Canad. Math. Bull. Vol. **29** (3), 1986

THE HERZOG-SCHÖNHEIM CONJECTURE FOR FINITE NILPOTENT GROUPS

BY

MARC A. BERGER, ALEXANDER FELZENBAUM and AVIEZRI FRAENKEL

ABSTRACT. The purpose of this note is to prove the Herzog-Schönheim [3] conjecture for finite nilpotent groups. This conjecture states that any nontrivial partition of a group into cosets must contain two cosets of the same index (Corollary IV below). See Porubský [4, Section 8] for a perspective on coset partitions.

We introduce certain sets of integer lattice points. A *product set*, $\mathcal{R}$, in $\mathbb{Z}^n$ is any finite nonempty set of the form

$$\mathcal{R} = A_1 \times \ldots \times A_n$$

where $A_1, \ldots, A_n \subset \mathbb{Z}$. The set A_i is referred to as the i-th *projection* of $\mathcal{R}$, denoted

$$A_i = \pi_i(\mathcal{R});\ 1 \leq i \leq n.$$

We shall also need to make use of the product set $\hat{\mathcal{R}}$ in $\mathbb{Z}^{n-1}$ obtained from $\mathcal{R}$ by

$$\hat{\mathcal{R}} = \pi_1(\mathcal{R}) \times \ldots \times \pi_{n-1}(\mathcal{R}).$$

Product sets $\mathcal{R}$ and $\mathcal{R}'$ are said to be *equivalent* if

$$|\pi_i(\mathcal{R})| = |\pi_i(\mathcal{R}')|;\ 1 \leq i \leq n.$$

For $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{N}^n$ the set

$$\mathcal{P} = \{\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{Z}^n : 0 \leq c_i < b_i;\ 1 \leq i \leq n\}$$

is called a *parallelepiped*. Observe that to each product set there corresponds a unique parallelepiped which is equivalent to it.

THEOREM 1. *Let $\mathcal{R}_1, \ldots, \mathcal{R}_k$ be product sets in $\mathbb{Z}^n$ and let $\mathcal{P}_1, \ldots, \mathcal{P}_k$ be the parallelepipeds which are equivalent to them. Then*

$$\left|\bigcup_{i=1}^{k} \mathcal{R}_i\right| \geq \left|\bigcup_{i=1}^{k} \mathcal{P}_i\right|.$$

Received by the editors November 5, 1984 and, in revised form, May 9, 1985.
AMS Subject Classification (1980): 05A17, 10A45, 20D15, 20D60
Key words and phrases: coset partition, Euler φ-function, nilpotent group

https://doi.org/10.4153/CMB-1986-050-0 Published online by Cambridge University Press

PROOF. We shall say that a nonempty set of integers S is *connected* if

$$S = \{m \in \mathbb{Z}: m_1 \leq m \leq m_2\}$$

for some $m_1, m_2 \in \mathbb{Z}$. For any finite nonempty set $T \subset \mathbb{Z}$ denote by $l(T)$ the maximal connected subset of T containing $t = \min(m: m \in T)$. In other words $l(T)$ is the leftmost connected component of T. Define

$$L(T) = (l(T) + 1) \cup (T \backslash l(T)).$$

That is, L modifies T by shifting its leftmost component one unit to the right. Observe that $t + m$ is the smallest element in $L^m(T)$, and that this set is connected when m is sufficiently large. Now define, for $s \in \mathbb{Z}$,

$$L(T;s) = \begin{cases} T & , s \leq t, \\ L^{s-t}(T), & s > t. \end{cases}$$

That is, $L(T;s)$ is that iterate $L^m(T)$ whose smallest element is s (or else it is just T, if $s \leq t$). We can extend this definition to product sets $\mathcal{R}$ by defining

$$L(\mathcal{R};s) = \hat{\mathcal{R}} \times L(\pi_n(\mathcal{R});s).$$

When s is sufficiently small $L(\mathcal{R};s) = \mathcal{R}$, and when s is sufficiently large $\pi_n(L(\mathcal{R};s))$ is connected. From these considerations it becomes evident that in order to prove Theorem 1 it suffices to establish that

$$(1) \qquad \left| \bigcup_{i=1}^{k} L(\mathcal{R}_i;s) \right| \geq \left| \bigcup_{i=1}^{k} L(\mathcal{R}_i;s+1) \right|$$

for any $s \in \mathbb{Z}$.

Fix $s \in \mathbb{Z}$. Let $I \subset \{1, \ldots, k\}$ be the index set

$$I = \{i: L(\mathcal{R}_i;s+1) \neq L(\mathcal{R}_i;s)\},$$

and set

$$\mathcal{S} = \bigcup_{i \in I} \hat{\mathcal{R}}_i.$$

When we make the transition $s \to s+1$ to go from $\cup_{i=1}^k L(\mathcal{R}_i;s)$ to $\cup_{i=1}^k L(\mathcal{R}_i;s+1)$ we lose

$$\left| \left(\bigcup_{i=1}^{k} L(\mathcal{R}_i;s) \right) \Big\backslash \left(\bigcup_{i=1}^{k} L(\mathcal{R}_i;s+1) \right) \right| = |\mathcal{S}|$$

elements, and we gain

$$\left| \left(\bigcup_{i=1}^{k} L(\mathcal{R}_i;s+1) \right) \Big\backslash \left(\bigcup_{i=1}^{k} L(\mathcal{R}_i;s) \right) \right| \leq |\mathcal{S}|$$

elements. Thus (1) is obvious. □

https://doi.org/10.4153/CMB-1986-050-0 Published online by Cambridge University Press

Let $p_1, \ldots, p_n$ be distinct primes. We define $\Lambda(n; p_1, \ldots, p_n)$ to be the family of those product sets $\mathcal{R}$ in $\mathbb{Z}^n$ for which $|\pi_i(\mathcal{R})|$ is a (nonnegative) power of p_i, $1 \leq i \leq n$.

THEOREM II. *Let $\mathcal{P}_1, \ldots, \mathcal{P}_k$ be parallelpipeds in $\Lambda(n; p_1, \ldots, p_n)$. Set*

$$D = \{d \in \mathbb{N} : d \,\big|\, |\mathcal{P}_j| \text{ for some } j\}.$$

Then

$$\left| \bigcup_{i=1}^{k} \mathcal{P}_i \right| = \sum_{d \in D} \varphi(d),$$

where φ denotes the Euler φ-function.

PROOF. Set

$$D_i = \{d \in \mathbb{N} : d \,\big|\, |\mathcal{P}_i|\}.$$

Observe that for any index set $I \subset \{1, \ldots, k\}$

$$\bigcap_{i \in I} D_i = \{d \in \mathbb{N} : d \,\big|\, g.c.d.(|\mathcal{P}_i| : i \in I)\} \tag{2}$$

and

$$\left| \bigcap_{i \in I} \mathcal{P}_i \right| = g.c.d.(|\mathcal{P}_i| : i \in I). \tag{3}$$

Using the well known fact that

$$m = \sum_{d \mid m} \varphi(d)$$

we conclude from (2), (3) that

$$\left| \bigcap_{i \in I} \mathcal{P}_i \right| = \sum_{d \in \cap_{i \in I} D_i} \varphi(d).$$

Since $D = \cup_{i=1}^{k} D_i$ the desired result follows now from the inclusion-exclusion principle. □

THEOREM III. *Let $\mathcal{P}$ be a parallelepiped in $\Lambda(n; p_1, \ldots, p_n)$, and let $\mathcal{T} \subset \Lambda(n; p_1, \ldots, p_n)$ be a partition of $\mathcal{P}$ into at least two sets. Then $\mathcal{T}$ must contain two sets of the same cardinality.*

PROOF. The proof rests heavily on the fact that the sets in $\mathcal{T}$ must belong to $\Lambda(n; p_1, \ldots, p_n)$. We use induction on n. For $n = 1$ the result follows from an immediate counting argument, and so we proceed directly to the induction step. Assume, without loss of generality, that p_n is larger than any of $p_1, \ldots, p_{n-1}$. Let

$$|\pi_n(\mathcal{P})| = p_n^s$$

and set

$$\mathcal{T}_1 = \{\mathcal{C} \in \mathcal{T} : p_n^s \nmid |\mathcal{C}|\}.$$

If $\mathcal{T}_1 = \phi$ then $\hat{\mathcal{T}} \subset \Lambda(n-1; p_1, \ldots, p_{n-1})$ must be a partition of $\hat{\mathcal{P}}$, where $\hat{\mathcal{T}}$ denotes

$$\hat{\mathcal{T}} = \{\hat{\mathcal{C}} : \mathcal{C} \in \mathcal{T}\}.$$

Then the result follows from the induction step. Otherwise, if $\mathcal{T}_1 \neq \phi$, since $\mathcal{T}$ is a partition we must have

$$\sum_{\mathcal{C} \in \mathcal{T}_1} |\mathcal{C}| = p_n^s \Big| \bigcup_{\hat{\mathcal{C}} \in \hat{\mathcal{T}}_1} \hat{\mathcal{C}} \Big|. \tag{4}$$

Suppose now that all the sets in $\mathcal{T}$ have distinct cardinalities. Let

$$M = \{|\hat{\mathcal{C}}| : \hat{\mathcal{C}} \in \hat{\mathcal{T}}_1\}.$$

Then

$$\sum_{\mathcal{C} \in \mathcal{T}_1} |\mathcal{C}| \leq \Big(\sum_{m \in M} m\Big)\Big(\sum_{j=0}^{s-1} p_n^j\Big) = \frac{p_n^s - 1}{p_n - 1} \sum_{m \in M} m. \tag{5}$$

According to Theorems I and II

$$\Big| \bigcup_{\hat{\mathcal{C}} \in \hat{\mathcal{T}}_1} \hat{\mathcal{C}} \Big| \geq \sum_{d \in D} \varphi(d) \tag{6}$$

where

$$D = \{d \in \mathbb{N} : d \,|\, m \text{ for some } m \in M\}.$$

Since the prime divisors of any $d \in D$ can only be $p_1, \ldots, p_{n-1}$ and since p_n is larger than any of them we have

$$\varphi(d) \geq \frac{d}{p_n - 1}, \; d \in D. \tag{7}$$

Putting (5), (6), (7) together, and using the fact that $M \subset D$, gives

$$\sum_{\mathcal{C} \in \mathcal{T}_1} |\mathcal{C}| \leq \frac{p_n^s - 1}{p_n - 1} \sum_{m \in M} m \leq \frac{p_n^s - 1}{p_n - 1} \sum_{d \in D} d < \frac{p_n^s}{p_n - 1} \sum_{d \in D} d \leq p_n^s \sum_{d \in D} \varphi(d)$$
$$\leq p_n^s \Big| \bigcup_{\hat{\mathcal{C}} \in \hat{\mathcal{T}}_1} \hat{\mathcal{C}} \Big|,$$

contradicting (4). □

https://doi.org/10.4153/CMB-1986-050-0 Published online by Cambridge University Press

COROLLARY IV. *Any coset partition of a finite nilpotent group into at least two cosets must contain two cosets of the same order.*

PROOF. Let G be a finite nilpotent group. As is well known (e.g. Rotman [5, p. 120]) G is the direct product of its sylow subgroups,

$$G = P_1 \times \ldots \times P_n.$$

where P_i is a p_i-group. We can thus identify G as a parallelepiped in $\Lambda(n; p_1, \ldots, p_n)$. Furthermore, any subgroup $H \subset G$ is of the form

$$H = Q_1 \times \ldots \times Q_n$$

where each Q_i is a subgroup of P_i. This means that each coset of G can be identified as a product set in $\Lambda(n; p_1, \ldots, p_n)$. Hence the desired result follows at once from Theorem III. □

REMARK. Theorem III can be strengthened as follows. Let

$$N = \left[(p_n - 1) \prod_{j=1}^{n-1} (1 - p_j^{-1}) \right],$$

where $[\cdot]$ denotes the greatest integer function. Then in fact T must contain $N + 1$ sets of the same cardinality. In the proof above the inequality (5) gets modified to

$$\sum_{\mathscr{C} \in \mathscr{T}_1} |\mathscr{C}| \leq N \frac{p_n^s - 1}{p_n - 1} \sum_{m \in M} m$$

and the inequality (7) gets modified to

$$\varphi(d) \geq \frac{Nd}{p_n - 1}.$$

When this is applied, as in Corollary IV, to a cyclic group it establishes the Burshtein [2] conjecture, which was first proved by alternate methods in Berger, Felzenbaum and Fraenkel [1, Thm. 4.II].

REFERENCES

1. Berger, M. A., Felzenbaum, A. and Fraenkel, A., *Lattice parallelepipeds and disjoint covering systems*, Discrete Math. (in press).

2. Burshtein, N., *On natural covering systems of congruences having moduli occurring at most* M *times*, Discrete Math. **14**(1976), pp. 205–214.

3. Herzog, M. and Schönheim, J., *Research problem No.* 9, Canad. Math. Bull. **17**(1974), p. 150

4. Porubský, S., *Results and problems on covering systems of residue classes*, Mitteilungen aus dem Math. Sem. Giessen, Heft 150, Giessen Univ., 1981.

5. Rotman, J. J., *The Theory of Groups: An Introduction*, Allyn and Bacon, Boston, 1973.

DEPARTMENT OF MATHEMATICS
THE WEIZMANN INSTITUTE OF SCIENCE
REHOVOT 76100, ISRAEL