COVERING INTERVALS WITH ARITHMETIC PROGRESSIONS

PAUL BALISTER, BÉLA BOLLOBÁS, ROBERT MORRIS,
JULIAN SAHASRABUDHE, AND MARIUS TIBA

Abstract. In this short note we give a simple proof of a 1962 conjecture of Erdős, first proved in 1969 by Crittenden and Vanden Eynden, and note two corollaries.

Covering systems were introduced by Erdős [3] in 1950, and over the last few years there has been much activity in the area. In particular, the famous 'minimum modulus problem', posed by Erdős [3] in his original paper on the topic, was resolved in 2015 by Hough [8], following an earlier breakthrough by Filaseta, Ford, Konyagin, Pomerance and Yu [7]. In this note we shall concern ourselves with two other questions about covering systems, asked by Erdős [4] in 1962.

We say that a family $\mathcal{A} = \{A_1, \ldots, A_k\}$ of arithmetic progressions *covers* a set $S \subset \mathbb{Z}$ if $S \subset A_1 \cup \cdots \cup A_k$, and if $\mathcal{A}$ covers $\mathbb{Z}$ then it is called a *covering system*. Strengthening a conjecture of Stein [9], made in 1958, Erdős [4] conjectured that if $\mathcal{A}$ covers the set $[2^k] = \{1, \ldots, 2^k\}$ then it covers all of $\mathbb{Z}$. The family of progressions $A_i = \{2^{i-1} \pmod{2^i}\}$ for $i = 1, \ldots, k$ shows that 2^k cannot be decreased to $2^k - 1$. Erdős mentioned this conjecture in several of his later papers, see for example [5, 6].

In support of this conjecture, Erdős (see [5]) proved that there exists $N(k) \in \mathbb{N}$ such that if $\mathcal{A}$ covers $[N(k)]$ then it also covers $\mathbb{Z}$. However, the full conjecture was only proved in 1969 by Crittenden and Vanden Eynden [1, 2]. Our aim in this note is to give a short proof of this theorem.

Theorem 1. *Let $\mathcal{A} = \{A_1, \ldots, A_k\}$ be a collection of k arithmetic progressions. If $\mathcal{A}$ covers 2^k consecutive numbers, then it covers $\mathbb{Z}$.*

Proof. Let $I = \{a+1, \ldots, a+2^k\}$ be an interval of 2^k consecutive integers, and suppose (for a contradiction) that $\mathcal{A}$ covers I but fails to cover $\mathbb{Z}$. Since translating all of the arithmetic progressions by a constant makes no difference, let us assume that $a = 0$. Let us write $\mathrm{lcm}(\mathcal{A})$ for the least common multiple of the moduli $d_1, \ldots, d_k$ of the progressions in $\mathcal{A}$, and observe that every translation of the interval I by a multiple of $\mathrm{lcm}(\mathcal{A})$ is also covered by $\mathcal{A}$. Therefore, setting $q := \mathrm{lcm}(\mathcal{A})$, there exists an integer $2^k < c \leqslant q$ that is not covered by $\mathcal{A}$.

Set $\omega := \exp(2\pi i/q)$ and let $\Omega = \{1, \omega, \ldots, \omega^{q-1}\}$ be the multiplicative cyclic group of order q generated by ω. Thus $\omega^q = 1$, and the map $n \mapsto \omega^n$ is a homomorphism from the

The first two authors were partially supported by NSF grant DMS 1600742, the third author was partially supported by CNPq (Proc. 303275/2013-8) and FAPERJ (Proc. 201.598/2014), and the fifth author was supported by a Trinity Hall Research Studentship.

additive group $\mathbb{Z}$ onto the multiplicative group Ω, mapping A_i into a set Z_i with $|Z_i| = q/d_i$. Set $Z := Z_1 \cup \cdots \cup Z_k$, and observe that

$$\big\{\omega^j : 1 \leqslant j \leqslant 2^k\big\} \subset Z \qquad \text{and} \qquad \omega^c \notin Z, \tag{1}$$

for some $2^k < c \leqslant q$, by the assumptions above. Now, observe that Z is precisely the set of zeros of the polynomial

$$P(z) = \prod_{i=1}^{k} \big(z^{q/d_i} - \omega^{a_i q/d_i} \big),$$

where $A_i = \big\{ a_i + n d_i : n \in \mathbb{Z} \big\}$. Expanding $P(z)$ as a linear combination of monomials, we find that

$$P(z) = \sum_{S \subset [k]} c_S z^{\sum_{j \in S} q/d_j} = \sum_{S \subset [k]} c_S z^{\alpha_S},$$

where the coefficients c_S are (possibly zero) complex numbers. In particular, $P(z)$ is in the linear span W of the monomials z^{α_S}, and the dimension of W is at most 2^k.

Now, for each $m \in \mathbb{Z}$, define $P_m(z) := P\big(\omega^{-m} z\big)$, and observe that $P_m(z) \in W$, since

$$P\big(\omega^{-m} z\big) = \sum_{S \subset [k]} \big(c_S \, \omega^{-m\alpha_S} \big) z^{\alpha_S}.$$

To contradict the bound $\dim W \leqslant 2^k$, we shall show that the $2^k + 1$ polynomials $P_0(z)$, $P_1(z), \ldots, P_{2^k}(z)$ are linearly independent. To this end, it suffices to show the following for each $0 \leqslant \ell \leqslant 2^k$: if

$$\sum_{m=\ell}^{2^k} \lambda_m P_m(z) = 0 \tag{2}$$

then $\lambda_\ell = 0$. To do so, let $2^k < s \leqslant q$ be minimal such that $P(\omega^s) \neq 0$, and recall from (1) that such an s exists. Since $P_\ell(\omega^{s+\ell}) = P(\omega^s) \neq 0$, but $P_m(\omega^{s+\ell}) = P(\omega^{s-(m-\ell)}) = 0$ for all $\ell < m \leqslant 2^k$, it follows from (2) that

$$\lambda_\ell P_\ell(\omega^{s+\ell}) = \lambda_\ell P(\omega^s) = 0.$$

Thus $\lambda_\ell = 0$, and this completes the proof. □

To conclude, let us note two simple consequences of Theorem 1. To state the first, let us say that a covering system $\mathcal{A}$ is *minimal* if no proper subset of $\mathcal{A}$ covers $\mathbb{Z}$.

Corollary 2. *In a minimal covering system of k arithmetic progressions, every modulus is at most 2^{k-1}.*

Proof. Let $\mathcal{A}$ be a minimal covering system of k arithmetic progressions, and let $A \in \mathcal{A}$. Set $\mathcal{A}' := \mathcal{A} \setminus \{A\}$ and $I := \{a+1, \ldots, a+d-1\}$, where $A = \{a + nd : n \in \mathbb{Z}\}$. Then $\mathcal{A}'$ is a collection of $k-1$ arithmetic progressions that covers the interval I but does not cover $\mathbb{Z}$. By Theorem 1, it follows that $|I| \leqslant 2^{k-1} - 1$, and hence $d \leqslant 2^{k-1}$, as claimed. □

The family of progressions $\{A_1, \ldots, A_k\}$, where $A_i = \{2^{i-1} \pmod{2^i}\}$ for $i = 1, \ldots, k-1$ and $A_k = \{0 \pmod{2^{k-1}}\}$, shows that the bound 2^{k-1} in Corollary 2 is best possible.

The second consequence of Theorem 1 is also almost immediate, and answers the following question[1] of Erdős [6]: "Let the moduli $d_1, \ldots, d_k$ of a collection of arithmetic progressions satisfy $\sum_{i=1}^k 1/d_i \leqslant 1 - 1/2^k$. Is it true that there is a number u, $1 \leqslant u \leqslant 2^k$, that does not satisfy any of the congruences?" In fact, more is true.

Corollary 3. *Let $\mathcal{A}$ be a collection of k arithmetic progressions whose moduli $d_1, \ldots, d_k$ satisfy $\sum_{i=1}^k 1/d_i < 1$. Then no set of 2^k consecutive numbers is covered by $\mathcal{A}$.*

Proof. Set $q := \operatorname{lcm}(\mathcal{A})$, the least common multiple of the moduli $d_1, \ldots, d_k$. We have

$$\left| [q] \cap \bigcup_{i=1}^k A_i \right| \leqslant \sum_{i=1}^k \big| [q] \cap A_i \big| = \sum_{i=1}^k \frac{q}{d_i} < q,$$

so $\mathcal{A}$ does not cover $\mathbb{Z}$. The result now follows by Theorem 1. □

We remark that if the moduli are assumed to be distinct, then the conclusion of Corollary 3 holds under the slightly weaker assumption that $\sum_{i=1}^k 1/d_i \leqslant 1$, using the fact[2] (see [4, 5]) that $\mathbb{Z}$ cannot be covered by a finite number of disjoint progressions with distinct differences.

References

[1] R.B. Crittenden and C.L. Vanden Eynden, A proof of a conjecture of Erdős, *Bull. Amer. Math. Soc.*, **75** (1969), 1326–1329.

[2] R.B. Crittenden and C.L. Vanden Eynden, Any n arithmetic progressions covering the first 2^n integers cover all integers, *Proc. Amer. Math. Soc.* **24** (1970) 475–481.

[3] P. Erdős, On integers of the form $2^k + p$ and some related problems, *Summa Brasil. Math.*, **2** (1950), 113–123.

[4] P. Erdős, Számelméleti megjegyzések, IV. Extremális problémák a számelméletben, I. (Remarks on number theory, IV. Extremal problems in number theory, I., in Hungarian), *Mat. Lapok*, **13** (1962). 228–255.

[5] P. Erdős, Extremal problems in number theory, in *Proc. Sympos. Pure Math.*, Vol. VIII, pp. 181–189, Amer. Math. Soc., Providence, R.I., 1965.

[6] P. Erdős, Számelméleti megjegyzések, V. Extremális problémák a számelméletben, II. (Remarks on number theory, V. Extremal problems in number theory, II., in Hungarian), *Mat. Lapok*, **17** (1966), 135–155.

[7] M. Filaseta, K. Ford, S. Konyagin, C. Pomerance and G. Yu, Sieving by large integers and covering systems of congruences, *J. Amer. Math. Soc.*, **20** (2007), 495–517.

[8] R. Hough, Solution of the minimum modulus problem for covering systems, *Ann. Math.*, **181** (2015), 361–382.

---

[1] Erdős asked this question immediately after stating the conjecture that was proved by Crittenden and Vanden Eynden, but (rather surprisingly) he did not remark that it would follow as a consequence.

[2] To be precise, Erdős [4] proved that if $A_1, \ldots, A_k$ are disjoint (infinite) arithmetic progressions with distinct moduli $1 < d_1 < \cdots < d_k$, then $\sum_{i=1}^k 1/d_i \leqslant 1 - 2^{-k}$, which is sharp. He attributes the method to L. Mirsky and D. Newman, who proved (unpublished) that $\sum_{i=1}^k 1/d_i < 1$.

[9] S.K. Stein, Unions of arithmetic sequences, *Math. Ann.*, **134** (1958), 289–294.

Department of Mathematical Sciences, University of Memphis, Memphis, TN 38152, USA
Email address: pbalistr@memphis.edu

Department of Pure Mathematics and Mathematical Statistics, Wilberforce Road, Cambridge, CB3 0WA, UK, and Department of Mathematical Sciences, University of Memphis, Memphis, TN 38152, USA
Email address: b.bollobas@dpmms.cam.ac.uk

IMPA, Estrada Dona Castorina 110, Jardim Botânico, Rio de Janeiro, 22460-320, Brazil
Email address: rob@impa.br

Peterhouse, Trumpington Street, University of Cambridge, CB2 1RD, UK and IMPA, Estrada Dona Castorina 110, Jardim Botânico, Rio de Janeiro, 22460-320, Brazil
Email address: julians@impa.br

Department of Pure Mathematics and Mathematical Statistics, Wilberforce Road, Cambridge, CB3 0WA, UK
Email address: mt576@dpmms.cam.ac.uk