#A34 INTEGERS 15 (2015)

# ON THE REDUCIBILITY OF EXACT COVERING SYSTEMS

**Ofir Schnabel**
*Institute of Algebra and Number Theory, University of Stuttgart,*
*Stuttgart, Germany*
os2519@yahoo.com

*Received: 2/17/14, Revised: 3/9/15, Accepted: 6/20/15, Published: 7/17/15*

**Abstract**

There exist irreducible exact covering systems (ECS). These are ECS which are not a proper split of a coarser ECS. However, an ECS admiting a maximal modulus which is divisible by at most two distinct primes, primely splits a coarser ECS. As a consequence, if all moduli of an ECS $A$ are divisible by at most two distinct primes, then $A$ is natural. That is, $A$ can be formed by iteratively splitting the trivial ECS.

## 1. Introduction

An *exact covering system* (ECS) is a partition of $\mathbb{Z}$ into finitely many arithmetic progressions

$$A = \{a_s(n_s)\}_{s=1}^{k}, \tag{1}$$

where $a(n)$ is the arithmetic progression $a + \mathbb{Z}n$. Here, $n$ is the *modulus* of the arithmetic progression $a(n)$. An ECS (1) admits *multiplicity* if there exist $1 \leq i < j \leq k$ such that $n_i = n_j$. The ECS $A = \{0(1)\}$ is called the *trivial ECS.*

The concept of ECS was first introduced by P. Erdős in the early 1930's. A main concern in the research on ECS is finding restraints on the number of times a modulus occurs in an ECS. Erdős conjectured the following: Every non-trivial ECS admits multiplicity. Erdős conjecture was proved in the beginning of the 1950's independently by H. Davenport, L. Mirsky, D. Newman and R. Rado (see [3]). In fact, the proof shows that such multiplicity occurs in the *greatest* modulus. This result was generalized by Š. Znám [11] and later by Y.G. Chen and Š. Porubskỳ [2]. The proofs in these papers use generating functions of an ECS and a deep relation between the number of times the greatest difference $m$ occurs in an ECS and minimal vanishing sums of $m$-th roots of unity (see [6]). However, results in the spirit of the above results were obtained in [1],[10] using combinatorical methods.

For a more comprehensive study of ECS the reader is referred to a monograph by Š. Porubský [8] and to a review by Š. Porubský and J. Schönheim [9].

Our main concern in this note is *reducibility* of ECS. Notice that for any natural number $n$, there is a *basic* ECS

$$\{i(n)\}_{i=0}^{n-1}. \tag{2}$$

This is a *splitting* of the trivial ECS. In a similar way we can split any ECS by splitting an arithmetic progression $a(t)$ into $n$ arithmetic progressions

$$\{a+it(tn)\}_{i=0}^{n-1}. \tag{3}$$

An ECS is *natural* if it is formed by iteratively splitting the trivial ECS.

**Definition 1.1.** An ECS $A$ primely splits an ECS $B$, (denote $A \models B$), if there exists a prime number $p$ such that

$$B=\{a_i\,(n_i)\}_{i=1}^{k}\,, \quad A=\{a_i\,(n_i)\}_{i=1}^{k-1}\bigcup\{a_k+jn_k(pn_k)\}_{j=0}^{p-1}.$$

In other words: $A$ is obtained from $B$ by splitting one of the arithmetic progressions into $p$ arithmetic progressions.

Throughout this note, maximality will be with respect to the division partial order. In particular, when given an ECS, a modulus is maximal if it does not divide any other modulus in this ECS. Our main theorem is the following

**Theorem A.** *Suppose that an ECS $A=\{a_s(n_s)\}_{s=1}^{k}$ has a maximal modulus of the form $p_1^{k_1}p_2^{k_2}$, where $p_1,p_2$ are primes and $k_1,k_2\geq 0$. Then $A$ primely splits an ECS $B$.*

In a sense, Theorem A discusses reducibility of ECS. Denote the least common multiple of $B=\{n_1,n_2,\ldots,n_k\}\subseteq\mathbb{N}$ by $N(B)$. For an ECS (1), denote the least common multiple of all the moduli by $N(A)$. Throughout this note $p_i$ stands for prime number. In two papers [4, 5], I. Korec investigate ECS with $N(A)=p_1^{k_1}p_2^{k_2}$ and $N(A)=p_1^{k_1}p_2^{k_2}p_3^{k_3}$. In particular, he discusses the reducibility (see [4]) of such ECS. In [7], I. Polách generalizes some of Korec's results. The approach adopted by Korec and Polách is essentially different from the classical approach of generating functions. Theorem A is in the same spirit as Korec and Polách results. However, our methods are similar to the classical methods and rely heavily on the above mentioned relation between ECS and vanishing sums of roots of unity. As a corollary of Theorem A we get the following result which deals with some natural ECS. In particular, it classifies all the ECS with $N(A)=p_1^{k_1}p_2^{k_2}$.

**Corollary 1.2.** *Let $A=\{a_s(n_s)\}_{s=1}^{k}$ be an ECS. If no modulus is divisible by more than two distinct primes then $A=A_1\models A_2\models\ldots\models A_{n-1}\models\{0(1)\}$. In particular, this holds in the case when $N(A)$ admits at most two prime factors (see [4]).*

Another corollary of Theorem A is a restraint on ECS $A$ with $N(A) = p_1^{k_1}p_2^{k_2}p_3^{k_3}$.

**Corollary 1.3.** *Let $A = \{a_s(n_s)\}_{s=1}^k$ be an ECS such that $N(A) = p_1^{k_1}p_2^{k_2}p_3^{k_3}$. Assume also there exist moduli $n_1, n_2, n_3$ such that*

$$\begin{array}{ccc} p_1 \mid n_1n_2, & p_2 \mid n_1n_3, & p_3 \mid n_2n_3, \\ p_1 \nmid n_3, & p_2 \nmid n_2, & p_3 \nmid n_1 \end{array} \tag{4}$$

*Then $p_1p_2p_3$ divides some modulus $n_j$.*

## 2. Preliminaries

Given an ECS (1) we may always assume that

$$0 \le a_s < n_s \quad \text{for all} \quad 1 \le s \le k. \tag{5}$$

The classical approach for investigating multiplicity is to consider the following generating function. For $|z| < 1$ we have:

$$\sum_{s=1}^{k} \frac{z^{a_s}}{1 - z^{n_s}} = \sum_{s=1}^{k}\sum_{q=0}^{\infty} z^{a_s+qn_s} = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}. \tag{6}$$

Let $B = \{n_1, n_2, \ldots, n_k\}$ be a set of natural numbers. Assume that $n_r$ is a maximal element in $B$. Denote the least common multiple of $n_1, n_2, \ldots, n_s$ by $N$. Let $C_{n_r}$ be the cyclic group of order $n_r$ generated by $\overline{z}$ and let $\zeta$ be a primitive $n_r$-th root of unity. Consider the following ring homomorphisms:

$$\begin{array}{ccc} \gamma : \mathbb{Z}[z] \to \mathbb{Z}C_{n_r} & \qquad & \varphi : \mathbb{Z}C_{n_r} \to \mathbb{C} \\ z \mapsto \overline{z} & & \overline{z} \mapsto \zeta. \end{array}$$

Here, $\mathbb{Z}[z]$ is the ring of polynomials with integral coefficients in the variable $z$ and $\mathbb{Z}C_{n_r}$ is the integral group algebra. The following two lemmas will be used in the proof of Theorem A.

**Lemma 2.1.** *With the above notation, let $t$ be a divisor of $N(B)$. Then $\varphi \circ \gamma\left(\frac{1-z^{N(B)}}{1-z^t}\right) \neq 0$ if and only if $n_r$ divides $t$. In particular,*

1. $$\varphi \circ \gamma\left(\frac{1-z^{N(B)}}{1-z}\right) = 0.$$

2. *By the maximality of $n_r$, for $1 \le i \le k$*

$$\varphi \circ \gamma\left(\frac{1-z^{N(B)}}{1-z^{n_i}}\right) = 0$$

*if and only if $n_i \neq n_r$.*

*Proof.* First, since $n_r$ divides $N(B)$,

$$\varphi \circ \gamma(1 - z^{N(B)}) = 1 - \zeta^{N(B)} = 0.$$

Now, $t$ admits the following decomposition: $t = qn_r + r$ such that $q, r$ are natural numbers and $0 \leq r < n_r$. Then, $\varphi \circ \gamma(1 - z^t) = 1 - \zeta^t = 1 - \zeta^r$. Hence, if $n_r$ is not a divisor of $t$ we get that

$$\varphi \circ \gamma(\frac{1 - z^{N(B)}}{1 - z^t}) \neq 0.$$

Assume now that $n_r$ is a divisor of $t$ and recall that if $r_1 | r_2$ then

$$\frac{1 - z^{r_2}}{1 - z^{r_1}} = \sum_{i=0}^{\frac{r_2}{r_1} - 1} z^{i \cdot r_1}. \tag{7}$$

Then, if we denote $N(B) = cn_r$ and $t = qn_r$ we get that

$$\frac{1 - z^N(B)}{1 - z^t} = \frac{\sum_{i=0}^{c-1} z^{in_r}}{\sum_{i=0}^{q-1} z^{in_r}}. \tag{8}$$

Hence,

$$\varphi \circ \gamma \left( \frac{1 - z^{N(B)}}{1 - z^t} \right) = \frac{\overbrace{1 + 1 + \ldots + 1}^{c \text{ times}}}{\underbrace{1 + 1 + \ldots + 1}_{q \text{ times}}} \neq 0. \tag{9}$$

□

Let $P_i = \{\bar{z}^{\frac{jn_r}{p_i}}\}_{j=0}^{p_i - 1}$ be the unique subgroup of order $p_i$ in $C_{n_r}$. Define

$$\sigma_{n_r}(P_i) := \sum_{g \in P_i} g \in \mathbb{Z}C_{n_r} = \sum_{j=0}^{p_i - 1} \bar{z}^{\frac{j \cdot n_r}{p_i}}.$$

**Lemma 2.2.** *([6, Theorem 3.3]) Let $n_r = p_1^{k_1} p_2^{k_2}$ and let $0 \neq x \in \mathbb{N}C_{n_r} \cap ker(\varphi)$. Then $x$ admits one of the following decompositions:*

$$x = \overline{z}^d \cdot \sigma_{n_r}(P_1) + \sum_{i=0}^{n_r - 1} b_i \overline{z}^i, \quad b_i \geq 0, \quad 0 \leq d < \frac{n_r}{p_1};$$

*or*

$$x = \overline{z}^d \cdot \sigma_{n_r}(P_2) + \sum_{i=0}^{n_r - 1} b_i \overline{z}^i, \quad b_i \geq 0, \quad 0 \leq d < \frac{n_r}{p_2}.$$

## 3. Main Part

*Proof of Theorem A.* Let $n_r = p_1^{t_1} p_2^{t_2}$ be a maximal modulus in $A$. Equation (6) can be written in the following way:

$$\sum_{s=1}^{k} \frac{z^{a_s}}{1-z^{n_s}} = \sum_{\{s:n_s=n_r\}} \frac{z^{a_s}}{1-z^{n_r}} + \sum_{\{s:n_s\neq n_r\}} \frac{z^{a_s}}{1-z^{n_s}} = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}. \tag{10}$$

Both sides of (10) are elements in $\mathbb{Q}(z)$, the field of rational functions with rational coefficients in the variable $z$. As before, denote the least common multiple of $n_1, n_2, \ldots, n_k$ by $N$. By multiplying both sides of (10) by $1 - z^N$ we get

$$\sum_{s=1}^{k} \frac{z^{a_s} \cdot (1-z^N)}{1-z^{n_s}} = \frac{1-z^N}{1-z}. \tag{11}$$

Hence, both sides of (11) are in $\mathbb{Z}[z]$. Consequently, by Lemma 2.1 the right-hand side of (11) is in the kernel of $\varphi \circ \gamma$. Hence the left-hand side is also in $ker(\varphi \circ \gamma)$. Therefore,

$$\sum_{\{s:n_s=n_r\}} \frac{z^{a_s} \cdot (1-z^N)}{1-z^{n_s}} = \frac{1-z^N}{1-z^{n_r}} \sum_{\{s:n_s=n_r\}} z^{a_s} \in \ker(\varphi \circ \gamma). \tag{12}$$

Thus, by Lemma 2.1 we get:

$$\sum_{\{s:n_s=n_r\}} z^{a_s} \in \ker(\varphi \circ \gamma). \tag{13}$$

Hence,

$$\gamma \left( \sum_{\{s:n_s=n_r\}} z^{a_s} \right) = \sum_{\{s:n_s=n_r\}} \overline{z}^{a_s} \in \ker(\varphi). \tag{14}$$

Now, by Lemma 2.2 we may assume without loss of generality that

$$\gamma \left( \sum_{\{s:n_s=n_r\}} z^{a_s} \right) = \textstyle\sum_1 + \sum_2, \tag{15}$$

where

$$\textstyle\sum_1 = \overline{z}^d \cdot \sigma_{n_r}(P_1) = \overline{z}^d \cdot \sum_{j=0}^{p_1-1} \overline{z}^{\frac{j \cdot n_r}{p_1}}, \tag{16}$$

where $d < \frac{n_r}{p_1}$. And

$$\textstyle\sum_2 = \sum_{i=0}^{n_r-1} b_i \overline{z}^i, \quad b_i \geq 0. \tag{17}$$

Notice that $\ker\gamma = (z^{n_r}-1)\mathbb{Z}[z]$. Consequently, the restriction of $\gamma$ to polynomials in $\mathbb{Z}[z]$ with degree smaller than $n_r$ is one-to-one. Let

$$g(z) = z^d \cdot \sum_{j=0}^{p_1-1} z^{\frac{j\cdot n_r}{p_1}}. \tag{18}$$

Then $\gamma(g(z)) = \sum_1$. Hence

$$\gamma\left(\sum_{\{s:n_s=n_r\}} z^{a_s} - g(z)\right) = \gamma\left(\sum_{i=0}^{n_r-1} b_i z^i\right) = \textstyle\sum_2. \tag{19}$$

By (5), the degree of

$$\sum_{\{s:n_s=n_r\}} z^{a_s} - g(z) \tag{20}$$

is smaller than $n_r$. Therefore by the one-to-one property on such polynomials,

$$\sum_{\{s:n_s=n_r\}} z^{a_s} - g(z) = \sum_{i=0}^{n_r-1} b_i z^i. \tag{21}$$

Consequently,

$$\sum_{\{s:n_s=n_r\}} z^{a_s} = g(z) + \sum_{i=0}^{n_r-1} b_i z^i = z^d \cdot \sum_{j=0}^{p_1-1} z^{\frac{j\cdot n_r}{p_1}} + \sum_{i=0}^{n_r-1} b_i z^i. \tag{22}$$

By (10) and (22) ,

$$\frac{z^d \cdot \sum_{j=0}^{p_1-1} z^{\frac{j\cdot n_r}{p_1}}}{1-z^{n_r}} + \frac{\sum_{i=0}^{n_r-1} b_i z^i}{1-z^{n_r}} + \sum_{\{s:n_s\neq n_r\}} \frac{z^{a_s}}{1-z^{n_s}} = \frac{1}{1-z}. \tag{23}$$

Notice that

$$\frac{z^d \cdot \sum_{j=0}^{p_1-1} z^{\frac{j\cdot n_r}{p_1}}}{1-z^{n_r}} = \frac{z^d}{1-z^{\frac{n_r}{p_1}}}. \tag{24}$$

So, by (23) and (24)

$$\sum_{\{s:n_s\neq n_r\}} \frac{z^{a_s}}{1-z^{n_s}} + \frac{z^d}{1-z^{\frac{n_r}{p_1}}} + \frac{\sum_{i=0}^{n_r-1} b_i z^i}{1-z^{n_r}} = \frac{1}{1-z}. \tag{25}$$

Since $b_i \geq 0$, every summand $z^{a_s}$ of the left-hand side of equation (22) is either a summand of $g(z)$ if $a_s \equiv d (\mathrm{mod}\ \frac{n_r}{p_1})$ or a summand in $\sum_{i=0}^{n_r-1} b_i z^i$. So, (25) is a generating function of a new ECS $B$, where $B$ is obtained by consolidation of the $p_1$ arithmetic progressions:

$$\left\{d(n_r), d+\frac{n_r}{p_1}(n_r), \ldots, d+\frac{(p_1-1)n_r}{p_1}(n_r)\right\} \subset A, \tag{26}$$

into one arithmetic progression $d(\frac{n_r}{p_1})$ in $B$. Hence $A$ is a primely split of the ECS $B$, and this completes the proof. □

It is important to notice that there exist ECS that are not prime splitting of any ECS. By Theorem A, the following example, which is a particular case of [6, Example 2.5], is minimal.

**Example 3.1.** The following ECS is not a prime splitting of any ECS.

$$\begin{aligned} A = \{&2(6), 4(6), 1(10), 3(10), 7(10), 9(10), 0(15),\\ &5(30), 6(30), 12(30), 18(30), 24(30), 25(30)\} \end{aligned} \tag{27}$$

Notice that the maximal modulus is 30. The reason that $A$ is not a primely split of any ECS follows from the fact that there is no way to split the following vanishing sum

$$\xi^5+\xi^6+\xi^{12}+\xi^{18}+\xi^{24}+\xi^{25}=0, \tag{28}$$

where $\xi$ is a 30-*th* primitive root of unity, into two vanishing sums (see [6]).

*Proof of Corollary 1.2.* First, notice that for two ECS, $A$ and $B$, if $A \models B$, then any modulus of $B$ is a divisor of a modulus of $A$. Now, since all moduli of $A$ admit at most two prime factors, then any maximal modulus of $A$ also admits at most two prime factors. By applying Theorem A to each maximal modulus we proceed by induction noticing that in each step of the induction all the moduli (and hence all the maximal moduli) admit at most two prime factors until we get the trivial ECS. □

**Remark 3.2.** Note that Corollary 1.2 gives a way to construct all ECS with $N = p_1^{s_1}p_2^{s_2}$ for two given primes $p_1, p_2$.

For the next proof note that by the Chinese remainder theorem, an ECS cannot contain coprime moduli.

*Proof of Corollary 1.3.* Assume that there is no modulus $n_j = p_1^{d_1}p_2^{d_2}p_3^{d_3}, d_1, d_2, d_3 > 0$. Let $A = A_1$. By the hypothesis of the corollary and by the above assumption there is a maximal modulus $p_1^{l_1}p_2^{l_2}(l_1, l_2 \geq 1)$. Hence by Theorem A there is an ECS $A_1 \models A_2$. We proceed by induction. As long as there is a modulus $p_1^{l_1}p_2^{l_2}(l_1, l_2 \geq 1)$ there is a maximal modulus of the same form. The sequence $A_1 \models A_2 \ldots \models A_l$, must terminate. The terminal ECS, $A_l$ has no modulus of the form $p_1^{l_1}p_2^{l_2}(l_1, l_2 \geq 1)$.

Hence, there is either a modulus $p_1^{l_1} (l_1 > 0)$ or a modulus $p_2^{l_2} (l_2 > 0)$. Since we assumed that $A$ contains moduli $p_1^{m_3} p_3^{m_4}$ and $p_2^{m_5} p_3^{m_6}$, then, in both cases $A_l$ contain coprime moduli. This cannot happen by the Chinese remainder theorem. □

**Acknowledgements.** This paper is a part of the author's M.Sc dissertation under the supervision of Y. Ginosar.

## References

[1] M. A. Berger, A. Felzenbaum, and A. S. Fraenkel, *A nonanalytic proof of the Newman-Znám result for disjoint covering systems*, *Combinatorica* **6** (1986), 235–243.

[2] Y. Chen and Š. Porubskỳ. Remarks on systems of congruence classes. *Acta Arith.* **71** (1995), 1–10.

[3] P. Erdős. On a problem concerning congruence systems, (Hungarian; English summery). *Mat. Lapok* **3** (1952), 122–128.

[4] I. Korec. Irreducible disjoint covering systems. *Acta Arith.* **44** (1984), 389–395.

[5] I. Korec. Irreducible disjoint covering systems of $\mathbb{Z}$ with the common modulus consisting of three primes. *Acta Math. Univ. Comenian.* **46/47** (1985), 75–81.

[6] T. Lam and K. Leung. On Vanishing Sums of Roots of Unity. *J. Algebra* **224** (2000), 91–109.

[7] I. Polách. A new necessary condition for moduli of non-natural irreducible disjoint covering system. *Acta Math. Univ. Comenian. (N.S.)* **63** (1994), 133–140.

[8] Š. Porubský. Results and problems on covering systems of residue classes. *Mitt. Math. Sem. Giessen* **150** (1981).

[9] Š. Porubský and J. Schönheim. Covering systems of Paul Erdős. Past, present and future. Paul Erdős and his mathematics . *János Bolyai Math. Soc.* **11** (2002), 581–627.

[10] R. J. Simpson. Exact coverings of the integers by arithmetic progressions, *Discrete Math.* **59** (1986), 181–190.

[11] Š. Znám. On exactly covering systems of arithmetic sequences. *Colloq., János Bolyai Math. Soc. Debrecen*, 1970.