78/45

Comment. Math. Helvetici 53 (1978) 448–457 Birkhäuser Verlag, Basel

Some new results in probabilistic group theory

P. ERDÖS AND R. R. HALL

Introduction

Let $(G,+)$ be an Abelian group of order n. Let us choose k elements $g_1, g_2, \ldots, g_k$ from g and denote by $R(g)$ the number of representations of the element $g \in G$ in the form $g = \varepsilon_1 g_1 + \varepsilon_2 g_2 + \cdots + \varepsilon_k g_k$: here and throughout the paper each ε_i takes one of the values $0, 1$. Set $d(r) = \text{card}\{g \in G: R(g) = r\}$.

Let us suppose that the elements $g_1, g_2, \ldots, g_k$ are chosen randomly and independently from G: each element has a probability $1/n$ of being chosen. We are interested in the distribution of the values of $R(g)$ when 2^k is approximately n. We write $\lambda = 2^k/n$, the mean value of $R(g)$.

Problems concerning $R(g)$ have been studied in [1]–[8]. We do not assume familiarity with these papers but we shall need to quote results from them.

In our main result we impose the following condition on G:

Condition A

For each fixed positive integer l, the number of elements of G of order l is $o(n)$.

Our main theorem is as follows:

THEOREM 1. *Let G satisfy A, and $k = (\log n/\log 2) + O(1)$. Then for each fixed integer $r \geq 0$, we have*

$$d(r) \sim ne^{-\lambda}\frac{\lambda^r}{r!}$$

with probability $\to 1$ as $n \to \infty$.

COROLLARY. *Let G satisfy A, and let $n \to \infty$, $k \to \infty$ together in such a way that with probability $\to 1$, every $g \in G$ is represented in the required form, i.e. $d(0) = 0$. Then $\lambda \to \infty$.*

We can say rather more if G is cyclic, or more generally if we are given any specific bound for the number of elements of each order. Thus we have

THEOREM 2. *There is an absolute positive constant b such that if G is cyclic* *and $n \to \infty$, $k \to \infty$ together in such a way that $\lambda < b \log\log n$, then with* probability $\to 1$, $d(0) > 0$.

In the opposite direction, Erdös and Rényi [2] proved, independently of any condition on G, that if $\lambda/\log n \to \infty$ arbitrarily slowly as $n \to \infty$, then $d(0) = 0$ with probability $\to 1$. It would be very interesting to know to what extent this is sharp.

Regarding the relevance of Condition A, we think that it is necessary for Theorem 1. We will show by an example that with no condition on the orders of the elements, both our theorems become false. The reason for this is as follows. The distribution of the values of $R(g)$ is closely connected with the moments $\sum\{R^m(g) : g \in G\}$ and with the expectations μ_m of these moments. Now it is not difficult to show that for $m \leqslant 3$, μ_m does not depend on the structure of G, in fact K. Bognár [1] gave the formulae

$$\mu_2 = \frac{4^k}{n} + 2^k\left(1 - \frac{1}{n}\right),$$

$$\mu_3 = \frac{8^k}{n^2} + 3 \cdot \frac{4^k}{n}\left(1 - \frac{1}{n}\right) + 2^k\left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right).$$

However, for $m \geqslant 4$, μ_m depends on the orders of the group elements. In particular, let G be the direct sum of t cyclic groups of order 2, so that $n = 2^t$. Bognár evaluated μ_4 precisely, all we need here is that in this case

$$\mu_4 \sim n\{\lambda^4 + 7\lambda^3 + 7\lambda^2 + \lambda\},$$

whereas according to Theorem 1, the coefficient of λ^3 on the right should be 6. This shows that some condition on the structure of G is needed. The same example shows that Theorem 2 also depends in some way on the group structure. For as R. J. Miech [7] noticed, G can be regarded as a vector space over Z_2 in this case, moreover $R(g)$ takes just two values. In fact $\varepsilon_1 g_1 + \varepsilon_2 g_2 + \cdots + \varepsilon_k g_k$ generates a subgroup of order 2^v say, and on this subgroup, $R(g) = 2^{t-v}$. But then

$$\sum_g (R(g) - \lambda)^2 = 2^{2k-t}(2^{t-v} - 1).$$

If $d(0) > 0$, we must have $v < t$ so that the right hand side is at least $2^{2k-t} = n\lambda^2$, whereas from the formula above for μ_2, the expected value of the left hand side is $2^k(1 - 1/n) \leqslant n\lambda$. It follows from Markoff's inequality that the probability that $d(0) > 0$ is less than $1/\lambda$. Hence we have immediately

THEOREM 3. *If G is a direct sum of cyclic groups of order 2 and $n \to \infty$ $\lambda \to \infty$ together, then $d(0) = 0$ with probability $\to 1$.*

It is interesting and rather surprizing that in Theorem 1, the distribution of $d(r)$ is (asymptotically) binomial, just as if all 2^k elements $\varepsilon_1 g_1 + \varepsilon_2 g_2 + \cdots + \varepsilon_k g_k$ had been chosen independently.

We would like to mention the following purely combinatorial problem: let G be a direct sum of t cyclic groups of order 3. What is the least value of k such that there exist $g_1, g_2, \ldots, g_k$ giving $d(0) = 0$?

Most of our notation is introduced as it is needed. We define here:

$$\omega(G, l) = \operatorname{card}\{g \in G : lg = 0_G\}$$

$$\omega^*(G, l) = \max\{\omega(G, l') : l' \leq l\}.$$

$\hat{G}$ denotes the group of characters χ acting on G and χ_0 denotes the principal character.

LEMMA 1. *Let K be an h-dimensional subspace of $\mathbf{R}^m$ and C^m an m-dimensional hypercube. Suppose that K contains 2^h vertices of C^m. Then we can choose an origin at a suitable corner of the hypercube such that these vertices are the vectors $\varepsilon_1\mathbf{v}_1 + \varepsilon_2\mathbf{v}_2 + \cdots + \varepsilon_h\mathbf{v}_h$, where the $\mathbf{v}_i$ are orthogonal and are themselves vertices. Moreover, for a fixed origin, each set of $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_h$ gives a different set of 2^h vertices.*

Remark. It was shown in [5] Lemma 1 that K cannot contain more than 2^h vertices of C^m. The present lemma characterizes the extremal configurations.

Proof. This is by induction on m. The result holds for $m = 1$ and we assume it holds for $m-1$. We may further assume that $h > 0$, otherwise we choose $\mathbf{O} = K \cap C^m$ and the result is trivial.

Let us begin by choosing $\mathbf{O}$ in $K \cap C^m$ and labelling the other vertices of C^m with coordinates $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m)$. This choice of $\mathbf{O}$ is somewhat arbitrary and may need revision.

Let H_j and H'_j be the hyperplanes with $x_j = 0$ and 1 respectively. Thus C^m is the space between two $(m-1)$-dimensional hypercubes C in H_j and C' in H'_j. Next $H_1 \cap H_2 \cap \cdots \cap H_m = 0$ so we may assume j fixed so that $K \not\subset H_j$. Plainly $K \not\subset H'_j$. Let us write $L = K \cap H_j$ so that $\dim L = h-1$. From the lemma mentioned in our remark above, L cannot contain more than 2^{h-1} vertices of C. Hence $K \cap H'_j$ is non-empty and is of the form $L + \mathbf{u}$. Again $L + \mathbf{u}$ cannot contain more than 2^{h-1} vertices of C' and to account for all 2^h vertices in $K \cap C^m$, there must be equality in both cases.

We apply the induction hypothesis to the intersection of L and C in the $(m-1)$-dimensional space H_j. We choose a (possibly) new origin so that $L \cap C$ is just the set of vectors $\varepsilon_1\mathbf{v}_1 + \varepsilon_2\mathbf{v}_2 + \cdots + \varepsilon_{h-1}\mathbf{v}_{h-1}$. The vectors $\mathbf{v}_i$ are orthogonal so they are a basis of L. Let $\mathbf{e}$ be the vertex in $K\cap C'$ nearest to the new origin. Then $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{h-1}$ and $\mathbf{e}$ are a basis for K, and we have to consider when $\mathbf{y}=\xi_1\mathbf{v}_1+\xi_2\mathbf{v}_2+\cdots+\xi_{h-1}\mathbf{v}_{h-1}+\xi\mathbf{e}$ can be a vertex of C^m.

With respect to the new origin, relabel the vertices, of C^m with coordinates $(\delta_1, \delta_2, \ldots, \delta_m)$, each $\delta_j=0$ or 1. The vertex $\mathbf{v}_i$ has coordinates $(\delta_{i1}, \delta_{i2}, \ldots, \delta_{im})$ where $\delta_{ij}=1$ for at most one i, by the orthogonality of the $\mathbf{v}_i$'s. As $\mathbf{e}\notin L$, if $\mathbf{e}$ has coordinates $(\delta_{h1}, \delta_{h2}, \ldots, \delta_{hm})$ there must be at least one j for which $\delta_{hj}=1, \delta_{ij}=0$ for $i<h$. Thus if $\mathbf{y}$ is a vertex, we must have $\xi=o$ or 1, and if $\xi=0$ $\mathbf{y}$ lies in $L\cap C$ so that $\xi_i=\varepsilon_i$, for $i<h$. Next, let $\xi=1$ and suppose one of the ξ_i, ξ_1 say, is negative, and that $\mathbf{y}$ is a vertex. Since $\mathbf{v}_1$ is orthogonal to the other $\mathbf{v}_i$'s and $\mathbf{y}$ has every coordinate 0 or 1, we must have $\xi_1=-1$ and $\delta_{ij}\leqslant\delta_{hj}$ for every j. But then $\mathbf{e}-\mathbf{v}_1$ is a vertex of C' and it is nearer than $\mathbf{e}$ to the origin. This is a contradiction, and we conclude that $\xi_i\geqslant 0$ for every $i<h$. Now suppose $\mathbf{y}$ is a vertex, and ξ_1 (say) is positive. Then $\mathbf{v}_1$ is orthogonal to $\mathbf{e}$, (otherwise $\mathbf{y}$ would have some coordinates $=2$), and in fact $\xi_1=1$. Hence for each $i<h$, either $\mathbf{v}_i$ is orthogonal to $\mathbf{e}$ and $\xi_i=\varepsilon_i$, or $\xi_i=0$. We have to find 2^{h-1} vertices $\mathbf{y}$ with $\xi=1$ and so $\mathbf{e}$ is orthogonal to all the $\mathbf{v}_i$. The result follows if we write $\mathbf{e}=\mathbf{v}_h$, $\xi=\varepsilon_h$.

To prove the last part of the lemma, we suppose there is an alternative set of vertices $\mathbf{v}_1'\mathbf{v}_2', \ldots, \mathbf{v}_h'$ giving rise to the same set of 2^h vertices. Then we have $\mathbf{v}_i'=\varepsilon_{i1}\mathbf{v}_1+\varepsilon_{i2}\mathbf{v}_2+\cdots+\varepsilon_{ih}\mathbf{v}_h$ and so $\mathbf{v}_i'$ is just the vector sum of some of the $\mathbf{v}_j$'s. But the $\mathbf{v}_i'$ are orthogonal, hence these sums must be disjoint, and as there are the same number of $\mathbf{v}_i'$ and $\mathbf{v}_j$, each sum has just one term. Hence the $\mathbf{v}_i'$ are just a permutation of the $\mathbf{v}_j$.

LEMMA 2. *Suppose that $d_r\geqslant 0$ for $r=0, 1, 2, \ldots, \lambda\geqslant 0$, and that for $0\leqslant m\leqslant M$ we have*

$$\left|\sum_{r=0}^{\infty} d_r r^m - e^{-\lambda}\sum_{r=0}^{\infty}\frac{\lambda^r}{r!}r^m\right|\leqslant\beta_m.$$

Then we have

$$\left|d_r-e^{-\lambda}\frac{\lambda^r}{r!}\right|\leqslant 2^M(M+1)\sum_{m=0}^{M}\beta_m+\frac{\lambda^M(1+\lambda)}{r!(M-r)!}$$

for each $r<M$.

Proof. Choose T in the range $r\leqslant T\leqslant M$ and set

$$\mathrm{Q}(x)=\mathrm{Q}(x;r,T)=\sum_{m=0}^{T}c_m x^m=\frac{1}{T!}\binom{T}{r}(-1)^{T-r}\prod_{j=0}^{T}{}'(x-j),$$

the factor $(x-r)$ being omitted from the product. Thus $\mathrm{Q}(r)=1, \mathrm{Q}(j)=0$ for

$0 \leq j \leq T, j \neq r$, and $\operatorname{sgn} Q(j) = (-1)^{T-r}$ for $j > T$. Since $T \leq M$, we have

$$\left| \sum_{j=0}^{\infty} d_j Q(j) - e^{-\lambda} \sum_{j=0}^{\infty} \frac{\lambda^j}{j!} Q(j) \right| \leq \sum_{m=0}^{T} |c_m| \beta_m$$

and by Cauchy's formula,

$$|c_m| \leq \frac{1}{2\pi} \int_0^{2p} |Q(e^{i\theta})| \, d\theta \leq \binom{T}{r}(T+1) \leq 2^T(T+1).$$

Next

$$\left| e^{-\lambda} \sum_{j=0}^{\infty} \frac{\lambda^j}{j!} Q(j) - e^{-\lambda} \frac{\lambda^r}{r!} \right| \leq e^{-\lambda} \sum_{j>T} \frac{\lambda^j}{r!(T-r)!(j-r)(j-T-1)!}$$

and putting these inequalities together, we get

$$\left| \sum_{j=0}^{\infty} d_j Q(j) - e^{-\lambda} \frac{\lambda^r}{r!} \right| \leq 2^T(T+1) \sum_{m=0}^{T} \beta_m + \frac{\lambda^{T+1}}{r!(T+1-r)!}$$

Now $\sum d_j Q(j)$ is either $\geq d_r$ or $\leq d_r$ according as $T \equiv r \pmod 2$ or not, and we are free to choose $T = M$ or $M-1$. Using both these values of T, we obtain the result stated.

LEMMA 3. *Let $p(m, h)$ denote the number of partitions of m distinct objects into h disjoint non-empty sets, the ordering of those sets and of the objects within the sets being immaterial. Then we have the identity*

$$\sum_{h=1}^{m} p(m, h) \lambda^h = e^{-\lambda} \sum_{j=0}^{\infty} \frac{j^m}{j!} \lambda^j.$$

Proof. Put $\lambda = e^y$ and denote the function on the left by $\phi_m(y)$: In view of the relation $p(m, h) = hp(m-1, h) + p(m-1, h-1)$ we have $\phi_m(y) = \phi'_{m-1}(y) + e^y \phi_{m-1}(y)$. It follows by induction that

$$\phi_m(y) \exp(e^y) = \frac{d^m}{dy^m} \exp(e^y)$$

and we expand $\exp(e^y)$ in powers of e^y and differentiate term by term.

Proof of Theorem 1. We use the notation $E(X)$ or simply EX for the expectation of the random variable X. The main step in the proof is to find asymptotic formulae for

$$\mu_m = E \sum_g R^m(g) \quad \text{and} \quad \sigma_m^2 = E\Big(\sum_g R^m(g) - \mu_m)^2$$

subject to condition A.

We recall from [3] Lemma 2 the formula

$$\mu_m = \frac{1}{n^{m-1}} \sum_{\chi_1} \sum_{\chi_2} \cdots \sum_{\chi_m} N^k(\chi_1, \chi_2, \dots, \chi_m)$$

where the sums are over all $\chi \in \hat{G}$ except in the innermost sum: here the dash indicates that $\chi_1\chi_2 \cdots \chi_m = \chi_0$ so that really this sum has just one term. $N(\chi_1, \chi_2, \dots, \chi_m)$ is the number of solutions of $\chi_1^{\varepsilon_1}\chi_2^{\varepsilon_2} \cdots \chi_m^{\varepsilon_m} = \chi_0$ so that $2 \leqslant N \leqslant 2^m$. We rewrite this in the form

$$\mu_m = \frac{1}{n^{m-1}} \sum_N M_m(\hat{G}, N) N^k$$

where $M_m(\hat{G}, N) = \operatorname{card}\{\chi_1, \chi_2, \dots, \chi_m : \chi_1\chi_2 \cdots \chi_m = \chi_0$ and $N(\chi_1, \chi_2, \dots, \chi_m) = N\}$. We proved in [3] Lemmas 1, 2

$$M_m(\hat{G}, N) \leqslant \binom{2^m}{N} n^\rho \quad \text{where} \quad \rho = \left[m - \frac{\log N}{\log 2} \right].$$

Let us define

$$\tau = \tau(m) = \max \left\{ \frac{\log N}{\log 2} + \left[-\frac{\log N}{\log 2} \right] : 2 \leqslant N \leqslant 2^m, N \neq 2^h \right\}.$$

All we need is that $\tau < 0$ for every m; in fact we have $\tau(m) = (\log 2)^{-1} \log(1 - 2^{-m})$. Then we have

$$\left| \mu_m - \frac{1}{n^{m-1}} \sum_{n=1}^{m} M(\hat{G}, 2^h) 2^{hk} \right| \leqslant n^{1+\tau} \sum_N \binom{2^m}{N} N^{k - (\log n)/(\log 2)},$$

and the right hand side does not exceed $n^{1+\tau} 2^{2^m} \lambda^m$.

It remains to consider $M_m(\hat{G}, 2^h)$. As G and $\hat{G}$ are isomorphic, this is equal to $M_m(G, 2^h)$, the number of sets $g_1, g_2, \dots, g_m$ such that $g_1 + g_2 + \cdots + g_m = 0_G$ and such that exactly 2^h equations

$$\varepsilon_{t,1} g_1 + \varepsilon_{t,2} g_2 + \cdots + \varepsilon_{t,m} g_m = 0_G, \qquad (1 \leqslant t \leqslant 2^h)$$

are satisfied. Let S denote such a system of $N = 2^h$ equations, $W_m(G, S)$ the number of sets $g_1, g_2, \dots, g_m$ satisfying precisely these equations, and no others, and $W_m^*(G, S)$ the number of sets $g_1, g_2, \dots, g_m$ satisfying these equations and possibly others as well. We have $M_m(G, N) = \sum W_m(G, S)$ where the sum is over all systems S of N distinct equations, also

$$W_m(G, S) = W_m^*(G, S) - \sum W_m^*(G, S') + \sum W_m^*(G, S'') - \cdots$$

where $S \subset S'$, $S \subset S^\circ$, *etc., and* $S', S'', \dots$ run through systems of $N+1, N+2, \dots$ equations. We always have $W_m(G, S) = W_m^*(G, S) - \theta \sum W_m^*(G, S')$ for some $\theta = \theta(S) \in [0, 1]$.

With each equation in a given system S we associate the vector $\mathbf{u}_t \in \mathbf{R}^m$ with coordinates $\{\varepsilon_{t,1}, \varepsilon_{t,2}, \ldots, \varepsilon_{t,m}\}$. Thus $\mathbf{u}_t$ is a vertex of the hypercube C^m. Let K be the subspace of $\mathbf{R}^m$ spanned by the vectors $\mathbf{u}_t$. Since K intersects C^m in 2^h vertices, we have $\dim K \geqslant h$, and we distinguish the two cases $\dim K > h$, $\dim K = h$.

Suppose then that $\dim K = l > h$. We can find l of our vectors, say $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_l$ which are a basis for K, and we have to solve the equations $\varepsilon_{t,1}g_1 + \varepsilon_{t,2}g_2 + \cdots + \varepsilon_{t,m}g_m = 0_G (1 \leqslant t \leqslant l)$. The matrix $\{\varepsilon_{i,j}\ 1 \leqslant i \leqslant l, 1 \leqslant j \leqslant m\}$ has rank l and so we can find l independent columns, say the first l. It follows from Cramer's rule that given $g_{l+1}, g_{l+2}, \ldots, g_m$, of which there are n^{m-l} choices, Δg_i is determined for each $i \leqslant l$ where Δ is the determinant $\|\varepsilon_{i,j}\|\ (1 \leqslant i \leqslant l, 1 \leqslant j \leqslant l)$. It follows that $W_m(G, S) \leqslant W_m^*(G, S) \leqslant n^{m-l}\omega(G, \Delta)$ and so

$$\left| M_m(G, 2^h) - \sum{}' W_m(G, S) \right| \leqslant \binom{2^m}{2^h} n^{m-h-1}\omega^*(G, m!),$$

where the dash denotes that the K associated with S has dimension h. Let S' be a system of $N+1$ equations, $S' \supset S$. Plainly the K' associated with S' has dimension exceeding h, moreover when we sum over S each S' has to be considered N times, and so $\leqslant N$ times in the restricted sum above. Thus

$$\left| M_m(G, 2^h) - \sum{}' W_m^*(G, S) \right| \leqslant (2^h + 1)\binom{2^m}{2^h} n^{m-h-1}\omega^*(G, m!).$$

If K is a subspace of $\mathbf{R}^m$ intersecting C^m in the maximum number 2^h of vertices, by Lemma 1 there exists vertices $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_h$ which are orthogonal and such that the $\mathbf{u}_t$ associated with S are just $\varepsilon_1\mathbf{v}_1 + \varepsilon_2\mathbf{v}_2 + \cdots + \varepsilon_h\mathbf{v}_h$ in some order. We relabel so that $\mathbf{v}_i = \mathbf{u}_i$ for $i \leqslant h$ thus $\mathbf{v}_i$ has coordinates $\{\varepsilon_{i,1}, \varepsilon_{i,2}, \ldots, \varepsilon_{i,m}\}$. Since S contains the equation $g_1 + g_2 + \cdots + g_m = 0_G$, one of the $\mathbf{u}_t$'s is the vertex of C^m opposite the origin: this vertex must be $\mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_h$. Therefore for every $j \leqslant m$, there is exactly one $i \leqslant h$ such that $\varepsilon_{ij} = 1$. Hence the number of ways of choosing $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_h$ is $p(m, h)$, and each choice gives a different S. Moreover, each of these special systems S has exactly n^{m-h} solutions, for the equation corresponding to $\mathbf{v}_i$ determines one group element for each $i \leqslant h$, and the others may be chosen freely. Hence

$$\sum{}' \overset{*}{W}_m(G, S) = p(m, h)n^{m-h}$$

and putting all our inequalities together, we get

$$\left| \mu_m - n \sum_{h=1}^{m} p(m, h)\lambda^h \right| \leqslant 2^{2^m}\lambda^m(n^{1+\tau} + (2^m + 1)\omega^*(G, m!))$$

It follows that if G satisfies Condition A, we have for each fixed m that

$$\mu_m \sim n \sum_{h=1}^{m} p(m, h)\lambda^h \quad \text{as} \quad n \to \infty.$$

We need an upper bound for σ_m and we begin from the formula

$$\mu_m^2 + \sigma_m^2 = E\Big(\sum_g R^m(g)\Big)^2 = \frac{1}{n^{2m-2}} \sum N^k(\chi_1, \chi_2, \ldots \chi_m, \chi_1', \chi_2', \ldots \chi_m')$$

where the sum is over all sets of characters $\chi_1, \chi_2, \ldots, \chi_m, \chi_1', \chi_2', \ldots, \chi_m'$ satisfying both $\chi_1\chi_2 \cdots \chi_m = \chi_0$ and $\chi_1'\chi_2' \cdots \chi_m' = \chi_0$. This is proved by the method used in [3] Lemma 2. the calculation that remains is very similar to the one for μ_m and we do not give the details: the conclusion is that provided G satisfies Condition A, we have $\sigma_m = o(n)$ for each fixed m.

We apply Tchebycheff's inequality and deduce that for each fixed m there is a function $\beta_m(n)$ such that $\beta_m(n) \to 0$ as $n \to \infty$ and such that with probability $\to 1$ as $n \to \infty$, we have

$$\Big| \sum_g R^m(g) - n \sum_{h=1}^{m} p(m, h)\lambda^h \Big| < n\beta_m(n) \tag{1}$$

Let us denote by $\gamma_m(n)$ the probability that this inequality is false, so that $\gamma_m(n) \to 0$ as $n \to \infty$. By a familiar diagonal argument, we can find an $M = M_n$ such that simultaneously:

$$M_n \to \infty, \sum_{m=0}^{M} \gamma_m(n) \to 0, 2^M(M+1) \sum_{m=0}^{M} \beta_m(n) \to 0,$$

as $n \to \infty$. Therefore with probability $\to 1$ as $n \to \infty$, (1) holds for every $m \leq M$ and so by Lemma 2, we have

$$\Big| d(r) - ne^{-\lambda} \frac{\lambda^r}{r!} \Big| \leq n.2^M(M+1) \sum_{m=0}^{M} \beta_m(n) + n.\frac{\lambda^M(1+\lambda)}{r!(M-r)!}$$

for each $r < M$. For any fixed r, ultimately $M > r$, moreover since $\lambda = O(1)$, the right hand side is $o(n)$. This completes the proof.

Proof of Theorem 2. When g is cyclic we have $\omega^*(G, m!) \leq m!$ and therefore

$$\Big| \mu_m - n \sum_{h=1}^{m} p(m, h)\lambda^h \Big| \leq 2^{2^m} \lambda^m (n^{1+\tau} + (2^m + 1)m!).$$

Recall that $\tau(m) = (\log 2)^{-1} \log(1 - 2^{-m}) < -2^{-m}/\log 2$. Hence there exists an absolute constant C such that the left hand side does not exceed $Cn\lambda^m \exp(-a\sqrt{\log n})$ provided $2^m \leq \sqrt{\log n}$: here $a = (\log 2)^{-1} - \log 2$. In a similar way, it can be shown that provided $4^m \leq \sqrt{\log n}$ we have $\sigma_m^2 \leq C'n^2\lambda^{2m} \exp(-a\sqrt{\log n})$. Let us set $\beta_m(n)=2Cn\lambda^m\exp(-\frac{1}{3}a\sqrt{\log n})$. Then we have

$$\begin{aligned}\gamma_m(n)&=\operatorname{prob}\left(\left|\sum_g R^m(g)-n\sum_{h=1}^m p(m,h)\lambda^h\right|\geq\beta_m(n)\right)\\&\leq\operatorname{prob}\left(\left|\sum_g R^m(g)-\mu_m\right|\geq Cn\lambda^m\exp\left(-\frac{1}{3}a\sqrt{\log n}\right)\right)\\&\leq C'C^{-2}\exp\left(-\frac{1}{3}a\sqrt{\log n}\right).\end{aligned}$$

by Tchebycheff's inequality. Let $M=M_n$ be the greatest integer such that $4^M\leq\sqrt{\log n}$, and suppose that $\lambda^M\leq\exp(\frac{1}{4}a\sqrt{\log n})$. Then we have

$$M\to\infty,\ \sum_{m=0}^M\gamma_m(n)\to 0,\ 2^M(M+1)\sum_{m=0}^M\beta_m(n)\to 0$$

as $n\to\infty$. Therefore with probability $\to 1$ as $n\to\infty$ we have by Lemma 2 as before that

$$|d(0)-ne^{-\lambda}|\leq n2^M(M+1)\sum_{m=0}^M\beta_m(n)+n\frac{\lambda^M}{M!}(1+\lambda).$$

Let us suppose that $d(0)=0$. Then we have

$$e^{-\lambda}\leq C''(\log n)\exp\left(-\frac{1}{3}a\sqrt{\log n}\right)+\frac{\lambda^M}{M!}(1+\lambda)$$

for a suitable absolute constant C'', and if $\lambda\leq M/4$, this is a contradiction if n is large enough. Thus $d(0)>0$, indeed $d(0)\sim ne^{-\lambda}$. This proves the theorem, and gives $1/16\log 2$ as a permissible value of b.

REFERENCES

[1] BOGNÁR K. *On a problem of statistical group theory.* Studia Scientiarum Mathematicaium Hungarica *5* (1970) 29–36.

[2] ERDÖS P. and RÉNYI A., *Probabilistic methods in group theory.* J. Analyse Math. *14* (1965) 127–138.

[3] ERDÖS P. and HALL R. R., *Probabilistic methods in group theory II.* Houston Journal of Mathematics *2* (1976) 173–180.

[4] HALL R. R., *On a theorem of Erdös and Rényi concerning Abelian groups.* J. London Math. Soc. (2) *5* (1972) 143–153.

[5] HALL R. R. and SUDBERY A., *On a conjecture of Erdös and Rényi concerning Abelian groups.* J. London Math. Soc. (2) *6* (1972) 177–189.

[6] HALL R. R., *Extensions of a theorem of Erdös-Rényi in probabilistic group theory.* Houston Journal of Mathmematics *3* (1977) 225–234.

[7] MIECH R. J., *On a conjecture of Erdös and Rényi I11.* J. Math. *11* (1967) 114–127.

[8] WILD K., *A theorem concerning products of elements of Abelian groups.* Proc. London Math. Soc., (3) *27* (1973) 600–616.

P. Erdös
Mathematical Institute of the Hungarian Academy of Sciences Budapest

R. R. Hall
Department of Mathematics University of York England

Received October 25, 1977