COMBINATORICA 2 (1) (1982) 71—78

EXPLICIT CONSTRUCTIONS OF GRAPHS WITHOUT SHORT CYCLES AND LOW DENSITY CODES

G. A. MARGULIS

Received 19 March 1978
Extended 13 September 1981

We give an explicit construction of regular graphs of degree $2r$ with n vertices and girth $\geqq c \log n/\log r$. We use Cayley graphs of factor groups of free subgroups of the modular group. An application to low density codes is given.

1. Introduction

In this paper we consider graphs whose vertices have bounded degree ($\geqq 3$). We study the girth of such graphs, that is the length of their shortest cycle. One can easily show that this quantity grows at most at the rate of the logarithm of the number of vertices. It isn't difficult either to prove the existence of such graphs whose girth is a logarithmic function of the number of vertices. An explicit construction, however, presents difficulties. In fact, to the author's knowledge none of the known proofs of the existence of such graphs is constructive. (For literature, see [8], pp. 108—125.) The basic aim of this paper is to give an explicit construction. As an application, we give an explicit construction of a sequence of low density codes for which the probability of errors of decoding tends to zero.

2. Preliminaries

For a graph X, we shall denote by $n(X)$ the number of vertices and by $c(X)$ the girth of X. By a *walk* of length k we mean a sequence of steps along adjacent vertices $x_0, x_1, \ldots, x_k$ such that $x_{i-1} \neq x_{i+1}$.

Let us consider regular graphs of degree 4 (without loops and multiple edges). For any vertex x, the number of walks of length at most k beginning at x is

$$4(1+3+\ldots+3^{k-1}) = 2(3^k-1).$$

AMS subject classification (1980): 05 C 35, 94 B 05, 05 C 38; 05 C 25, 20 E 05, 30 F 40

On the other hand it is clear that if $c(X)>2k$ then all walks counted above end at different vertices. From this it follows that

$$2(3^{(c(X)-1)/2}-1)\leqq n(X)$$

and consequently

$$c(X)\leqq 2\log_3\left(\frac{n(X)}{2}+1\right)+1. \tag{1}$$

From this inequality we see that $c(X)$ grows at most at the rate of the logarithm of $n(X)$. With the aim of providing an explicit construction of a sequence of graphs for which $c(X)$ does grow logarithmically as a function of $n(X)$, we first describe a common way of constructing a graph from a group and a set of its generators.

3. Cayley graphs

Let G be a group and A a subset of G. Let us define the graph $X(G, A)$ in the following way. The vertices of $X(G, A)$ are the elements of the group G. Two elements $g_1, g_2 \in G$ are adjacent if and only if $g_1^{-1}g_2 \in A$, i.e. $g_2=g_1a$ for some $a\in A$. If we want to get an undirected graph, we have to assume $A=A^{-1}$, i.e. that $a\in A$ implies $a^{-1}\in A$. The graph $X(G, A)$ is sometimes called the Cayley graph of the group G with respect to the subset A. The graph $X(G, A)$ is homogeneous (vertex-transitive) since left multiplication by any element of G preserves the adjacency relation in this graph. If $\varphi\colon G\to G'$ is a group homomorphism then there is a natural map of $X(G, A)$ to $X(G', \varphi(A))$.

4. Notation

For any commutative ring K with identity, we denote by $SL_2(K)$ the group of unimodular two-by-two matrices over K (i.e. those having determinant 1). $\mathbf{Z}$ and $\mathbf{Z}_p$ denote the ring of integers and the field of residues mod p for any prime p, respectively.

If A is a subset of the group G then a *word W over A* is a finite sequence $f_1, \dots, f_n$ such that for each i, $1\leqq i\leqq n$, either f_i or f_i^{-1} belongs to A. The word W is *reduced* if $f_{i+1}\neq f_i^{-1}$ for any $i=1, \dots, n-1$.

5. The construction

Let us consider the integral matrices $A=\begin{pmatrix}1&2\\0&1\end{pmatrix}$ and $B=\begin{pmatrix}1&0\\2&1\end{pmatrix}$. It is known that there is no nontrivial multiplicative relation between A and B, that is any two reduced words over $\{A, B\}$ define different elements of $SL_2(\mathbf{Z})$ (see e.g. [7, Chapter 2.3, Exercise 13 (h)]).

For any prime p, we denote the group $SL_2(\mathbf{Z}_p)$ by G_p. There is a homomorphism φ_p of $SL_2(\mathbf{Z})$ onto G_p which associates with each matrix $X\in SL_2(\mathbf{Z})$ the matrix $\varphi_p(X)$ obtained by reducing each element of X mod p. Let us set $A_p=\varphi_p(A)$, $B_p=$

$=\varphi_p(B)$, $A_p^{-1}=\varphi_p(A^{-1})$, $B_p^{-1}=\varphi_p(B^{-1})$. Furthermore, let us consider the set $\mathfrak{A}_p=\{A_p, B_p, A_p^{-1}, B_p^{-1}\}$ and the Cayley graph $X_p=X(G_p, \mathfrak{A}_p)$.

We estimate $c(X_p)$ from below. To this end, we estimate the quantity $d(X_p)$, defined as the largest integer such that any two walks in X_p of lengths $\leqq d(X_p)$ starting at $E=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ end at different vertices. By the homogeneity of X_p, we have $c(X_p)\geqq \geqq 2d(X_p)-1$. (In fact, either $c(X_p)=2d(X_p)$ or $c(X_p)=2d(X_p)-1$.)

6. The lower bound for $d(X_p)$

Assume we are given two walks $P=(p_0, p_1, \dots, p_r)$ and $S=(s_0, s_1, \dots, s_t)$ in X_p, both starting at $E=p_0=s_0$ and having a common end $p_r=s_t$. By the definition of the graph X_p, we find that $p_i=p_{i-1}v_i$ and $s_j=s_{j-1}w_j$, $1\leqq i\leqq r$, $1\leqq j\leqq t$, where $v_i, w_j\in\mathfrak{A}_p$. The walks P and S correspond to the words $V=(v_1, \dots, v_r)$ and $W=(w_1, \dots, w_t)$ over $\mathfrak{A}_p$. Clearly $p_i=v_1\cdot\ldots\cdot v_i$ and $s_j=w_1\cdot\ldots\cdot w_j$. Hence, since $p_r=s_t$, we have

$$v_1\cdot\ldots\cdot v_r = w_1\cdot\ldots\cdot w_t. \tag{2}$$

Let us define the word $\tilde{V}=(\tilde{v}_1, \dots, \tilde{v}_r)$ by

$$\tilde{v}_i = \begin{cases} A & \text{if } v_i = A_p \\ B & \text{if } v_i = B_p \\ A^{-1} & \text{if } v_i = A_p^{-1} \\ B^{-1} & \text{if } v_i = B_p^{-1} \end{cases}$$

and $\tilde{W}=(\tilde{w}_1, \dots, \tilde{w}_t)$ analogously. By our definition of a walk (cf. Section 2), the words V and W and hence the words $\tilde{V}$ and $\tilde{W}$ are reduced. Since the walks P and S are different and $p_0=s_0=E$, the words V and W and thus the words $\tilde{V}$ and $\tilde{W}$ are different. As V and W are different reduced words over $\{A, B\}$, we infer that

$$\tilde{v}_1\cdot\ldots\cdot\tilde{v}_r \neq \tilde{w}_1\cdot\ldots\cdot\tilde{w}_t \tag{3}$$

since there is no multiplicative relation between A and B.

On the other hand, by (2) we have

$$\varphi_p(\tilde{v}_1\cdot\ldots\cdot\tilde{v}_r) = \varphi_p(\tilde{w}_1\cdot\ldots\cdot\tilde{w}_t). \tag{4}$$

Therefore all elements of the matrix $\tilde{v}_1\cdot\ldots\cdot\tilde{v}_r-\tilde{w}_1\cdot\ldots\cdot\tilde{w}_t$ are divisible by p and at least one of them is different from zero by (3). We conclude that

$$\|\tilde{v}_1\cdot\ldots\cdot\tilde{v}_r-\tilde{w}_1\cdot\ldots\cdot\tilde{w}_t\| \geqq p, \tag{5}$$

where the norm of a matrix L is defined by $\|L\|=\sup\limits_{x\neq 0}\|Lx\|/\|x\|$ and the norm of $x=\begin{pmatrix}x_1\\x_2\end{pmatrix}$ is $\|x\|=\sqrt{x_1^2+x_2^2}$. From (5) we infer

$$\max\{\|\tilde{v}_1\cdot\ldots\cdot\tilde{v}_r\|, \|\tilde{w}_1\cdot\ldots\cdot\tilde{w}_t\|\} \geqq p/2. \tag{6}$$

Let us now calculate the norms of the matrices A, B, A^{-1}, B^{-1}. It is known that $\|A\|^2=\|A^*A\|$ where A^* is the conjugate-transpose of A. The norm of the hermitian matrix A^*A coincides with its largest eigenvalue. Now, a simple calculation shows that $\alpha \overset{\text{def}}{=} \|A\|=1+\sqrt{2}$. Furthermore, A, B, A^{-1} and B^{-1} are similar under orthogonal transformations and therefore

$$\|A\| = \|B\| = \|A^{-1}\| = \|B^{-1}\| = \alpha = 1+\sqrt{2} = 2.4142\dots \tag{7}$$

By the submultiplicativity of the norm of matrices, from (6) and (7) we deduce:

$$\alpha^{\max\{r,s\}} \geqq p/2. \tag{8}$$

Recalling now the definition of $d(X_p)$, by (8) we obtain the inequality

$$d(X_p) \geqq \log_\alpha (p/2) \tag{9}$$

and consequently

$$c(X_p) \geqq 2\log_\alpha (p/2)-1. \tag{10}$$

Let us remark, that the order of the group G_p is $n(X_p)=p(p^2-1)$. From this and from (10) it follows that $\frac{2}{3}\log_\alpha n(X_p)=0.756\dots\log n(X_p)$ is an asymptotic lower estimate for $c(X_p)$.

For comparison, let $c(n)$ denote the maximum girth of regular graphs of degree 4 and at most n vertices. The non-constructive lower bound of Erdős and Sachs [1] and of others (cf. [8, pp. 119—120]) yields $c(n)\geqq(1+o(1))\log_3 n=0.91\dots\log n$.

7. An application to low density codes

First we describe a natural correspondence between binary codes and bipartite graphs. Let us be given a binary code, i.e. a matrix over the field $\mathbf{Z}_2$. Let C denote the set of columns of this matrix and R the set of rows. Let us consider the undirected graph having vertex set $C\cup R$ such that $x\in C$ and $y\in R$ are adjacent if and only if the matrix element in column x and row y is 1. There will be no edges within either C or R. Conversely, from any graph X whose vertices are partitioned as $C\dot{\cup} R$ with all edges going between C and R one can define the corresponding binary matrix with $|C|$ colums and $|R|$ rows.

Now we construct the graph Y_p. To this end, we set $R_p=G_p$ and $C_p=G_p\dot{\cup}G_p=G_p\times\{0, 1\}$. We shall join $g\in R_p$ to the following six elements of C_p: $(gA_p^2, 0)$, $(gA_pB_pA_p^{-1}, 0)$, $(gB_p, 0)$, $(gA_p^{-2}, 1)$, $(gA_pB_p^{-1}A_p^{-1}, 1)$, $(gB_p^{-1}, 1)$. From the fact that there are no multiplicative relations between A and B, we infer that there are no multiplicative relations between A^2, ABA^{-1} and B either (*cf.* [7, Chapter 2.3, Exercise 10]). From this it follows by the same arguments as in Section 6 that the quantity $d(Y_p)$ tends to infinity at the rate of $\log p$, where $d(Y_p)$ is defined as the maximum of those k for which the following holds: any two walks in Y_p of lengths at most k, starting at the same vertex which belongs to C_p end at different vertices. Now, $d(Y_p)$ is twice the number of iterations needed in decoding the code $\tilde{Y}_p$ corresponding to the graph Y_p (see [2, Ch. 4]). Therefore the probability of an error in decoding the code

$\tilde{Y}_p$ using the method proposed in [2, Ch. 4] tends to zero while $p \to \infty$. (We note that the results of [2] apply here because in the code $\tilde{Y}_p$ each symbol occurs in three parity check relations and each parity check relation involves six elements.)

Remarks. (a) It is to be noted that the upper bound on the error probability of decoding obtained by the method of [2, Ch. 4] tends to zero very slowly as a function of p. **(b)** In Appendix C of [2], an algorithm is given to construct a low density code with a logarithmic number of independent iterations. This algorithm, however, is less "explicit" in comparison with the one described above in the following sense: (i) in order to determine any particular element of the parity-check matrix of [2], one has to perform n^b operations, where n is the order of the parity-check matrix and $b>3$ whereas in our construction O (log n log log n) operations suffice; (ii) the determination of any particular matrix element in [2] costs $O(n^2)$ storage space while in our construction $O(\log n)$ space suffices.

8. Arbitrary even degrees

Now we generalize the construction given in Section 5 to the case of regular graphs of arbitrary even degree $2r \geqq 4$. Again, we use Cayley graphs of the groups G_p. In the place of $\mathfrak{A}_p$ we take a set of the form $\varphi_p(\Omega_r)$ where $\Omega_r = \{g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots, \ldots, g_r, g_r^{-1}\}$ where $g_i \in SL_2(\mathbf{Z})$ and there is no relation between the g_i, that is $g_1, \ldots, \ldots, g_r$ are free generators of a free subgroup of $SL_2(\mathbf{Z})$.

For sake of an explicit construction, we use the following device. We take a sufficiently large positive integer n and select $r+1$ distinct integral vectors (m_i, q_i), $1 \leqq i \leqq r+1$, satisfying the following conditions: (a) m_i and q_i are relatively prime for every i; (b) $0 \leqq m_i < n/2$ and $0 \leqq q_i < n/2$.

Note that no two of these vectors are proportional; in particular, (0, 0) is not among them.

Since m_i and q_i are relatively prime, there exists an integral unimodular matrix

$$C_i = \begin{pmatrix} m_i & a_i \\ q_i & b_i \end{pmatrix} \in SL_2(\mathbf{Z}).$$

By adding a suitable multiple of the first column to the second we may assume $|a_i| < n/2$ and $|b_i| < n/2$. Now, we set

$$g_i = C_i \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} C_i^{-1} \quad (i = 1, \ldots, r+1),$$

and finally

$$\Omega_r = \{g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots, g_r, g_r^{-1}\}.$$

(Observe that the element g_{r+1} has been omitted.)

Let $SL_2(n\mathbf{Z})$ denote the set of those integral matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a-1 \equiv b \equiv c \equiv d-1 \equiv 0 \mod n$. Clearly, $SL_2(n\mathbf{Z})$ is a normal subgroup of $SL_2(\mathbf{Z})$. Since $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in SL_2(n\mathbf{Z})$ and $C_i \in SL_2(\mathbf{Z})$, we infer that $g_i \in SL_2(n\mathbf{Z})$. The matrices g_i are *unipotent*, i.e. all their eigenvalues are equal to 1.

Lemma 1. *For $i \neq j$, $h \in SL_2(n\mathbf{Z})$, and u and t arbitrary nonzero integers, we have $g_i^u \neq h g_j^t h^{-1}$.*

Proof. Assume by contradiction that $g_i^u = h g_j^t h^{-1}$. One can easily verify that $g_l \begin{pmatrix} m_l \\ q_l \end{pmatrix} = \begin{pmatrix} m_l \\ q_l \end{pmatrix}$, and any vector invariant under g_l is proportional to $\begin{pmatrix} m_l \\ q_l \end{pmatrix}$. From this and the unipotency of the matrix g_l it follows that for any nonzero integer s, the vectors invariant under g_l^s are again precisely those proportional to $\begin{pmatrix} m_l \\ q_l \end{pmatrix}$. On the other hand, the vector x is invariant under $g_i^u = h g_j^t h^{-1}$ if and only if $h^{-1}x$ is invariant under g_j^t. Hence, $h \begin{pmatrix} m_j \\ q_j \end{pmatrix}$ is proportional to $\begin{pmatrix} m_i \\ q_i \end{pmatrix}$, i.e. $h \begin{pmatrix} m_j \\ q_j \end{pmatrix} = b \begin{pmatrix} m_i \\ q_i \end{pmatrix}$ for some integer b. Since both h and h^{-1} are integral matrices, we infer that $b = \pm 1$. As $h \in SL_2(n\mathbf{Z})$, the components of the vector $h \begin{pmatrix} m_j \\ q_j \end{pmatrix} - \begin{pmatrix} m_j \\ q_j \end{pmatrix}$ are divisible by n. But $0 \leqq m_j < n/2$, $0 \leqq q_j < n/2$. Therefore either $h \begin{pmatrix} m_j \\ q_j \end{pmatrix} = b \begin{pmatrix} m_i \\ q_i \end{pmatrix} = \begin{pmatrix} m_j \\ q_j \end{pmatrix}$, or the absolute value of at least one of the components of the vector $h \begin{pmatrix} m_j \\ q_j \end{pmatrix} = b \begin{pmatrix} m_i \\ q_i \end{pmatrix}$ is greater than $n/2$. The first case contradicts the fact that $\begin{pmatrix} m_i \\ q_i \end{pmatrix}$ and $\begin{pmatrix} m_j \\ q_j \end{pmatrix}$ are not proportional. The second case contradicts condition (b). ▮

The group $SL_2(n\mathbf{Z})$ is a discrete subgroup of $SL_2(\mathbf{R})$. The factor space $SL_2(\mathbf{R})/SL_2(n\mathbf{Z})$ is not compact and has finite volume with respect to Haar measure. For $n \geqq 3$, the group $SL_2(n\mathbf{Z})$ is torsion free (cf. [3, Ch. 1]). Therefore, by Lemma 1, the nonexistence of relations between $g_1, \ldots, g_r$ will follow from

Lemma 2. *Let Γ be a discrete subgroup of $SL_2(\mathbf{R})$ and $h_1, \ldots, h_{r+1}$ a finite set of unipotent nonidentity elements of Γ. Assume that the following conditions hold:*

(i) *The factor space $SL_2(\mathbf{R})/\Gamma$ is not compact and has finite volume with respect to Haar measure.*

(ii) *Γ does not contain any nonidentity elements of finite order.*

(iii) *For any $i \neq j$, $h \in \Gamma$ and arbitrary nonzero integers t, u we have $h_i^u \neq h h_j^t h^{-1}$.*

Then there is no nontrivial multiplicative relation between $h_1, \ldots, h_n$, i.e. they generate a free group of rank r.

Proof. The group $SL_2(\mathbf{R})$ acts in a natural way on the upper half plane $X = \{x + iy | x, y \in \mathbf{R}, y > 0\}$. The action is given by the formula

$$gz = \frac{az+b}{cz+d}, \quad \text{where} \quad z \in X, \ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{R}).$$

Condition (ii) implies that Γ acts freely on X (no nonidentity member of Γ has any fixed points). Therefore we can naturally identify Γ with the fundamental group $\pi_1(X/\Gamma)$ of the factor space X/Γ. In view of condition (i), X/Γ is a punctured compact Riemann surface, that is there exists a compact Riemann surface S containing X/Γ such that $S - (X/\Gamma)$ consists of a finite set of points. Furthermore, the points in $S - (X/\Gamma)$ are in a natural one-to-one correspondence with the conjugacy classes of maximal unipotent subgroups of Γ (cf. [6, Chapter II, §2]). Hence for each $i=1, \dots$ $\dots, r+1$ there exist $x_i \in S-(X/\Gamma)$ and $d_i \in \mathbf{Z}$, $d_i \neq 0$ such that the curves representing $h_i \in \Gamma = \pi_1(X/\Gamma)$ are homotopic (in the free homotopy class) and thus homological to the d_i-fold walk around x_i. In addition, $x_i \neq x_j$ for $i \neq j$ by condition (iii). Now, the intersection index of a curve joining x_i to x_{r+1} and of the curve representing h_j is equal to $d_i \delta_{ij}$ where δ_{ij} is the Kronecker symbol $(1 \leqq i, j \leqq r)$. Consequently, the homology classes $\varphi(h_i) \in H_1(X/\Gamma, \mathbf{Z})$ are linearly independent for $i=1, \dots, r$, where $\varphi \colon \pi_1(X/\Gamma) \to H_1(X/\Gamma, \mathbf{Z})$ denotes the natural homomorphism to the one-dimensional homology group of X/Γ. Since there is a natural isomorphism between $H_1(X/\Gamma, \mathbf{Z})$ and the quotient of $\Gamma = \pi_1(X/\Gamma)$ by its commutator subgroup $\mathscr{D}(\Gamma)$, we have the following

Proposition. *Let $\tilde{\varphi} \colon \Gamma \to \Gamma/\mathscr{D}(\Gamma)$ denote the natural homomorphism. Then $\tilde{\varphi}(h_i)$, $1 \leqq i \leqq r$, are linearly independent (over $\mathbf{Z}$).* ▮

Let H denote the subgroup generated by the elements h_i, $i=1, \dots, r$. As Γ is the fundamental group of the noncompact two-dimensional surface X/Γ, the group Γ is free and therefore H is free as well. On the other hand, by the Proposition, the factor of H by its commutator subgroup is a free abelian group of rank r. Hence H is a free group of rank r. Any r-set of generators of a free group of rank r being free (cf. [4, Thm. 4.2.3]) we conclude that there is no relation between $h_1, \dots, h_r$. ▮

9. Concluding remarks

The norms of the matrices g_i are $\|g_i\| < n^3$. Therefore the girth of the corresponding Cayley graph $X(G_p, \varphi(\Omega_r))$ is greater than $\frac{2}{3}\log_n(p/2)-1$ (cf. inequality (10) in Section 6). For $n \to \infty$, the total number of vectors satisfying (a) and (b) is $(3/2\pi^2+o(1))n^2$ (cf. [5, Ch. 18.5]). So, for infinitely many values of r we can choose n to be less than $\sqrt{7r}$. The number of vertices of the resulting Cayley-graph is $n(X) = |G_p| = p(p^2-1)$. To sum up, *for any $\varepsilon > 0$ we have infinitely many values r_i and for each r_i an infinity of regular graphs X_{ij} of degree $2r_i$ with girth*

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

For comparison, the non-constructive bound of Erdős and Sachs [1] can be written essentially as

$$c(X) > \frac{\log n(X)}{\log(d-1)}+2$$

where d is the degree of the graph X. Note, that the upper bound, analogous to (1) says

$$c(X) < 2\left(\frac{\log n(X)}{\log(d-1)}+1\right).$$

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] R. G. Gallager, *Low-density parity-check codes,* M. I. T. Press, Cambridge, Mass. 1963.
[3] K. C. Gunning, *Lectures on modular forms,* Ann. Math. Studies **48**, Princeton Univerity Press, Princeton N. J. 1962.
[4] M. Hall, Jr., *The theory of groups,* Macmillan, N. Y. 1959.
[5] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers,* 5th ed., Clarendon Press, Oxford 1979.
[6] I. Kra, *Automorphic forms and Kleinian groups,* Benjamin, Reading, Mass. 1972.
[7] W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory,* Interscience, N. Y. 1966.
[8] H. Walther and H.-J. Voss, *Über Kreise in Graphen,* VEB Deutscher Verlag der Wiss., Berlin 1974.

G. A. Margulis

Institute for Problems of Information Transmission
19 Yermolovoi Str., 103051 Moscow, U.S.S.R.