_m the generating set of V_m as defined above. Then $X(U_m, A_m \cup A_m^{-1})$ is a homogeneous tree of degree $2r=2^{m+1}$ and $X(V_m, B_m \cup B_m^{-1})$ a homogeneous tree of degree $2r-1$.

More generally, let A be a generating set of a subgroup U of L such that $X = X(U, A \cup A^{-1})$ is a tree. The homomorphism f_p: $L \to G_p$ maps U into a subgroup U_p of G_p with a generating set $A_p = f_p A$ and extends to a homomorphism of X onto $X_p = X(U_p, A_p \cup A_p^{-1})$. We shall denote this homomorphism also by f_p. If f_p is injective on A then f_p is a local isomorphism and therefore a covering.

If f_p is injective not only on A, but on all vertices of distance $<r$ from I in X, then the length of the smallest cycle in X_p is at least $2r-1$. Following Margulis [4] we observe that the images $f_p a$ and $f_p b$ of two elements a, b of L can be the same only if the norm of a or the norm of b is $\geqq p/2$. In other words, if γ is the maximum of the norms of the elements in A and if

$$\gamma^r \geqq p/2, \tag{1}$$

then the girth $c(X_p)$ of X_p, i.e. the length of the smallest cycle in X_p, is at least $2r-1$. This yields the bound

$$c(X_p) \geqq 2 \log_\gamma (p/2) - 1$$

of [4]. Since the number $p(p^2-1)/2$ of elements in G_p is an upper bound for the number of elements $n(X_p)$ of X_p this implies

$$c(X_p) > (2/3) \log_\gamma \big(n(X_p)/4\big) - 1. \tag{2}$$

Let d be a given valency and m the smallest integer with $d \leqq 2^{m+1}$. For even d we delete $(2^{m+1}-d)/2$ elements from A_m and for d odd $(2^{m+1}-d+1)/2$ elements of infinite order from B_m. In either case we denote the set obtained by A and observe that the Cayley graph $X(U, A \cup A^{-1})$ of the group $U = \langle A \rangle$ is a homogeneous tree of degree d. Furthermore, $2^m \leqq d-1$, by the choice of m and thus $\beta^{2 \log_2 (d-1)}$ is an upper bound for the norm of the generators of A. Together with (2) this implies

$$c(X_p) > (1/3)(\log_\beta 2) \log_{d-1} \big(n(X_p)/4\big) - 1,$$

which readily yields the first assertion of the theorem.

If one takes advantage of the fact that

$$\gamma \leqq \beta^{2m-2} \tag{3}$$

one can also show that

$$c(X_p) > 0.4801 \ldots (\log n(X_p))/\log (d-1) + \text{const.}$$

for $p \gg r$. Furthermore, for $m=1$, i.e. for degree 4, the inequalities (3) and (2) yield the bound

$$c(X_p) > (2/3)\log_\alpha(n(X_p)/4)-1$$

of Margulis [4].

For degree 3 we consider the group $U=\langle S, RSR\rangle$ of Figure 1. It is easy to see by induction that any product of r generators or their inverses contains at most $r+1$ elements R or R^{-1}. We thus have to replace the inequality (1) by $\beta^r \geqq p/2$ to obtain

$$c(X_p) \geqq 2r-1 \geqq 2\log_\beta(p/2)-3$$

and

$$c(X_p) > (2/3)(\log_\beta 2)(\log n(X_p))/\log 2-5.$$

6. Cubic graphs

Let $n(d, c)$ be the minimal number of vertices of regular graphs of degree d and girth c. Walther [6, 7] showed non-constructively that

$$n(d, c) \leqq (2d-4/d)[(d-1)^{c-2}-1]/(d-2)+2d$$

if d is odd. For cubic graphs X this implies

$$c(X) = \log_2(n(X)-6)-\log_2(14/3)+2, \tag{4}$$

which is better than the constructive result of this paper.

However, at least for $p \leqq 73$, the actual girths of the graphs

$$Y_p = f_p X(U, \{S, RSR, R^{-1}SR^{-1}\})$$

are larger than predicted by (4). They have been computed by G. Schwarz and are listed in the following table:

p	3	5	7	11	13	17	19	23	29	31
$c(Y_p)$	3	5	7	11	13	15	15	17	18	19
$c_w(Y_p)$	3	6	8	10	10	12	12	13	14	14

p	37	41	43	47	53	59	61	67	71	73
$c(Y_p)$	20	19	21	21	$\geqq 21$	$\geqq 21$	$\geqq 21$	$\geqq 21$	21	22
$c_w(Y_p)$	15	15	16	16	16	17	17	17	18	18

For comparison the bounds $c_w(Y_p)$ of Walther, computed from (4), are also included. Since the evaluation of the right side of (4) requires the knowledge of $n(X_p)$ we wish to remark that $n(Y_p)=|G_p|$ if $\langle S, RSR\rangle = G_p$. For odd p this is easily seen to be the case, because

$$(SR)^2 = S(RSR) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in G_p$$

and thus also

$$((SR)^2)^{(p+1)/2} = \begin{pmatrix} 1 & p+1 \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = -(SR)^{-1} \in G_p.$$

But then $R=S(SR)$ is also in G_p and since S, R generate L they also generate G_p.

References

[1] P. ERDŐS and H. SACHS, Reguläre Graphen gegebener Taillenweite mit minimaler Knotenzahl, *Wiss. Z. Univ. Halle—Wittenberg, Math.-Nat. R.* **12** (1963), 251—258.

[2] P. J. HIGGINGS, *Categories and Groupoids*, Van Nostrand, London, 1971.

[3] W. IMRICH, Subgroup theorems and graphs, *Combinatorial Mathematics, V* (Proc. Fifth Austral. Conf. Roy. Melbourne Inst. Techn., Melbourne, 1976), pp. 1—27. *Lecture Notes in Math.* **622**, Springer, Berlin, 1977.

[4] W. MAGNUS, A. KARRASS and D. SOLITAR, *Combinatorial group theory*, Interscience, N.Y. 1966.

[5] G. A. MARGULIS Graphs without short cycles, *Combinatorica* **2** (1982), 71—78.

[6] H. WALTHER, Über reguläre Graphen gegebener Taillenweite und minimaler Knotenzahl, *Wiss. Z. HfE Ilmenau* **11** (1965), 93—96.

[7] H. WALTHER, Eigenschaften von regulären Graphen gegebener Taillenweite und minimaler Knotenzahl, *Wiss. Z. HfE Ilmenau* **11** (1965), 167—168.

Wilfried Imrich

Institut für Mathematik und Angewandte Geometrie
Montanuniversität Leoben A—8700 Leoben, Austria