ON A CONJECTURE OF ERDÖS AND RÉNYI

BY
R. J. MIECH

Let G be a finite Abelian group of order n, $a_1, \cdots, a_k$ be a sequence of elements of G, and let

$$B = B(a_1, \cdots, a_k) = \{\varepsilon_1 a_1 + \cdots + \varepsilon_k a_k : \varepsilon_i = 0 \text{ or } 1, i = 1, \cdots k\}.$$

Note that if $B = G$ then we must have $k \geq (\log n)/\log 2$. In a recent paper [1] Erdös and Rényi raised the question: how large must k be in order that every element b of G have approximately the same number of representations of the form

$$b = \varepsilon_1 a_1 + \cdots + \varepsilon_k a_k$$

for nearly every sequence $a_1, \cdots, a_k$ of G? In other words, how large must k be in order that nearly every sequence $a_1, \cdots, a_k$ of G will generate G in a uniform fashion? They proved that any k such that

$$k \geq (2 \log n + c)/\log 2,$$

where c is a certain constant, is sufficient and they conjectured that the coefficient of $\log n$ in this inequality, 2, could not be replaced by anything better. The purpose of this paper is to show that the 2 can be replaced by $\frac{3}{2}$ for most groups and that the conjecture, if it is true, is valid only for groups of a particular nature.

Several definitions are needed before precise results can be stated. Let G_k be the Cartesian product of k copies of G, let P be the probability measure on G_k whose value at each point of G_k is n^{-k}, and let, for each b in G, $V_k(b)$ be the random variable whose value at each point $(a) = (a_1, \cdots, a_k)$ of G_k is given by

$$V_k(b, (a)) = N\{(\varepsilon_1, \cdots, \varepsilon_k) : \varepsilon_1 a_1 + \cdots + \varepsilon_k a_k = b\}$$

where $N\{\mathfrak{U}\}$ is the number of elements in the set $\mathfrak{U}$. Suppose, furthermore, that if G is expressed as a direct sum of cyclic groups of prime power order then r of the summands have orders that are powers of 2. Then we have the

THEOREM. *Let G be a finite Abelian group of order n and let P, $V_k(b)$, and r be defined as above. Let ε and δ be any fixed positive numbers. Then if k is any integer such that*

$$k \geq \left(\max\left\{\frac{3}{2} \log n, \log n + r \log 2\right\} + 4 \log \frac{1}{\epsilon} + \log\right) \frac{1}{\log 2} + 8$$

Received December 9, 1965.

we have

$$P\{\max_{b \epsilon G} | V_k(b) - 2^k/n | < \varepsilon \cdot 2^k/n\} > 1 - \delta.$$

It is also quite easy to show, using a result of [1], that if all of the summands of G are of order 2, in which case G is of order 2^r, then the conclusion of this theorem holds provided that

$$k \geq \frac{1}{\log 2}\left(r \log 2 + \log r + 2 \log \frac{1}{\delta}\right) + 5.$$

Thus, the Erdös-Rényi conjecture will hold only if the direct sum decomposition of G contains a relatively large number of groups of order 2 and a small positive number of groups whose order exceeds 2. I suspect that the coefficient of $\log n$ can be reduced to $\frac{3}{2}$ for these exceptional cases, but so far I have been unable to prove it.

A large part of this paper is devoted to an examination of $3 \times k$ and $4 \times k$ 0-1 matrices, for the proof of the theorem is based on the value of a fourth moment and the calculation of this moment depends on certain properties of these matrices.

Section 1

It will be evident later that the main problem we have is that of finding the number of solutions of the system of equations

$$(1) \qquad \varepsilon_{i1}\, a_1 + \cdots + \varepsilon_{ik}\, a_k = b$$

where $i = 1, \cdots, j$, $A = (\varepsilon_{pq})$ is a 0-1 matrix of rank j and $j = 1, 2, 3$, or 4. Under certain circumstances the problem is very simple, for since row and columns can be interchanged and rows can be added and subtracted in (1) without changing the nature of the system it is equivalent to a system of the form

$$(2) \qquad \begin{aligned} \delta_{11}\, a_1 + \cdots + \delta_{1k}\, a_k &= \delta_1\, b \\ \delta_{22}\, a_2 + \cdots + \delta_{2k}\, a_k &= \delta_2\, b \\ \delta_{jj}\, a_j + \cdots + \delta_{jk}\, a_k &= \delta_j\, b \end{aligned}$$

where the δ's are integers and $\delta_{11}, \cdots, \delta_{j-1\, j-1}\, \delta_{jv}$ is the determinant of a $j \times j$ minor of A for $v = j, \cdots, k$. Thus if one of these determinants is equal to 1 or, more generally, relatively prime to the order of the group G the system has n^{k-j} solutions for every b in G.

Those systems of the form (1) for which $|\det A_j| \geq 2$ where A_j is any non-singular $j \times j$ minor of A are less transparent. Since $|\det A_j| \leq 1$ if $j = 1$ or 2 we begin with the case $j = 3$. Then we have

$$(3) \qquad |\det A_3| \leq 2$$

and, if any matrix that is obtained by interchanging the rows and columns of a given matrix is considered to be equal to the given matrix,

$$\text{(4)} \qquad \text{if } |\det A_3| = 2 \quad \text{then} \quad A_3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

To prove (3) note that if A_3 is a non-singular 3×3 0-1 matrix then A_3 must contain a 0, hence its determinant can be expressed as a sum of at most two 2×2 0-1 matrices; (4) is a consequence of the facts that if $|\det A_3| = 2$ then no row or column of A_3 contains two or three 0's and if A_3 contains no, one or two 0's, then $|\det A_3| \leq 1$. In short, if A is a $3 \times k$ matrix that is of interest to us it must contain the three columns $C_1 = (1, 0, 1)'$, $C_2 = (1, 1, 0)'$, and $C_3 = (0, 1, 1)'$, where the prime indicates the transpose. One can also show that A cannot contain any other non-zero column C, for if it did then at least one of the minors (C_1, C_2, C), (C_1, C_3, C) or (C_2, C_3, C) would have a value of 1, that is, the absolute value of the determinant of one of these minors would be equal to 1. These results imply that $\delta_{11} = \delta_{22} = 1$, $\delta_{33} = 2$, $\delta_{3v} = 0$ or ± 2 for $v = j + 1, \cdots, k$, $\delta_3 = 1$ in (2), and that the last equation of this system can be written as

$$2(a_3 + \lambda_4 a_4 + \cdots + \lambda_k a_k) = b,$$

where $|\lambda_i| = 0$ or 1. Suppose now that G is expressed as a direct sum,

$$G = H_1 \oplus \cdots \oplus H_r \oplus K_1 \oplus \cdots \oplus K_s .$$

where H_i, which is generated by h_i, is of order 2^{e_i} and K_i, which is generated by k_i, if of order p^{f_i} where p_i is an odd prime. Then if

$$b = v_1 h_1 + \cdots + v_r h_r + t_1 k_1 + \cdots + t_s k_s$$

and $v_i \equiv 0 \bmod 2$ for $i = 1, 2, \cdots, r$ the system of equations has $2^r n^{k-3}$ solutions. If b is not equal to $2g$ where g is some element of G there are no solutions. Since there are $n/2^r$ elements b of G for which the system is solvable we have proved:

LEMMA 1. *Let A be a $3 \times k$ 0-1 matrix that is of rank 3 and let $p(b, A)$ be the number of solutions of the system of equations* (1). *Then*

$$\textstyle\sum_{b \in G} p(b, A) = n^{k-2}.$$

Note also that if R_1 is the set of rank 3 $3 \times k$ matrices A such that $|\det A_3| = 2$ for every non-singular 3×3 minor of A then $N(R_1)$, the number of such matrices does not exceed $3!\, 4^k$, for A can only contain the columns C_1, C_2, C_3 and the zero column. Furthermore if A is in R_1 and $b = 0$ then (1) has $2^r n^{k-3}$ solutions since the condition $v_i \equiv 0 \bmod 2$ for $i = 1, 2, \cdots, r$ is always satisfied if $b = 0$.

If $j = 4$ we can prove

LEMMA 2. *Let A be a $4 \times k$ 0-1 matrix that is of rank 4 and let $q(b, A)$ be the number of solutions of* (1). Then

$$\sum_{b\epsilon G} q(b, A) = En^{k-3} \tag{5}$$

where $E = 1$ *or* $E = 2^r$. *Moreover, the number of matrices A for which* $E = 2^r$ *does not exceed* $4!\ 8^k$.

We assume as usual that if A_4 is any non-singular minor of A then $|\det A_4| \geq 2$. Equation (5) will be proved once we establish that

$$|\det A_4| \leq 3 \tag{I}$$

This implies that we can set $\delta_{11} = \delta_{22} = \delta_{33} = 1$ in (2).

(II) If $|\det A_4| = 3$ for some minor of A then $|\det A_4'| = 0$ or 3, where A_4' is any other minor of A, and δ_4, the coefficient of b in the last equation of (2), is equal to ± 1.

Under these circumstances the last equation in (2) can be written as

$$3(a_4 + \lambda_5 a_5 + \cdots + \lambda_k a_k) = \pm b$$

where $|\lambda_i| = 0$ or 1. Hence, if the direct sum decomposition of G into cyclic groups of prime power order contains s groups whose orders are powers of 3, the system has no or $3^s n^{k-4}$ solutions and there will be $n/3^s$ elements b of G for which it is solvable.

(III) If $|\det A_4| = 2$ for some non-singular minor of A then $|\delta_4| \leq 2$ and the last equation of (2) can be written as

$$2(a_4 + \lambda_5 a_5 + \cdots + \lambda_k a_k) = \delta_4 b.$$

Thus if $\delta_4 = 0$, 2, or -2 the system will have $2^r n^{k-4}$ solutions for every b in G; if $\delta_4 = 1$ or -1 the system has no or $2^r n^{k-4}$ solutions and there are $n/2^r$ elements b of G for which it is solvable.

These facts will be proved by classifying 4×4 matrices according to the number and distribution of their 0's. The pattern of our argument will be determined by non-singular matrices which have at least two 1's in each row and each column and at least one row or column that contains two 0's.

We begin by examining exceptions. Suppose first of all that a non-singular minor A_4 of A contains three 0's in a column. Then system (1) assumes a form which can be treated by the methods employed for the case $j = 3$. Equation (5) holds with $E = 1$ in this case.

Suppose next that no non-singular minor A_4 of A contains three 0's in a column but that one of these minors has a row that contains three 0's. Then, since $|\det A_4| \geq 2$,

$$A_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ x & 1 & 0 & 1 \\ y & 0 & 1 & 1 \\ z & 1 & 1 & 0 \end{pmatrix} \tag{6}$$

where x, y, and z are 0's or 1's and $x + y + z \neq 0$. We also have $\delta_{44} = 2$ and $\delta_4 = 1 - x - y + z$ in (2).

We have to find the type and number of matrices A that can contain (6) as a minor. To this end, let us list the possible non-zero columns of A as:

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}
0	0	0	1	1	1	1	1	1	0	1	1	0	0	0
1	0	1	1	0	0	1	1	0	1	1	0	1	0	0
0	1	1	0	1	0	1	0	1	1	1	0	0	1	1
1	1	0	0	0	1	0	1	1	1	1	0	0	0	1

Set $V = (1, x, y, z)'$; thus $A_4 = (V, C_1, C_2, C_3)$. Suppose next that A contains a non-zero column $C = (\alpha, \beta, \delta, \varepsilon)'$ that is distinct from those of A_4. We have

$$\det (V, C_1, C_2, C) = \alpha(x + y - z) - \beta - \delta + \varepsilon$$

$$\det (V, C_1, C_3, C) = \alpha(x - y - z) - \beta + \delta + \varepsilon$$

$$\det (V, C_2, C_3, C) = \alpha(x - y + z) - \beta + \delta - \varepsilon$$

and we know that A cannot contain any column C for which one of these determinants is equal to ± 1.

If, for example $x = 0, y = 0, z = 1$ then $V = C_6$ and all columns C, except except $C = C_4$, C_5, or C_{11} can be eliminated from consideration. We also have $\det (V, C_1, C_2, C) = 0, 2$, or -2 when $C = C_4$, C_5 or C_{11}, consequently the last equation in (2) can be written in the form

$$2(a_4 + \lambda_5 a_5 + \cdots + \lambda_k a_k) = \delta_4 b.$$

A similar result holds for the remaining values of x, y, z for which $\delta_4 = 1 - x - y + z = 0$ or 2: V must be one of the columns C_4, C_5, C_6, C_{11}, the remaining three are the only others that might appear in A, and the last equation of (2) has the form given above. These matrices give us the $\delta_4 = 0, 2$, or -2 case of (III); in addition since they contain at most eight distinct columns, the seven just mentioned and the zero column, their number does not exceed $4!\, 8^k$.

We consider next those values of x, y, z for which $\delta_4 = 1 - x - y + z = \pm 1$. If $x = 1, y = 1, z = 0$ then $V = C_7$ and, as an examination of the three determinants above shows, the only non-zero columns that can be adjoined to A are C_8 and C_9. Furthermore since $\det (C_7, C_1, C_2, C_3) = 2$ for $j = 8$ or 9 the last equation of (2) assumes the form given in (III). Similar results hold if $x = 1, y = 0, z = 1$ or $x = 0, y = 1, z = 1$. In each case V is one of the columns C_7, C_8, C_9, the remaining two are the only non-zero columns that can be adjoined to A, and the last equation of (2) takes on the form given in (III). The conclusion of Lemma 2 holds with $E = 1$ for these cases.

We can now assume that any non-singular minor A_4 of A has at most two 0's in any row or column; we would also like to assume that A_4 has a row or column containing two 0's. If it doesn't then it contains at most 4. But if

A_4 has no, one, two, or three 0's then $|\det A_4| \leq 1$. If it contains four 0's we can have

$$(7) \qquad A_4 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} = (C_9, C_8, C_7, C_{10}),$$

since $|\det A_4| = 3$. Since, if $C = (\alpha, \beta, \delta, \varepsilon)'$,

$$\det(C_9, C_8, C_7, C) = -2\alpha + \beta + \delta + \varepsilon,$$

$$\det(C_9, C_8, C_{10}, C) = -\alpha - \beta - \delta + 2\varepsilon,$$

$$\det(C_9, C_7, C_{10}, C) = \alpha + \beta - 2\delta + \varepsilon,$$

$$\det(C_8, C_7, C_{10}, C) = -\alpha + 2\beta - \delta - \varepsilon,$$

and since at least one of these determinants is equal to ± 1 for every non-zero columns C distinct from those of A_4, one can say that A must contain the columns C_9, C_8, C_7, C_{10} and cannot contain any other non-zero column. Straight-forward calculations show that $\delta_4 = 1$ in this case, so the situation here is the one described in (II).

We can now assume that for every non-singular minor A_4 of A: (M_1), $|\det A_4| \geq 2$; (M_2), no row or column of A_4 contains three 0's; (M_3), at least one row or column of A_4 contains two 0's. Then

$$A_4 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & x \\ 1 & 1 & y & z \\ 1 & u & v & w \end{pmatrix}$$

where the roman letters denote 0's or 1's. To see this set

$$A_4 = (a_{ij}), \qquad i, j = 1, 2, 3, 4.$$

If we assume that a column of A_4 contains two 0's then, after interchanging rows and columns, we can conclude that $a_{11} = a_{21} = 0$. Hence, by M_2, $a_{31} = a_{41} = 1$ Now, if $a_{ij} = 1$ for $i = 1, 2$ and $j = 2, 3, 4$ then the first two rows of A are identical; thus at least one of these elements must be a 0. Assume that $a_{12} = 0$. Since $a_{11} = a_{12} = 0$ we have, by M_2, $a_{13} = a_{14} = 1$. If $a_{22} = 0$ then, by M_2, $a_{23} = a_{24} = 1$, and the first two rows of A are identical, hence $a_{22} = 1$. Condition M_2 also implies that $a_{23} = 1$ or $a_{24} = 1$; assume that $a_{23} = 1$. Similarly, $a_{32} = 1$. If we assume that A_4 has a row containing two 0's we get the same result. The following form of A_4 will be more convenient than the one above for our purposes:

$$(8) \qquad A_4 = \begin{pmatrix} 1 & u & v & w \\ 0 & 1 & 1 & x \\ 0 & 0 & 1 & 1 \\ 1 & 1 & y & z \end{pmatrix}$$

Note that

$$\det A_4 = v + z - w - y + (1 - x)(1 - u). \tag{9}$$

Let us first consider a matrix A which satisfies conditions M_1, M_2, M_3 and which contains a minor A_4 such that $|\det A_4| = 3$. Then, by (9), $x = 0, y = 0, z = 1, u = 0, v = 1, w = 0$, so

$$A_4 = (C_6, C_1, C_7, C_2).$$

Since, if $C = (\alpha, \beta, \delta, \varepsilon)'$

$$\det(C_6, C_1, C_7, C) = -\alpha - \beta + 2\delta + \varepsilon$$

$$\det(C_6, C_7, C_2, C) = -\alpha + 2\beta - \delta + \varepsilon$$

$$\det(C_1, C_7, C_2, C) = -2\alpha + \beta + \delta - \varepsilon$$

we can now show in the usual fashion that any matrix A that contains A_4 contains precisely four distinct kinds of non-zero columns, C_6, C_1, C_7 and C_2. Since $\delta_4 = 1$ in this case, (II) holds.

We can now replace the condition M_1, $|\det A_4| \geq 2$, by $|\det A_4| = 2$. Then $\delta_{44} = 2$, $\delta_{4v} = 0$ or 2 for $v = 5, \cdots, k$, and $\delta_4 = v - y$ in (2). If $v \neq y$ there is no problem; (5) holds with $E = 1$. If $v - y = 0$, then by (9)

$$|\det A_4| = |v - y + z - w + (1 - x)(1 - u)| = 2,$$

and it follows that $z = 1$, $w = 0$, $x = 0$, $u = 0$. If $v = y = 0$ then $u = v = w = 0$ and the matrix A_4 of (8) has three 0's in a row so this possibility need not be considered. If $v = y = 1$ then

$$A_4 = (C_6, C_1, C_{11}, C_2).$$

Since

$$\det(C_6, C_1, C_{11}, C) = -\alpha - \beta + \delta + \varepsilon$$

a matrix A that contained the columns C_6, C_1, C_{11}, C_2 might also contain the columns C_3, C_4, C_5, but it cannot contain any other non-zero columns. Since all the matrices of this type were included when the previous bound was computed the number of matrices A such that $E = 2^r$ does not exceed $4!\ 8^k$. This completes the proof of Lemma 2.

We now turn to the problem of determining the number of solutions of a system (1) where the matrix A has no row that is identically zero, does not have two identical rows, and is not of rank j. If $j = 1$ or 2 there is no problem. If $j = 3$, A might be of rank 2. In this case one of its rows, say the third, is a linear combination of the other two, so, if $A = (\varepsilon_{pq})$, there are numbers δ_1 and δ_2 such that

$$\delta_1 \varepsilon_{1q} + \delta_2 \varepsilon_{2q} = \lambda_q,$$

where $\lambda_q = 0$ or 1, for $q = 1, \cdots, k$. Moreover, there are integers v and t such that the system of equations

$$\delta_1 \varepsilon_{1v} + \delta_2 \varepsilon_{2v} = \lambda_v$$

$$\delta_1 \varepsilon_{1t} + \delta_2 \varepsilon_{2t} = \lambda_t$$

has one solution. Solving it, we see that $\delta_i = -1, 0,$ or 1. Now, we cannot have $\delta_1 = 0$ or $\delta_2 = 0$ for then one row of A would be identical to another. If $\delta_1 = \delta_2 = 1$ then we must have

$$(\varepsilon_{1q}, \varepsilon_{2q})' = (1, 0)' \quad \text{or} \quad (0, 1)' \quad \text{or} \quad (0, 0)'$$

and

$$(\varepsilon_{1q}, \varepsilon_{2q}, \varepsilon_{3q})' = (1, 0, 1)' = C_1 \quad \text{or} \quad (0, 1, 1)' = C_2 \text{ or } (0, 0, 0)'.$$

That is, if $\delta_1 = \delta_2 = 1$, A must contain the columns C_1 and C_2 and cannot contain any other non-zero columns; similar considerations for those cases where $\delta_1 \delta_2 = -1$ lead to a matrix that can be obtained by interchanging the rows of this C_1, C_2 matrix. Thus, if the 1st through the u^{th} columns of A are of the form C_1 and the $(u + 1)^{\text{st}}$ through the w^{th} are of the form C_2 then the system (1) must be of the form

$$\begin{aligned} B_1 &= b \\ B_1 + B_2 &= b \\ B_2 &= b \end{aligned} \tag{10}$$

where $B_1 = a_1 + \cdots + a_u$ and $B_2 = a_{u+1} + \cdots + a_w$. This system has n^{k-2} solutions if $b = 0$ and no solutions if $b \neq 0$. Furthermore, if Q_0 is the set of $3 \times k$ matrices associated with a system of the form (10) then $N(Q_0)$, the number of such matrices, does not exceed $3!\, 3^k$.

If $j = 4$ and A is not of rank 4 then A is of rank 3. For if it were of rank 2 then B, the matrix that consists of the first three rows of A, would be of rank 2. However, if B is of rank 2 then it contains but two distinct kinds of non-zero columns; this implies that A has two identical rows, a contradiction to our assumptions. The essential facts about rank 3 matrices are summarized in

LEMMA 3. *The set of* $4 \times k$ *matrices* A *of rank* 3 *such that no row of* A *is identically zero and no two rows of* A *are identical can be split into three sets* Q_1, Q_2, Q_3 *relative to the system of equations* (1). Q_1 *consists of those matrices for which the associated system is solvable if and only if* $b = 0$, Q_2 *those for which the system is solvable if and only if* $2b = 0$, *and* Q_3 *those for which the system is solvable for every* b *in* G. *Moreover, if in each case the system is solvable then there are* n^{k-3} *solutions. We also have* $N(Q_2) \leq 4!\, 4^k$ *and* $N(Q_3) \leq 4!\, 6^k$.

This lemma will be proved, as usual, by considering the possible forms the columns might take. If it is assumed that the last row of $A = (\varepsilon_{pq})$ is a linear combination of the first three then there are numbers δ_1, δ_2, δ_3 such that

$$\delta_1 \varepsilon_{1q} + \delta_2 \varepsilon_{2q} + \delta_3 \varepsilon_{3q} = \lambda_q,$$

where $\lambda_q = 0$ or 1, for $q = 1, \cdots, k$. Since A is of rank 3 one can show, by solving an appropriate system of equations, that $\delta_i = 0, \pm\frac{1}{2}, \pm 1$, or ± 2. It is clear that not all three of the numbers $\delta_1, \delta_2, \delta_3$ are negative. Furthermore if δ_1, δ_2, and δ_3 are fixed and x, y, and z are considered to be the first three entries of a column of A then the equation

$$\delta_1 x + \delta_2 y + \delta_3 z = 0 \text{ or } 1 \tag{11}$$

must have three distinct non-zero solutions, since A is of rank 3. Finally, if (11) has exactly three non-zero solutions (x_i, y_i, z_i) then the matrix

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \\ t_1 & t_2 & t_3 \end{pmatrix}$$

where $t_i = \delta_1 x_i + \delta_2 y_i + \delta_3 z_i$, cannot have two identical rows nor can any row be identically zero if it is to be of interest to us.

We shall now consider particular values of $\delta_1, \delta_2, \delta_3$. Suppose first of all that for some fixed selection of $\delta_1, \delta_2, \delta_3$ at least one of the δ_1 is equal to $\pm\frac{1}{2}$. We cannot have exactly one of them, say δ_1, equal to $\pm\frac{1}{2}$ for then the first row of A would be identically zero. If exactly two, say δ_1 and δ_2 were equal to $\pm\frac{1}{2}$ the first and second row of A would be identical. We can have $\delta_1 = \delta_2 = \delta_3 = \frac{1}{2}$ or $\delta_1 = \delta_2 = \frac{1}{2}, \delta_3 = -\frac{1}{2}$. Then the non-zero columns of A have the forms

$$\begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{matrix} \qquad \text{or} \qquad \begin{matrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{matrix}$$

and simple computations show that A belongs to Q_1 in each case. These two selections, and their permutations, exhaust all the selection of $\delta_1, \delta_2, \delta_3$ that contain at least one $\pm\frac{1}{2}$. The only other possibility $\delta_1 = \frac{1}{2}, \delta_2 = \delta_3 = -\frac{1}{2}$ can be ruled out since (11) has only two distinct non-zero solutions under these circumstances.

We can now assume that the δ_i are integers. Since a selection of $\delta_1, \delta_2, \delta_3$ that contained two or three 0's would lead to a matrix which has two identical rows or a row of 0's any selection of these numbers that contains at least one 0 contains exactly one 0. Thus, if the three conditions on the δ_i given two paragraphs above are applied to the possible choices, we see that the only selections of $\delta_1, \delta_2, \delta_3$ that contain a 0 are $\delta_1 = 0, \delta_2 = \delta_3 = 1$ and $\delta_1 = 0$, $\delta_2 = 1, \delta_3 = -1$. These three conditions also yield the fact that the only choices of these numbers that contain a ± 2 are $\delta_1 = 2, \delta_2 = -1, \delta_3 = 1$; $\delta_1 = 1, \delta_2 = \delta_3 = -1$; and $\delta_1 = -2, \delta_2 = \delta_3 = 1$. Observe that in all these cases $\delta_1 + \delta_2 + \delta_3 = \lambda = 0$ or 2. Consequently, since the last equation of a system associated with these choices is the sum of the first three,

$$\lambda b = \varepsilon_{41} a_1 + \cdots + \varepsilon_{4k} a_k = b.$$

That is, the system is solvable only if $b = 0$. To establish the converse note that for any one of these particular choices of δ_1, δ_2, δ_3 there always exist two δ's whose sum is not equal to 0 or 1. Therefore B, the matrix consisting of the first three rows of A cannot contain a minor whose value is 2. For if

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

were a minor of B then the corresponding elements of the last row of A, being a sum of two of the δ's, would not consist of 0's and 1's. In short, B contains a minor whose value is 1, so if $b = 0$ the system has n^{k-3} solutions.

Those selections of the δ's which consist solely of $+1$'s and -1's remain. If $\delta_1 = \delta_2 = \delta_3 = 1$ or if $\delta_1 = 1$, $\delta_2 = \delta_3 = -1$ the corresponding matrices must contain the columns

$$\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{matrix} \qquad \text{or} \qquad \begin{matrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{matrix},$$

and cannot contain any other non-zero columns. Since, upon adding the first three equations of the system together, we have

$$\lambda b = \varepsilon_{41} a_1 + \cdots + \varepsilon_{4k} a_k = b$$

where $\lambda = 3$ or -1, it is not difficult to show that these matrices belong to Q_2. Finally, since the second block is a permutation of the rows of the first block, $N(Q_2) \leq 4!\, 4^k$.

If $\delta_1 = \delta_2 = 1$, $\delta_3 = -1$ then the columns of A must have one of the following forms

$$\begin{matrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{matrix}$$

Since $\delta_1 + \delta_2 + \delta_3 = 1$ and since no 3×3 determinant that can be derived from the first three rows of this block has a value of ± 2 any rank 3 matrix whose columns are elements of this block has n^{k-3} solutions for every b in G. We also have $N(Q_3) \leq 4!\, 6^k$, so this completes the proof of Lemma 3.

Section 2

We shall now prove the theorem of this paper. By Tchebichev's inequality

$$P\left\{\max_{b\epsilon G}\left(V_k(b) - \frac{2^k}{n}\right)^2 \geq \left(\frac{\varepsilon\cdot 2^k}{n}\right)^2\right\} \leq \frac{n^4}{2^{4k}\varepsilon^4} E\left[\max_{b\epsilon G}\left(V_k(b) - \frac{2^k}{n}\right)^4\right]$$

where $E[X]$ is the expectation of X. Since

$$E[\max_{b\epsilon G} (v_k(b) - 2^k/n)^4] \leq \sum_{b\epsilon G} E[(V_k(b) - 2^k/n)^4],$$

the theorem will be proved once a suitable bound is established for this sum of expectations.

Several definitions are in order. If $(\varepsilon^i) = (\varepsilon_{i1}, \cdots, \varepsilon_{ik})$ is a 0-1 k-tuple and $(a) = (a_1, \cdots, a_k)$ is an element of G_k let the notation

$$(\varepsilon^1, \cdots, \varepsilon^j; a) = b$$

denote the fact that

$$\varepsilon_{i1} a_1 + \cdots + \varepsilon_{ik} a_k = b$$

for $i = 1, 2, \cdots, j$. Set

$$S(j) = \sum_{b\epsilon G} \sum_{((\varepsilon^1),\cdots,(\varepsilon^j))} P\{(\varepsilon^1, \cdots, \varepsilon^j; a) = b\},$$

where the index of summation runs over those j-tuples $((\varepsilon^1), \cdots, (\varepsilon^j))$ that satisfy the conditions:

$$(\varepsilon^i) \neq (0) \qquad \text{for } i = 1, 2, \cdots, j.$$

$$(\varepsilon^p) \neq (\varepsilon^q) \qquad \text{for } p \neq q,\ 1 \leq p, q \leq j.$$

Let $\mathfrak{U}_1$ be the set of rank 4 4 × k matrices A for which the number E of Lemma 2 is equal to 1, let $\mathfrak{U}_2$ be those for which $E = 2^r$, and let Q_1, Q_2, Q_3 be those described in Lemma 3. Finally let

$$u(j) = (2^k - 1)(2^k - 2) \cdots (2^k - j).$$

Then we have

$$(12) \qquad \begin{aligned} S(j) &= u(j)/n^{j-1} \qquad \text{for } j = 1, 2, 3 \\ S(4) &= \frac{u(4)}{n^3} + \frac{(2^r - 1)}{n^3}(N(\mathfrak{A}_2) + N(Q_2)) + \frac{N(Q_3)}{n^2}\left(1 - \frac{1}{n}\right). \end{aligned}$$

Since the proof of the first three equations is similar to and simpler than the proof of the fourth, the details concerning the last equation will be the only ones given here.

As for these details, let $((\varepsilon^1), \cdots, (\varepsilon^4))$ be considered as a 4 × k matrix A whose i^{th} row is (ε^i). Then, if A is in $\mathfrak{A}_1$,

$$\sum_{b\epsilon G} P\{(\varepsilon^1, \cdots, \varepsilon^4; a) = b\} = 1/n^3$$

Consequently, since the index of summation of the inner sum of $S(4)$ runs over $(2^k - 1) \cdots (2^k - 4) = u(4)$ j-tuples, we have

$$S(4) = \frac{u(4)}{n^3} - \frac{(N(\mathfrak{A}_2) + N(Q_1) + N(Q_2) + N(Q_3))}{n^3} + F$$

where F consists of those terms of $S(4)$ for which $((\varepsilon^1), \cdots, (\varepsilon^4))$ is not in $\mathfrak{A}_1$. According to Lemma 2,

$$\textstyle\sum_{b\epsilon G} \sum_{\mathfrak{A}_2} P\{(\varepsilon^1, \cdots, \varepsilon^4; a) = b\} = (2^r/n^3)N(\mathfrak{A}_2).$$

According to Lemma 3, for $i = 1, 2, 3$

$$\textstyle\sum_{b\epsilon G} \sum_{Q_i} P\{(\varepsilon^1, \cdots, \varepsilon^4; a) = b\} = N(Q_i)w(i)$$

where $w(1) = 1/n^3$, $w(2) = 2^r/n^3$, and $w(3) = 1/n^2$. If these results are brought together we have the stated equation for $S(4)$.

The results of (12) will be used to prove:

$$\sum_{b\epsilon G} E[V_k^j(b)] = v(0) + \frac{j(j-1)}{2}\frac{v(1)}{n} + \frac{(j-1)(j-2)}{2}\frac{v(2)}{n^2}$$

for $j = 1, 2, 3$, and

$$\sum_{b\epsilon G} E[V_k^4(b)] = v(0) + \frac{7v(1)}{n} + \frac{6v(2)}{n^2} + \frac{v(3)}{n^3} + \frac{4N(Q_0) + N(Q_3)}{n^2}\left(1 - \frac{1}{n}\right)$$
$$+ \frac{(2^r - 1)}{n^3}(4N(R_1) + N(\mathfrak{A}_2) + N(Q_2))$$

where $v(l) = 2^k(2^k - 1) \cdots (2^k - l)$. As before, only the last equation will be considered.

To prove the last equation let, for each fixed b and (ε), $X[b, \varepsilon]$ be the random variable whose value at the point $(a) = (a_1, \cdots, a_k)$ of G_k is given by

$$\begin{aligned} X[b, \varepsilon, a] &= 1 \qquad\qquad \text{if } (\varepsilon; a) = \varepsilon_1 a_1 + \cdots + \varepsilon_k a_k = b \\ &= 0 \qquad\qquad \text{if } (\varepsilon, a) \neq b \end{aligned}$$

Then

$$V_k(b) = X[b, 0] + \textstyle\sum_{(\varepsilon)\neq(0)} X[b, \varepsilon] = Y + W$$

where $Y = X[b, 0]$ and W is the sum, and

$$\textstyle\sum_{b\epsilon G} E[V_k^4(b)] = \sum_{b\epsilon G} E[Y + 4Y\cdot W + 6Y\cdot W^2 + 4\cdot Y\cdot W^3 + W^4].$$

Now, since $X[b, 0]X[b, \varepsilon] = 1$ only if $b = 0$,

$$\textstyle\sum_{b\epsilon G} E[Y] = E[X[0, 0]] = 1,$$

$$\textstyle\sum_{b\epsilon G} E[Y\cdot W] = E[\sum_{(\varepsilon)\neq(0)} X[0, \varepsilon] = (2^k - 1)/n = u(1)/n,$$

$$\textstyle\sum_{b\epsilon G} E[Y\cdot W^2] = E[(\sum_{(\varepsilon)\neq(0)} X[0, \varepsilon])^2] = u(1)/n + u(2)/n^2,$$

and, by the comments following Lemma 1 and (10),

$$\sum_{b\epsilon G} E[Y\cdot W^3] = E[(\sum_{(\varepsilon)\neq(0)} X[0,\varepsilon])^3]$$

$$= \frac{u(1)}{n} + \frac{3u(2)}{n^2} + \frac{u(3)}{n^3} + \frac{N(Q_0)}{n^2}\left(1 - \frac{1}{n}\right) + \frac{(2^r - 1)N(R_1)}{n^3}.$$

Elementary combinatorial arguments yield the equation

$$\textstyle\sum_{b\epsilon G} E[(\sum_{(\varepsilon)\neq(0)} X[b,\varepsilon])^4] = S(1) + 7S(2) + 6S(3) + S(4).$$

If these results are combined with those of (12) we have the desired result.

We now have, after a few more calculations,

$$\sum_{b\epsilon G} E\left[\left(V_k(b) - \frac{2^k}{n}\right)^4\right]$$

$$= 2^k\left(1 - \frac{1}{n}\right)\left(1 - \frac{6}{n} + \frac{6}{n^2}\right) + \frac{3\cdot 2^{2k}}{n}\left(1 - \frac{1}{n}\right)^2$$

$$+ \frac{4N(Q_0) + N(Q_3))}{n^2}\left(1 - \frac{1}{n}\right)$$

$$+ \frac{(N(\mathfrak{A}_2) + N(Q_2) + 4N(R_1))}{n^3}(2^r - 1)$$

According to (10), Lemma 1, Lemma 2, and Lemma 3,

$$4N(Q_0) + N(Q_3) \leq 4!\,4^k + 4!\,6^k \leq (36)\cdot 6^k$$

$$N(\mathfrak{A}_2) + N(Q_2) + 4N(R_1) \leq 4!\,8^k + 4!\,4^k + 4!\,4^k \leq (36)8^k$$

for $k \geq 2$. Hence

$$\textstyle\sum_{b\epsilon G} E[(V_k(b) - 2^k/n)^4] \leq 2^k + 3\cdot 2^{2k}/n + 36\cdot 6^k/n^2 + (36)8^k(2^r - 1)/n^3.$$

This gives us

$$P\left\{\max_{b\epsilon G}\left|V_k(b) - \frac{2^k}{n}\right| \geqq \frac{\varepsilon\cdot 2^k}{n}\right\}$$

$$\leqq \frac{1}{\varepsilon^4}\frac{n^4}{2^{3k}} + \frac{3}{\varepsilon^4}\frac{n^3}{2^{2k}} + \frac{36}{\varepsilon^4}\cdot\frac{n^2\cdot 3^k}{2^{3k}} + \frac{36}{\varepsilon^4}(2^r - 1)\frac{n}{2^k},$$

which completes the proof of the theorem since each of the terms in this sum does not exceed $\delta/4$ provided that

$$k \geqq \frac{1}{\log 2}\left[\max\left\{\frac{3}{2}\log n, \log n + r\log 2\right\} + 4\log\frac{1}{\varepsilon} + \log\frac{1}{\delta} + \log(144)\right].$$

To prove the comment following the theorem suppose that

$$G = H_1 \oplus \cdots \oplus H_r$$

where the H_i are of order 2. Then since G is a vector space over the integers modulo 2 any sequence $h_1, \cdots, h_k$ of G that generates G must contain a subsequence $h_1, \cdots, h_r$ that is a basis for G. Using these facts one can show, by induction, that if $h_1, \cdots, h_k$ generates G then every b in G has the same number of representations, 2^{k-v}, of the form $b = \varepsilon_1 h_1 + \cdots + \varepsilon_k h_k$. Now, Erdös and Rényi have shown (see Theorem 2 of [1] that if G is a finite Abelian group of order n, if $\delta > 0$, and if

$$k \geqq \frac{1}{\log 2}\left[\log n + \log\left(\frac{\log n}{\log 2}\right) + 2 \log \frac{1}{\delta}\right] + 5$$

then

$$P\{\min_{b \epsilon G} V_k(b) > 0\} > 1 - \delta.$$

That is, nearly every sequence $h_1, \cdots, h_k$ generates G. This, of course, yields what was claimed.

Bibliography

1. P. Erdös and A. Rényi, *Probabilistic methods in group theory*, J. Analyses Math., vol. 14 (1965), pp. 127–138.

University of California
Los Angeles, California