COLLOQUIUM MATHEMATICUM

VOL. 80 1999 NO. 1

THE GRAPH OF GENERATING SETS OF AN ABELIAN GROUP

BY

PERSI DIACONIS (STANFORD, CALIFORNIA) AND
RONALD GRAHAM (FLORHAM PARK, NEW JERSEY)

1. Introduction. Let G be a finite abelian group. By the fundamental theorem, $G \cong \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$ with $m_n \mid m_{n-1} \mid \ldots \mid m_1$, $m_i \geq 2$, for uniquely defined m_i and n. In a combinatorial problem explained below, a graph of ordered t-tuples of generating elements of G is introduced. Using the notation $\langle S \rangle$ for the group generated by S, this has vertex set

$$\mathcal{X} = \mathcal{X}(t, G) = \{(g_1, \ldots, g_t) : g_i \in G,\ \langle g_1, \ldots, g_t \rangle = G\}. \tag{1.1}$$

The edge set is determined by adding $\pm$ the jth component to the ith. Thus

$$((g_1, \ldots, g_t), (g'_1, \ldots, g'_t)) \tag{1.2}$$

is an edge if for some $i \neq j$, $g'_i = g_i \pm g_j$ and $g'_k = g_k$ for all $k \neq i$.

THEOREM. *The graph of ordered generating t-tuples is connected for $t \geq n+1$. For $t = n$ the graph has $\varphi(m_n)$ components. If $g_1, \ldots, g_n$ are written as $g_i = (a_{i1}, \ldots, a_{in})$, $a_{ij} \in \mathbb{Z}_{m_j}$, the components have constant values of $\det(a_{ij}) \pmod{m_n}$. Any value with $(\det(a_{ij}), m_n) = 1$ is possible and the $\varphi(m_n)$ components have equal size.*

Motivation. The theorem solves a problem arising in two contexts. In computational group theory, algorithms in systems like GAP and MAGMA make use of random elements of a group G (now not necessarily abelian). Often G is given by specifying a generating set $G = \langle g_1, \ldots, g_t \rangle$. In applications, g_i are permutations or matrices (e.g. in S_{52} or $\mathrm{GL}_{100}(\mathbb{F}_2)$) and t is often small (e.g., all simple groups are generated by two elements). One simple way to generate random elements is to do a random walk. That is, start at the identity and repeatedly multiply by a generator uniformly chosen with replacement. This generates a sequence $x_0, x_1, \ldots, x_N$ and theory [5, 6] shows that if N is suitably large, x_N is close to uniformly distributed on G.

In practical trials, Holt and Rees [12] found that N had to be impractically large. They suggested working with ordered t-tuples of generators (the set $\mathcal{X}$ of (1.1)) and moving at random from $(g_1, \ldots, g_t)$ to $(g'_1, \ldots, g'_t)$ as in

1991 *Mathematics Subject Classification*: 60C05, 20P05.

(1.2). Spectacular speedups using this algorithm are reported by Celler *et al.* [1].

Some rigorous analysis based on Markov chain theory has been given by Diaconis and Saloff-Coste [7]–[9] and Chung and Graham [2]–[4]. One basic question is: What is the state space of the underlying Markov chain? In particular, what is $|\mathcal{X}|$ in (1.1)?

For a general group G, let $m(G)$ be the size of a minimum set of generators. Let $\overline{m}(G)$ be the maximum size of a minimal generating set (thus for $\mathbb{Z}_6$, $m = 1$, $\overline{m} = 2$). In [8, Lemma 2.1] it is shown that the state space (1.1) is connected by moves (1.2) provided $t \geq m + \overline{m}$. In applications, t is often chosen fairly small (e.g., $t = \max(2m + 1, 10)$ in the experiments of [1]). It is of interest to determine the state space for general values of t.

The same problem was independently posed as a probability problem by David Aldous (personal communication). Consider the graph (1.1), (1.2) for $G = \mathbb{Z}_2$. Each coordinate can be interpreted as "infected" or not as it is one or zero. A process proceeds on this graph by having a randomly infected particle change a randomly chosen neighbor (mod 2). In the binary case $m = \overline{m} = 1$, so the state space is all non-zero t-tuples. Chung and Graham [3]–[4] present good bounds on the rate of convergence for this problem for the complete graph as in (1.2). Aldous was also interested in more general graphs. See [7].

The general problem of counting the number of ordered t-tuples which generate G was studied by Philip Hall [11] who introduced abstract Möbius inversion for the purpose. His results are used to give formulae for $|\mathcal{X}|$ in Remark 1 of Section 3 below.

The non-abelian case seems quite difficult. For example, consider the symmetric group $G = S_n$. When is the graph (1.1), (1.2) connected? For the symmetric group S_n, $m = 2$, $\overline{m} \leq \frac{3}{2}n$. So the graph is connected for $t \geq \frac{3}{2}n + 2$. We conjecture that the graph is connected for all n, for $t \geq 3$. This has been verified for $n = 4$, $n = 5$ by John Laffrety and Dan Rockmore [13] in an elaborate enumeration: $|\mathcal{X}(S_4, 3)| = 10{,}080$, $|\mathcal{X}(S_5, 3)| = 1{,}401{,}120$.

The abelian case seemed like a reasonable place to start a careful study. We prove the theorem in Section 2. Some remarks are in Section 3.

2. Proof of the Theorem. For $G = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$, $m_n \,|\, m_{n-1} \,|\, \ldots \,|\, m_1$, and any t elements of G, write $g_i = (a_{i1}, \ldots, a_{in})$, $a_{ij} \in \mathbb{Z}_{m_j}$, and form the associated $n \times m$ matrix

$$A := \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2n} \\ \vdots & & \vdots \\ a_{t1} & \ldots & a_{tn} \end{bmatrix}.$$

We assume throughout that $\langle g_1, \dots, g_t \rangle = G$ so that for all i, $1 \le i \le n$, there are integers u_{ij}, $1 \le j \le t$, such that $\sum u_{ij} g_j = e_i = (0, \dots 0, 1, 0, \dots, 0)$. A *move* consists of an elementary row operation on the matrix A, adding the $\pm j$th row to the ith row. For present purposes any number in the jth column can be reduced modulo m_j.

The theorem will be proved by showing that

(2.1) for $t \ge n+1$, A can be moved to the form

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix},$$

(2.2) for $t = n$, A can be moved to the form

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & b \end{bmatrix}, \qquad b = \det A \pmod{m_n}, \qquad 0 < b < m_n.$$

The first step is to work with two numbers in a single column:

(2.3) Suppose $(X, Y, M) = D$. Then the two numbers $\begin{smallmatrix} X \\ Y \end{smallmatrix}$ appearing in a single column can be moved to $\begin{smallmatrix} 0 \\ D \end{smallmatrix} \pmod{M}$.

For this, write $X = xD$, $Y = yD$, $M = mD$ so $(x, y, m) = 1$. Work with $\begin{smallmatrix} x \\ y \end{smallmatrix} \pmod{m}$. Write $\delta = (x, y)$, so $(\delta, m) = 1$, and

$$\begin{matrix} x \\ y \end{matrix} = \begin{matrix} x'\delta \\ y'\delta \end{matrix},$$

$(x', y') = 1$. By successive moves,

$$\begin{matrix} x \\ y \end{matrix} \to \begin{matrix} x + uy \\ y \end{matrix} = \begin{matrix} (x' + uy')\delta \\ y'\delta \end{matrix}$$

for any u. By Dirichlet's theorem, u can be chosen so that $x' + uy' = p$, a prime, with $p > m$. (It is also possible to avoid appealing to Dirichlet's theorem here but using it takes us where we want to go somewhat more quickly. In fact, the Euclidean algorithm is sufficient.) This results in $\begin{smallmatrix} p\delta \\ y'\delta \end{smallmatrix} \pmod{m}$. From this, we may move to $\begin{smallmatrix} p\delta \\ (y' + vp)\delta \end{smallmatrix}$ for any v. Now $(\delta, m) = 1$ and $(p, m) = 1$ yield $(\delta p, m) = 1$. Thus for suitable v, $(y' + vp)\delta \equiv 1 \pmod{m}$. This gives moves to $\begin{smallmatrix} p\delta \\ 1 \end{smallmatrix}$ which may finally be moved to $\begin{smallmatrix} 0 \\ 1 \end{smallmatrix} \pmod{m}$. Putting back the multiple D gives (2.3).

Iterating this argument for t numbers in a single column modulo M shows that if $\gcd(X_1, \ldots, X_t, M) = D$, there is a sequence of moves taking

$$\begin{matrix} X_1 \\ X_2 \\ \vdots \\ X_t \end{matrix} \quad \text{to} \quad \begin{matrix} D \\ 0 \\ \vdots \\ 0 \end{matrix} \pmod{M}. \tag{2.4}$$

Note that $\langle g_1, \ldots, g_t \rangle = G$ implies that for the jth column, $D \not\equiv 0 \pmod{m_j}$. Indeed, $(D, m_j) = 1$. Note also that the sequence of moves

$$\begin{matrix} x \\ y \end{matrix} \to \begin{matrix} x+y \\ y \end{matrix} \to \begin{matrix} x+y \\ -x \end{matrix} \to \begin{matrix} y \\ -x \end{matrix}$$

shows that if a column has a single zero entry, then all permutations of that column are possible by appropriate moves.

From (2.4) working left to right, A may be moved to the form

$$\begin{matrix} D_1 & X_{12} & X_{13} & \ldots & X_{1n} \\ 0 & D_2 & X_{23} & \ldots & X_{2n} \\ 0 & 0 & D_3 & \ldots & X_{3n} \\ & & & \ddots & \\ 0 & 0 & 0 & \ldots & D_n \\ 0 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 \end{matrix} \tag{2.5}$$

The next stage is to clean up the entries above the diagonal.

Consider the first row. By hypothesis, there are $u_1, \ldots, u_n$ so that

$$u_1(D_1, X_{12}, \ldots, X_{1n}) + u_2(0, D_2, X_{21}, \ldots, X_{2n}) + \ldots + u_n(0, \ldots, D_n) = e_1.$$

Thus $u_1 D_1 = 1 \pmod{m_1}$ so that adding u_1 copies of the first row to the second gives

$$\begin{matrix} D_1 & X_{12} & \ldots & X_{1n} \\ 1 & Y_2 & \ldots & Y_n \\ & \vdots & & \end{matrix} \to \begin{matrix} 0 & X'_{12} & \ldots & X'_{1n} \\ 1 & Y'_2 & \ldots & Y'_n \\ & \vdots & & \end{matrix} \to \begin{matrix} 1 & X''_{12} & \ldots & X''_{1n} \\ 0 & Y''_2 & \ldots & Y''_n \\ & \vdots & & \end{matrix} \tag{2.6}$$

Suppose successive moves have given the form

$$\begin{array}{cccc|cc} 1 & 0 & \ldots & 0 & X_1 & \ldots \\ 0 & 1 & \ldots & 0 & X_2 & \ldots \\ & & \ddots & & \vdots & \\ 0 & 0 & \ldots & 1 & X_{s-1} & \ldots \\ \hline 0 & 0 & \ldots & 0 & D_s & \ldots \\ 0 & 0 & \ldots & 0 & 0 & \ldots \\ \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & \ldots & 0 & 0 & \ldots \end{array} \tag{2.7}$$

By hypothesis, there are $v_1, v_2, \ldots, v_n$ such that

$$v_1(1,0,\ldots,X_1,\ldots)+\ldots+v_{s-1}(0,1,\ldots,X_{s-1},\ldots) \\ +v_s(0,0,\ldots,D_t,\ldots)+\ldots=e_s.$$

Thus $v_1 \equiv 0 \pmod{m_1}$ and since $m_s \mid m_1 \mid v_1$, we have $v_1 \equiv 0 \pmod{m_s}$. Similarly, $v_i \equiv 0 \pmod{m_s}$ for $1 \le i \le s-1$, and $v_s D_s \equiv 1 \pmod{m_s}$. Thus, if $s < t$, the moves used for (2.6) give the form (2.7) with s replaced by $s+1$.

Continue with this process until $s = t$. If $t > n$, the form (2.1) has been reached. If $t = n$, the form (2.2) has been reached.

Observe that when $t = n$, the number b of (2.2) can be chosen arbitrarily with $(b, m_n) = 1$ and a generating set results. Further, multiplying the last column of any generating set with a fixed value of b by b^{-1} gives a 1-1 correspondence with generating sets having $b = 1$. ∎

3. Remarks. 1. The size of the state space $\mathcal{X}$ of (1.1) can be determined using results of P. Hall [11]. All the properties needed here appear in Section 6B of [8]. To begin, write the abelian group G as the direct product of its Sylow p-groups: $G = \prod S_p$. An abelian p-group is of form $\prod_{i=1}^{B} \mathbb{Z}_{p^{\lambda_i}}$. Let $A = \sum \lambda_i$, and

$$F(S_p,t) = p^{t(A-B)} \sum_{i=0}^{B} (-1)^i \binom{B}{i}_p p^{t(B-i)+\binom{i}{2}},$$

$$\binom{B}{i}_p = \frac{(p^B-1)\ldots(p^{B-i+1}-1)}{(p^i-1)\ldots(p-1)}.$$

Then for any t, the total number of generating t-tuples is $\prod_{p \mid |G|} F(S_p,t)$. It follows that this is $|\mathcal{X}|$ for $t \ge n+1$. For $t = n$, following the theorem, the generating n-tuples split into $\varphi(m_n)$ equal classes so $|\mathcal{X}| = \varphi(m_n)^{-1} \prod_p F(S_p,t)$.

An abelian p-group with factors $\mathbb{Z}_{p^{\lambda_1}} \times \ldots \times \mathbb{Z}_{p^{\lambda_j}}$ is specified by the partition $\lambda_1 \ge \ldots \ge \lambda_j$. For a general abelian group, if $m_i = \prod_p p^{a(p,i)}$, $1 \le i \le n$, the partition associated to $S_p(G)$ is $a(p,1), a(p,2), \ldots$ To recover the m_i from these partitions, let j^* be the largest index so that $\sum_p a(p,j) > 0$. Then

$$m_n = \prod_p p^{a(p,j^*)}, \quad m_{n-1} = \prod_p p^{a(p,j^*-1)}, \quad \ldots, \quad m_{n-i} = \prod_p p^{a(p,j^*-i)}.$$

When $n = t$, we may show directly that $\varphi(m_n)$ divides $\prod_p F(S_p,t)$. Then $j^* = n = t$. We show $\varphi(p^{a(p,n)}) \mid \prod_p F(S_p,n)$. First, $\varphi(p^{a(p,n)}) = p^{a(p,n)-1}(p-1)$ and $a(p,n)-1 \le n(A-B)$ as defined above. So divisibility

follows from

$$(p-1) \mid \sum_{i=0}^{n} (-1)^i p^{n(n-i)+\binom{1}{2}} \binom{n}{i}_p = p^{\binom{n}{2}} \prod_{i=1}^{n} (p^i - 1).$$

The displayed sum is the number of generating n-tuples for the group $\mathbb{Z}_p^n$. This equals the order of $\mathrm{GL}_n(p)$, which is the displayed product.

As an example, let $G = \mathbb{Z}_6 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. Then $S_2(G) = \mathbb{Z}_2 \times \mathbb{Z}_2$, $S_3(G) = \mathbb{Z}_3$. When $t = 2$, we have $F(S_2, 2) = 2^4 - 3 \cdot 2^2 + 2 = 6$ and $F(S_3, 2) = 3^2 - 1 = 8$. So there are $6 \cdot 8 = 48$ pairs of generators. These are shown below with entries as in the theorem. For example, $g_1 = (3, 0)$, $g_2 = (4, 1)$ generate $\mathbb{Z}_6 \times \mathbb{Z}_2$.

3 0	3 0	1 0	1 0	1 0	5 0	5 0	5 0
4 1	2 1	0 1	4 1	2 1	0 1	4 1	2 1
3 0	3 0	1 0	1 0	1 0	5 0	5 0	5 0
1 1	5 1	3 1	1 1	5 1	3 1	1 1	5 1
0 1	0 1	4 1	4 1	4 1	2 1	2 1	2 1
1 0	5 0	3 0	1 0	5 0	3 0	1 0	5 0
0 1	0 1	4 1	4 1	4 1	2 1	2 1	2 1
1 1	5 1	3 1	1 1	5 1	3 1	1 1	5 1
3 1	3 1	1 1	1 1	1 1	5 1	5 1	5 1
1 0	5 0	3 0	1 0	5 0	3 0	1 0	5 0
3 1	3 1	1 1	1 1	1 1	5 1	5 1	5 1
4 1	2 1	0 1	4 1	2 1	0 1	4 1	2 1

Here $m_n = 2$, so all determinants are $1 \pmod 2$.

2. It is natural to consider also the case with $t < n$. Then $g_1, \ldots, g_t$ generate a proper subgroup of G, which in turn can be written as $\mathbb{Z}_{m_1'} \times \ldots \times \mathbb{Z}_{m_k'}$ for $m_k' \mid m_{k-1}' \mid \ldots \mid m_1'$ with $k \geq t$. Now the theorem as stated determines the connectedness properties of the graph.

3. The diameters of the graphs (1.1), (1.2) are not easy to understand. Consider the simple case when $G = \mathbb{Z}_p$, p prime and $t = 2$. Then $\mathcal{X}$ consists of pairs $\binom{x}{y} \pmod p$, $\binom{x}{y} \neq \binom{0}{0}$, with connections to $\binom{x \pm y}{y}$, $\binom{x}{y \pm x}$. This is one of the basic expander graphs introduced by Margulis (see, e.g., [2] for references). It is known that this graph has diameter of order $\log p$.

4. If R is a ring with identity, $\mathrm{GL}_n(R)$ is the set of invertible linear maps from R^n to itself. Let $E_n(R)$ be the subgroup of GL_n generated by the elementary matrices. Then $E_n(R)$ is a normal subgroup of $\mathrm{GL}_n(A)$ containing the commutator subgroup. The abelian group $K_1(R) = \mathrm{GL}_n / E_n$ is a basic object of study in K-theory. In the special case $t = n$, $G = \mathbb{Z}_m^n$, the theorem

is the well-known result that $K_1(\mathbb{Z}_m) = \mathbb{Z}_m^*$ (see, e.g., Rosenberg [16, 2.2.7]). For closely related work see Dennis and Geller [5].

5. The basic reduction theorem leading to the canonical forms (2.1), (2.2) is similar to the Smith normal form (Schrijver [17, p. 50]). The Smith form allows both row and column operations and the additional freedom of transposing pairs of rows or columns.

6. There is related work in the language of T-systems [10], [14], [15]. These induce a finer orbit structure on $\mathcal{X}_t$, the set of generating t-tuples, by allowing permutations by automorphisms of G as well as automorphisms of the free group on t generators. Results of Neumann and Neumann [15] show that the group A_5 with $t = 2$ has at least two orbits in our sense. Results of Dunwoody [10] show there are p-groups with t generators, nilpotent of class 2, such that the set of generating t-tuples has many orbits.

Acknowledgements. We thank John Laffrety and Dan Rockmore for computational help and Ken Brown, Sue Geller and Bob Guralnick for helping us access the K-theory literature, Peter Neumann for telling us about T-systems, and a careful referee for a number of helpful remarks.

REFERENCES

[1] F. Celler, C. Leedham-Green, S. Murray, A. Wiemeyer and E. O'Brien, *Generating random elements of a finite group*, Comm. Algebra 23 (1995), 4831–4948.

[2] F. R. K. Chung, *Spectral Graph Theory*, CBMS Regional Conf. Ser. in Math. 92, Amer. Math. Soc., Providence, 1997.

[3] F. Chung and R. Graham, *Random walks on generating sets for finite groups*, Electron. J. Combin. 2 (1997), no. R7.

[4] —, —, *Stratified random walks on an n-cube*, Random Structures Algorithms (1997), to appear.

[5] R. K. Dennis and S. C. Geller, *K_i of upper triangular matrix rings*, Proc. Amer. Math. Soc. 56 (1976), 73–78.

[6] P. Diaconis, *Group Representations in Probability and Statistics*, IMS Lecture Notes—Monograph Ser. 11, Inst. Math. Statist., Hayward, CA, 1988.

[7] P. Diaconis and L. Saloff-Coste, *Random walks on finite groups: A survey of analytic techniques*, in: Probability Measures on Groups and Related Structures, XI, H. Heyer (ed.), World Scientific, River Edge, NJ, 1995, 44–75.

[8] —, —, *Walks on generating sets of abelian groups*, Probab. Theory Related Fields 105 (1996), 393–421.

[9] —, —, *Walks on generating sets of groups*, Technical Report, Dept. of Statistics, Stanford Univ., 1996.

[10] M. Dunwoody, *On T-systems of groups*, J. Austral. Math. Soc. 3 (1963), 172–179.

[11] P. Hall, *The Eulerian functions of a group*, Quart. J. Math. 7 (1936), 134–151.

[12] D. Holt and S. Rees, *An implementation of the Neumann–Praeger algorithm for the recognition of special linear groups*, J. Experiment. Math. 1 (1992), 237–292.

[13] J. Laffrety and D. Rockmore, Personal communication, 1997.

[14] B. Neumann, *On a question of Gaschütz*, Arch. Math. (Basel) 7 (1956), 87–90.
[15] B. H. Neumann and H. Neumann, *Zwei Klassen charakteristischer Untergruppen und ihre Faktorgruppen*, Math. Nachr. 4 (1951), 106–125.
[16] J. Rosenberg, *Algebraic K-Theory and its Applications*, Grad. Texts in Math. 147, Springer, New York, 1994.
[17] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, Chichester, 1986.

Departments of Mathematics and Statistics
Stanford University
Stanford, California 94305
U.S.A.
E-mail: diaconis@math.stanford.edu

AT&T Labs
Florham Park, New Jersey 07932
U.S.A.
E-mail: graham@ucsd.edu

Received 19 December 1997;
revised 15 April 1998