Journal of Pure and Applied Algebra 25 (1982) 113–120
North-Holland Publishing Company

ROBINSON'S CONJECTURE ON ABELIAN GROUPS

Ki Hang KIM and Fred W. ROUSH
Mathematics Research Group, Alabama State University, Montgomery, AL 36101, USA

Communicated by A. Heller
Received 5 January 1981

Let $x_1, \ldots, x_n$ be elements of a finite abelian group G, having respective orders $k_1, \ldots, k_n$ such that $(x_1 - 1)(x_2 - 1) \cdots (x_n - 1) = 0$ in $\mathbf{Z}(G)$, where $n > 1$. We prove that $\min k_i \leq n - 1$ with equality possible if only if $n - 1$ is prime. If all k_i are equal, and not divisible by the cube of a prime, we prove $n \geq k_1(1 + 1/r)$ where r is the least prime dividing k_1. We also establish an inequality concerning coverings of a set by subsets.

Robinson [3] has studied the following equation:

$$(x_1 - 1)(x_2 - 1) \cdots (x_n - 1) = 0$$

where the x_i are elements of a finite abelian group G and the equation holds in the group ring $\mathbf{Z}(G)$ of G over the integers.

A *k-fold tiling* of n-dimensional Euclidean space by a family of cubes is a collection of congruent cubes in n-dimensional space such that (1) all cubes are parallel to the coordinate axes, (2) any point lies in only a finite number of the cubes, and (3) any point not on the boundary of any cube lies in exactly k cubes. Robinson answered the question, when does a k-fold lattice tiling of n-dimensional space exist, in which no two cubes have a common face. Hajos [1] had earlier proved a famous conjecture of Minkowski by similar methods.

Evidently if any $x_i = 1$, the equation above holds. If G has a subgroup $\mathbf{Z}_2 \times \mathbf{Z}_2$ and if x_1, x_2, x_3 are the three distinct elements of order two in the subgroup, the equation holds. Robinson raised the question [4] how large can the least of the orders of the x_i be? We will denote this quantity, the maximum over all choices of $G, x_1, \ldots, x_n$, of the minimum of the orders of the x_i, as $k(n)$. In response to his question, several authors: Alfred Hales of UCLA, ourselves, Sidney C. Garrison, Martin R. Pettet, Stephen M. Gagola of Texas A & M, Masao Kiyota and Kazumasa Nomura of the University of Tokyo, Geoffrey R. Robinson of England proved that $k(n) < n$. Here we will prove a stronger result and obtain partial results on the case in which all x_i have the same order. Robinson has conjectured [5] that $k(n)$ is always equal to the largest prime less than n. It follows from a construction of his [3] that $k(n)$ is always at least this large. Namely in $\mathbf{Z}_p \times \mathbf{Z}_p$ we may take the elements $x_1, \ldots, x_{p+1}$ to be $(1, 1), (2, 1), \ldots, (0, 1)$ and $(1, 0)$. This equation will then hold (it is easiest to see this

0022-4049/82/0000–0000/$02.75

using Theorem 1, part (3) below). Robinson has generalized this construction to all integers [6]. First, in $\mathbf{Z}_{p^m} \times \mathbf{Z}_{p^m}$ we have the solution with $n = p^m + p^{m-1}$ where $x_1, \ldots, x_{p^m}$ are $(1,1), (2,1), \ldots, (p^m, 1)$ and $x_{p^m+1}, \ldots, x_{p^m+p^{m-1}}$ are $(1,p), (1,2p), \ldots, (1,p^m)$, all of order p^m. We extend this solution to other values of n by a direct product construction. If $G, x_1, \ldots, x_m$ is a solution and $H, y_1, \ldots, y_r$ is a solution then in $G \times H$ the set of all products $x_i y_j$ will form a solution. This gives a solution for any integers such that each x_i has order s and

$$n = s \prod_{p|s} \left(1 + \frac{1}{p}\right).$$

Robinson also introduces several other constructions in [3], which we will not need. He proved that his conjecture is valid for $n \leq 5$ (we extend this here to $n \leq 9$). He also raised some other questions, for example, a solution is called *primitive* if no x_i can be deleted. Can a proper homomorphic image of a primitive solution be primitive?

A *character* on G will refer to a multiplicative homomorphism from G into the nonzero complex numbers. A subgroup N of G will be called *cocyclic* if and only if G/N is cyclic.

Theorem 1. *The following are equivalent:*

(1) $(x_1 - 1)(x_2 - 1) \cdots (x_n - 1) = 0$,

(2) *for any character* χ, *there exists* i *such that* $\chi(x_i) = 1$,

(3) *any cocyclic subgroup of* G *contains some* x_i.

Proof. Every character on G has a unique extension to a ring homomorphism from $\mathbf{Z}(G)$ into the complex numbers.

The equation $(x_1 - 1)(x_2 - 1) \cdots (x_n - 1) = 0$ holds if and only if

$$\chi((x_1 - 1) \cdots (x_n - 1)) = 0$$

for every character χ if and only if for every χ,

$$\chi(x_1 - 1)\chi(x_2 - 1) \cdots \chi(x_n - 1) = 0,$$

if and only if for every x, there exists i such that $\chi(x_i - 1) = 0$, if and only if for every χ, there exists i such that $\chi(x_i) = 1$. Thus (1) is equivalent to (2).

To every character χ we associate the cocyclic subgroup which is the kernel of χ. For any cocyclic subgroup N, we can find a character whose kernel is N. Namely compose the homomorphism $G \to G/N$ with an isomorphism from the finite cyclic group G/N into the multiplicative group of roots of unit of order $|G/N|$. And x_i will belong to the kernel of χ if and only if $\chi(x_p) = 1$. This establishes the equivalence of (2) and (3). This completes the proof.

Part of the following result is due to Robinson [3], and the other solvers of Robinson's problem established results which are more or less equivalent to it.

Lemma 2. *Let G be a finite abelian group and H be a subgroup of G. Let G_p denote the p Sylow subgroup of G and let H_p denote $G_p \cap H$.*

(1) *H is cocyclic in G if and only if H_p is cocyclic in G_p for every prime p dividing $|G|$.*

(2) *H is minimal cocyclic in G if and only if H_p is minimal cocyclic in G_p for each prime p dividing $|G|$.*

(3) *If G is a p-group, H is cocyclic in G if and only if the quotient of $G \otimes \mathbf{Z}_p$ by the image of $H \otimes \mathbf{Z}_p$ is cyclic.*

(4) *If G is a p-group a cocyclic subgroup H is minimal cocyclic in G if and only if the mapping $H \otimes \mathbf{Z}_p$ to $G \otimes \mathbf{Z}_p$ is a monomorphism with cokernel $\mathbf{Z}_p$.*

(5) *Every cocyclic subgroup of G is pure and is therefore a direct summand.*

(6) *If G is isomorphic to $(\mathbf{Z}_m)^s$ then H is minimal cocyclic in G if and only if it is isomorphic to $(\mathbf{Z}_m)^{s-1}$.*

Proof. Statements (1), (2) follow from G/H being the direct product of G_p/H_p. Statement (3) follows from the right exactness of tensor product, i.e.

$$H \otimes \mathbf{Z}_p \to G \otimes \mathbf{Z}_p \to G/H \otimes \mathbf{Z}_p \to 0$$

is exact. Thus $G/H \otimes \mathbf{Z}_p$ is isomorphic to $G \otimes \mathbf{Z}_p$ / image$(H \otimes \mathbf{Z}_p)$. Thus one is cyclic if and only if the other is. And $G/H \otimes \mathbf{Z}_p$ is cyclic if and only if G/H is. Suppose G is a p-group and H is cocyclic but $H \otimes \mathbf{Z}_p \to G \otimes \mathbf{Z}_p$ is not a monomorphism. Let $h_1, \ldots, h_u \in H$ be elements whose images form a basis for the image of $H \otimes \mathbf{Z}_p$. Let H_1 be the subgroup generated by $h_1, \ldots, h_u$. Then $H_1 \otimes \mathbf{Z}_p \to G \otimes \mathbf{Z}_p$ is a monomorphism with cocyclic cokernel. Thus H_1 is not equal to H and H_1 is cocyclic. So H was not minimal. This proves that minimality of H implies that the mapping $H \otimes \mathbf{Z}_p \to G \otimes \mathbf{Z}_p$ is a monomorphism. Conversely suppose H is cocyclic, G is a p-group, and $H \otimes \mathbf{Z}_p \to G \otimes \mathbf{Z}_p$ is a monomorphism with cokernel $\mathbf{Z}_p$. If H_1 were a proper subgroup of H which is cocyclic in G then the mapping $H_1 \otimes \mathbf{Z}_p \to H \otimes \mathbf{Z}_p$ is not an epimorphism since its cokernel, $H/H_1 \otimes \mathbf{Z}_p$ is not zero. Thus image $H_1 \otimes \mathbf{Z}_p$ in $G \otimes \mathbf{Z}_p$ must have smaller vector space dimension than image $H \otimes \mathbf{Z}_p$. Thus G / image $H_1 \otimes \mathbf{Z}_p$ cannot be cyclic, since its vector space dimension is at least 2. This proves (3).

A subgroup H is *pure* if and only if it is a direct summand Schenkman [6, p. 62]. It is a direct summand if and only if H_p is a direct summand of G_p for each prime p dividing $|G|$. Thus we may in proving (5) restrict attention to the case in which G is a p-group. Then a subgroup H will be pure if and only if $pH = pG \cap H$. But this is equivalent to the condition $H \otimes \mathbf{Z}_p \to G \otimes \mathbf{Z}_p$ is a monomorphism. So a minimal cocyclic subgroup is pure, and is a direct summand.

By the preceding results it will suffice in proving the last assertion to deal with the case in which G is a p-group. Let G be $(\mathbf{Z}_{p^v})^s$ and let H be a minimal cocyclic subgroup. Then H is a direct summand, so it is $(\mathbf{Z}_{p^v})^w$ for some w. Since H is cocyclic and $H \neq G$, we must have $w = s - 1$.

Next suppose G is $(\mathbf{Z}_{p^u})^s$ and H is isomorphic to $(\mathbf{Z}_{p^v})^{s-1}$, we must show H is

minimal cocyclic. Since H, G are both free modules over the ring $\mathbf{Z}_{p^s}$, H is a direct summand of G. By uniqueness of direct sum decompositions, G/H must be $(\mathbf{Z}_{p^s})$. This means that $H\otimes\mathbf{Z}_p \to G\otimes\mathbf{Z}_p$ will be a monomorphism with kernel $\mathbf{Z}_p$. Thus the conditions in parts (3) and (4) of the lemma hold. Thus H is a minimal cocyclic subgroup of G. This completes the proof.

We prove one more characterization of our basic situation. The dual G^* of a group G is the group of characters on G.

Definition. A group G has *property* $R(k_1, \ldots, k_n)$ if G contains elements $x_1, \ldots, x_n$ of orders $k_1, \ldots, k_n$, respectively, such that for every character λ, there is an i, $1 \le i \le n$, such that $\lambda(x_i) = 1$.

Theorem 3. *A group G has property $R(k_1, \ldots, k_n)$ if and only if there exist cocyclic subgroups $H_1, \ldots, H_n$ of the dual G^* of G, having respective indexes $k_1, \ldots, k_n$, such that $G^* = \bigcup_{i=1}^n H_i$.*

Proof. If $x_1, \ldots, x_n$ exist let $Hi = \{\lambda : \lambda(x_i) = 1\}$. Then $\bigcup H_i = G^*$. And $|H_i| = |G/C_i| = |G|/k_i$ where C_i is the cyclic subgroup generated by x_i.

Conversely if $H_1, \ldots, H_n$ exist then let C_i be the subgroup $\{x : \lambda(x) = 1$ for all $\lambda \in H_i\}$. Then by duality [2, p. 196], $C_i \simeq G^*/H_i$, so C_i is cyclic. Let x_i be any generator of C_i. The order $|C_i|$ of x_i is the index of H_i. Let λ be any character. Then since $\bigcup H_i = G^*$, $\lambda \in H_i$ for some i. Thus if $x \in C_i$, $\lambda(x) = 1$. Thus $\lambda(x_i) = 1$. This proves the theorem.

We will next present our result in the general case.

Theorem 4. *Let $(x_1 - 1) \cdots (x_n - 1) = 0$ for elements $x_1, \ldots, x_n$ of a finite abelian group G. Let x_i have order k_i, and assume that the x_i are arranged so that $k_1 \le k_2 \le \cdots \le k_n$. Then if $k_1 > 1$,*

$$1 \le \sum_{i=2}^{n} \frac{1}{k_i}.$$

Moreover $k_1 \le n - 1$ where equality can hold if and only if $n - 1$ is prime.

Proof. We use the preceding theorem. Let $S_1, \ldots, S_n$ be cocyclic subgroups of G^* (which is isomorphic to G), having indexes $k_1, \ldots, k_n$, and whose union is G. We have the general formula

$$|\bigcup S_i| \le \sum_{i=1}^{n} |S_i| - \sum_{i=2}^{n} |S_1 \cap S_i|.$$

To see this, consider an element contained in $r > 0$ sets. Its contribution to the right-hand side will be $r - (r-1)$ or r according as it does, or does not belong to S_1. Its

contribution to the left-hand side is 1. Equality holds if and only if no terms r occur for $r>1$, i.e. when 1, i, j are distinct, $S_i \cap S_j \subset S_1$.

Now $|S_1 \cap S_i| \geq |G|/k_1 k_i$ by the isomorphism

$$\frac{S_i}{S_1 \cap S_i} \simeq \frac{S_1 S_i}{S_1}.$$

Equality holds if and only if $S_1 S_i = G$. If we divide both sides of the inequality above by $|G|$ we have

$$1 \leq \sum_{i=1}^{n} \frac{1}{k_i} - \sum_{i=2}^{n} \frac{1}{k_1 k_i},$$

$$1 - \frac{1}{k_1} \leq \sum_{i=2}^{n} \left(1 - \frac{1}{k_1}\right) \frac{1}{k_i}$$

so for $k_1 > 1$,

$$1 \leq \sum_{i=2}^{n} \frac{1}{k_i}.$$

Here the conditions for equality are (1) $S_1 S_i = G$ for all $i>1$, and (2) $S_i \cap S_j \subset S_1$, for all $1<i<j$. From the last inequality, it is immediate that $k_1 \leq k_2 \leq n-1$. If equality holds then all k_i must equal $n-1$, in addition to the conditions $S_1 S_i = G^*$ and $S_i \cap S_j \subset S_1$. By the isomorphism

$$\frac{S_i}{S_i \cap S_1} \simeq \frac{S_i S_1}{S_1}$$

we have that $|S_i \cap S_1| = |G|/(n-1)^2$ for all $i>1$. But $|S_i \cap S_j| \geq |G|/(n-1)^2$ for all $i \neq j$ by a similar isomorphism. Yet $S_i \cap S_j \subset S_1 \cap S_i$. So $S_i \cap S_j = S_1 \cap S_i$ for all i, j. Thus $S_i \cap S_1 = S_i \cap S_2 = S_2 \cap S_1$ for all $i>2$. Thus all intersections $S_i \cap S_j$ for $i \neq j$, coincide. If we take the quotient of G^* by $S_1 \cap S_2$ the indices k_i will not change, and we will still have $S_1 S_i = G^*$, $\bigcup_{i=1}^{n} S_i = G^*$, and all S_i are cocyclic. But now in addition $S_i \cap S_j = \{0\}$ for all $i \neq j$. Thus for $i>1$, G^* is the direct sum $S_1 \otimes S_i$. Therefore S_i for each i must be a cyclic subgroup of order $n-1$. Therefore also G^* is $\mathbf{Z}_{n-1} \times \mathbf{Z}_{n-1}$. Since $\bigcup S_i = G$, the S_i must include every cyclic subgroup of order $n-1$ of G^*. But the number of cyclic subgroups of order $n-1$ of $\mathbf{Z}_{n-1} \times \mathbf{Z}_{n-1}$ is

$$(n-1) \prod_{p \mid n-1} \left(1 + \frac{1}{p}\right).$$

Unless $n-1 = p$, this quantity exceeds n, which would be a contradiction. This completes the proof.

Although Robinson's stronger conjecture that $k(n) =$ largest prime less than n is very plausible, there seem to be a host of difficulties which will probably make it impossible to prove at present. Some of these are as follows:

(1) *Deal with the case where each k_i is p^a and G has at least 3 cyclic factors.*
(2) *Deal with the case G is not a p-group.*
(3) *Deal with the case where the x_i have varying orders.*
(4) *Prove that there is always at least one prime between m^2 and $(m+1)^2$.*

In particular the last of these is a famous unsolved problem of number theory, which arises in this setting because most approaches to the problem, if they worked, could yield an inequality like

$$\sum \frac{1}{k_i} \geq \frac{p+1}{p}$$

where p is a prime dividing a number $\leq k_1$ and is not the largest divisor, unless $k(n)$ is prime and $p = k(n)$. Thus $p^2 \leq k_1$ for $k(n)$ composite, and $n/k_1 \geq 1 + 1/p$,

$$k_1 \leq \frac{n}{1+1/p} \leq \frac{n}{1+1/\sqrt{n}}.$$

But if a prime exists between $n/(1+1/\sqrt{n})$ and n then $k(n)$ must be at least this prime by a construction of Robinson. This would give a contradiction to $k(n)$ composite. And the existence of a prime between $n/(1+1/\sqrt{n})$ and n is closely related to the existence of one between $(m+1)^2$ and m^2 for $m = \sqrt{n}$.

The third difficulty is combinatorial, but seems at least as hard as the first two. So here we will only consider (1), (2) that is, the case where all k_i are equal. We will deal with (1) in the case $a \leq 2$ and (2) in a similar case. The combinatorial problems for p^3 and higher seem quite hard.

Theorem 5. *Suppose all x_i have the same order p^a where p is prime, and $a \leq 2$, then*

$$\sum_{i=1}^{n} \frac{1}{k_i} \geq \frac{p+1}{p}.$$

Moreover equality can hold.

Proof. This statement is equivalent to saying that $n \geq p^{a-1}(p+1)$. Suppose $n < p^{a-1}(p+1)$. Let H_1 be the subgroup of G generated by $x_1, \ldots, x_n$. Write $H_1 = (\mathbf{Z}_p)^c \times (\mathbf{Z}_{p^2})^b$. Let G_1 be a group containing H_1 in which all factors $\mathbf{Z}_p$ are replaced by $\mathbf{Z}_{p^2}$, if $a = 2$. If $a = 1$ let $G_1 = H$. Assume that the number c of factors in H_1 is a minimum. Suppose first that there are at least 3 factors. The number of cyclic subgroups in $(\mathbf{Z}_p)^3$ is $p^2 + p + 1 > p^{a-1}(p+1) > n$. So we can find an element z in H such that mod p, z is not in the same cyclic subgroup as any x_i. Let N be the cyclic subgroup generated by z. Then in G_1/N all x_i still have order p^a. Also all cocyclic subgroups of G/N contain an x_i. Thus c the number of factors was not a minimum.

So there are at most two factors. In $\mathbf{Z}_{p^a} \times \mathbf{Z}_{p^a}$ all cyclic subgroups of order p^a are cocyclic. So each one contains an x_i. No two have an element of order p^a in

common. So the number of x^a is at least equal to the number of cyclic subgroups of order p^a. This number is equal to $p^{a-1}(p+1)$. This is a contradiction. Equality follows from Robinson's previously mentioned construction. This completes the proof.

Let $\mathcal{F}$ be a family of subsets of a set S. The problem of finding a subcollection $\mathcal{C} \subset \mathcal{F}$ whose union is S, having the least number of sets, occurs very frequently in combinatorial set theory and operations research. However there is no general method for solving it, in fact similar problems to this are NP-complete. In the present situation, suppose all x_i have the same order and the order of the group is divisible by more than one prime. Then we have a covering problem where S is a product $S_1 \times S_2$ and $\mathcal{F}$ is the set of corresponding products.

Theorem 6. *Let $S = S_1 \times S_2$, $\mathcal{F} = \{A \in B: A \in \mathcal{F}_1, B \in \mathcal{F}_2\}$. Suppose no element of $\mathcal{F}_1$ has more than w elements and that no subset of $\mathcal{F}_2$ having less than e members can cover S_2. Then no subset of $\mathcal{F}$ having less than*

$$\frac{|S_1|e}{w}$$

members can cover S.

Proof. Suppose F^* is a subset of F which covers S. For $s_1 \in S_1$, let $N(s_1)$ denote the number of subsets of F^* that intersect $s_1 \times S_2$ nontrivially. Then clearly $N(s_1) \geq e$, and so

$$\sum_{s_1 \in S_1} N(s_1) \geq |S_1|e.$$

On the other hand, each element of F^* intersects at most w of the $s_1 \in S_2$, so

$$\sum_{s_1 \in S_1} N(s_1) \leq w|F^*|,$$

which gives the desired result.

The matrix product

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

where $|S_1| = 3$, $e = w = 2$ shows that this bound is exact in some nontrivial cases.

Theorem 7. *Suppose all the x_i have order k where k is not divisible by the cube of a prime, and that r is the least prime dividing k. Then $n \geq k(1 + 1/r)$.*

Proof. We apply the preceding theorem. Let S be G^*, let S_2 be a Sylow r-subgroup

of G^* and let S_1 be the product of the other Sylow subgroups of G^*. Let $\mathcal{F}_i$ be the family of cocyclic subgroups of S_i of index the greatest common divisor $(k, |S_i|)$. Every cocyclic subgroup of $S_1 \times S_2$ will be a product of a cocyclic subgroup of S_1 and a cocyclic subgroup of S_2. Thus $\mathcal{F}$ is the family of cocyclic subgroups of S having index k. By Theorem 5, if $(k, |S_2|) = r^n$, it requires $r^n(1 + 1/r)$ cocyclic subgroups of S_2 of index r^n to cover S_2. Thus by Theorem 6, it requires at least

$$\frac{|S_1| r^n(1 + 1/r)}{|S_1|(k, S_1)} = r^n(k, S_1)(1 + 1/r) = k(1 + 1/r)$$

members of $\mathcal{F}$ to cover S. This completes the proof.

References

[1] G. Hajos, Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter, Math. Z. 47 (1942) 427–467.

[2] M. Hall, The Theory of Groups (Macmillan, New York, 1959).

[3] R.M. Robinson, Multiple tilings of n-dimensional space by unit cubes, Math. Z. 166 (1979) 225–264.

[4] R.M. Robinson, Solutions of an equations in Abelian groups, Amer. Math. Monthly 86 (1979) 690.

[5] R.M. Robinson, Private communication (Nov. 20, 1979).

[6] E. Schenkman, Group Theory (Van Nostrand, Princeton, 1965).