On Exact Covering Systems of the Integers and Partitions of $\mathbb{Z}^n$ into Translates of Sublattices

Alexander Schwartz

under the direction of
Dr. Payman Kassaei
Massachusetts Institute of Technology

Research Science Institute
August 7, 1999

Abstract

In this paper we introduce and apply various methods to analyze exact covering systems of the integers. We characterize and enumerate a certain class of irreducible exact covering systems and analyze the relationship between exact covering systems and certain polynomials. We then generalize this problem to n dimensions and exhibit various results towards the goal of proving an analogous theorem from the one dimensional case.

1 Introduction

An exact covering system (ECS) is a partition of the integers into a finite set of arithmetic sequences. A significant amount of work has been done in the last 20 years on ECS's. The primary results are enumerated in the following theorem [4]:

Theorem 1 (Classical Results on Exact Covering Systems) *Let d_i for $i = 1, \ldots, m$ be the common differences of the arithmetic sequences in an exact covering system with $m > 1$ such that $d_1 \leq d_2 \leq \ldots \leq d_m$. Then*
(i) $\sum_{i=1}^{m} \frac{1}{d_i} = 1$;
(ii) $\forall\ i\ \exists\ j \neq i$ *such that* $d_i \mid d_j$;
(iii) if p is the smallest prime divisor of d_m, then $d_m = d_{m-1} = \ldots = d_{m-p+1}$.

One would like to characterize all ECS's to better understand them. This paper has two parts. In the first part we introduce and apply certain new methods for analyzing ECS's as well as using standard methods to produce new results, all towards the end of complete characterization. In the second part we analyze a generalization of the problem to n dimensions.

Many generalizations have been proposed, but the most common is replacing arithmetic sequences by congruences

$$\sum_{j=1}^{n} a_{ij}x_j \equiv a_{i0} \pmod{d_i} \quad \text{for } i = 1, \ldots, m$$

in the space $\mathbb{Z}^n$. For example, in [3], Fabrykowski proves that Theorem 1 applies in the given generalization for all n when the common factors are removed so that $(d_i, a_{i0}, a_{i1}, \ldots, a_{in}) = 1$ for all i. However, in this paper we analyze the more general extension of partitioning $\mathbb{Z}^n$ into a finite number of translates of sublattices of $\mathbb{Z}^n$, of which the subsets defined by the congruences are a particular case. However, in both cases, taking $n = 1$ reduces to the problem of ECS's.

2 Exact Covering Systems: The case of $n = 1$

2.1 Definition

For simplicity, we define a general notation for ECS's to be used in this section. An ECS P is a set of m arithmetic sequences S_i for $i = 1, \ldots, m$ that partition $\mathbb{Z}$. Each arithmetic sequence is represented by an ordered pair of integers, (a_i, d_i), with $d_i \geq 1$. The sequence that corresponds to the ordered pair (a_i, d_i) is the numbers of the form $a_i + nd_i$ for $n \in \mathbb{Z}$. Also, let $D = [d_1, \ldots, d_m]$ be the *least common modulus* (LCM) of the ECS. Note that there is no restriction on the ordering of the d_i's as in Theorem 1.

2.2 The Inductive Method

We now define an inductive method useful for general questions about ECS's. An inductive method has already been defined and applied, as in [1], but the inductive method here is both simpler and easier to apply. First, we must define *simple substitution*, a method used to obtain more complex ECS's from simpler ones. In essence, simple substitution involves replacing an arithmetic sequence of P by k new arithmetic sequences each with k times as large a common difference and spaced to partition the original arithmetic sequence (see Appendix A for a formal definition). Given this definition we can now define our induction method as in the following theorem. Let Q be some property of ECS's and define $Q(P)$ to be true if P has the property Q and false otherwise.

Theorem 2 (The Inductive Method) *If $Q(P) \Leftrightarrow Q(P')$ whenever P' is obtained from P by simple substitution, and if Q holds for some particular ECS, then Q holds for all ECS's.*

Proof: We apply simple substitution to the given ECS with property Q and to an arbitrary ECS so that both are transformed into the same ECS, one which consists solely arithmetic sequences with the same common difference. Since property Q is preserved under

these transformations we see that property Q must hold for the arbitrary ECS, completing the proof. See Appendix B for details.

We now give new proofs of some classical results regarding ECS's using this induction method.

Theorem 3 *For any ECS P with $0 \leq a_i < d_i$ for $i = 1, \ldots, m$, we have*
(i) $\sum_{i=1}^{m} \frac{1}{d_i} = 1$;
(ii) $\sum_{i=1}^{m} \frac{a_i}{d_i} = \frac{m-1}{2}$;
(iii) $\sin \pi z = -2^{m-1} \prod_{i=1}^{m} \sin(\frac{\pi}{d_i}(a_i - z))$.

Proof: *(i)* clearly holds for the trivial partition with one arithmetic sequence. When we replace some arithmetic sequence by simple substitution we get k new arithmetic sequences each with new common difference k times the original. Summing k terms of the form $\frac{1}{kd_i}$ we get $\frac{1}{d_i}$. Hence, the sum is preserved by simple substitution; all the conditions for the induction method are met, and *(i)* holds for all ECS's. The other two follow similarly. See Appendix C for details.

2.3 Irreducible Exact Covering Systems

Definition 1 *An ECS is called* reducible *if there exists a nonempty proper subset I of $\{1, \ldots, m\}$ such that $\bigcup_{i \in I} S_i$ is itself an arithmetic sequence; otherwise the ECS is* irreducible.

The obvious *irreducible exact covering systems* (IECS's) are those such that for some prime p, $m = p$ and $(a_i, d_i) = (i, p)$ for all $1 \leq i \leq p$. However, other IECS's exist, such as $P = \{(0,6), (1,10), (2,15), (4,15), (5,15), (7,15), (8,15), (10,15), (13,15), (14,15), (3,30), (9,30), (15,30), (16,30), (26,30), (27,30)\}$. For any arbitrary reducible ECS P, we can repeatedly combine subsets of the arithmetic sequences of P into single arithmetic sequences until we obtain an IECS. It is therefore sufficient to characterize IECS's, on which the rest of our analysis will focus.

2.4 The Lattice Parallelotope Method

The general method of *lattice parallelotopes* (see Appendix A for a definition) was introduced originally in [2] to analyze the *multiplicity* of an ECS P, namely the largest number of times that any one d_i occurs among the arithmetic sequences of P. However, here we will use this method to analyze the structure of IECS's, also combining this method with the polynomial method we will introduce in Section 2.6. First, we will define a slightly different version of the lattice parallelotope method more appropriate for our purposes. In essence, we create one axis of the parallelotope for each prime factor of the LCM, counting multiplicities. We then use the Chinese Remainder Theorem to create a bijection between elements of $\mathbb{Z}/D\mathbb{Z}$ and points in the lattice parallelotope (see Appendix D for a detailed description). This is a useful description because all arithmetic sequences map to *cells* with certain restrictions on their index sets. These objects are easy to define and work with. Hence, we can reduce all questions about ECS's to questions about partitions of lattice parallelotopes into cells, sometimes with certain restrictions on the index sets of the cells. Let p_1, p_2, and p_3 be three distinct primes. In the following section we use this method to characterize and count the number of IECS's with LCM $p_1^2 p_2 p_3$.

2.5 Irreducible Exact Covering Systems with Least Common Modulus $p_1^2 p_2 p_3$

Let p_1, p_2, and p_3 be three distinct primes. All IECS's with LCM $p_1 p_2 p_3$ have been characterized and counted in [5]. It was shown that there are exactly $(2^{p_1} - 2)(2^{p_2} - 2)(2^{p_3} - 2)$ IECS's of this form. Here, we analyze the problem of characterizing and counting all IECS's with LCM $p_1^2 p_2 p_3$. We must first define a $p_1^2 p_2 p_3$ *partitioning set*. This is a complicated set consisting of a number of partitions of $\{0, \ldots, p_1 - 1\}$ and one subset of $\{0, \ldots, p_i - 1\} \times B_1$ for each of $i = 2, 3$ and for B_1 a subset of $\{0, \ldots, p_1 - 1\}$. See Appendix A for a complete definition.

Using $p_1^2p_2p_3$ partitioning sets we can characterize and count all IECS's with LCM $p_1^2p_2p_3$. The proofs of these theorems are in Appendix E.

Theorem 4 (Characterization of IECS's with LCM $p_1^2p_2p_3$) *There is a bijection between irreducible exact covering systems with least common modulus $p_1^2p_2p_3$ and $p_1^2p_2p_3$ partitioning sets.*

Theorem 5 *Let $f(a,b)$ be the number of subsets S of $\{1\dots a\}\times\{1\dots b\}$ so that fixing any one coordinate we can find a value for the other so that the ordered pair is not in S, and let $g(p_1,p_2,p_3)$ be the number of IECS's with LCM $p_1^2p_2p_3$. Then, the following equations give the values for these two functions.*

$$f(a,b)=\sum_{i=0}^{a}\sum_{j=0}^{b}(-1)^{i+j}\tbinom{a}{i}\tbinom{b}{j}2^{ab-ib-ja+ij}$$

$$g(p_1,p_2,p_3)=\sum_{k=1}^{p_1}((2^{p_2}-1)^k-f(k,p_2))((2^{p_3}-1)^k-f(k,p_3))(2^{p_1}-2)^k\tbinom{p_1}{k}2^{p_1-k}$$

The complexity of these equations and the $p_1^2p_2p_3$ partitioning set shows the difficulty of the general problem.

2.6 Polynomials and Generating Functions

A common method used to analyze problems about ECS's involves the method of generating functions. Fixing the a_k's so that[1], $0\le a_k<d_k$, we note that $x^{a_k}(1+x^{d_k}+x^{2d_k}\dots)=x^{a_k}/(1-x^{d_k})$ includes all the non-negative powers of x with exponents in S_i. Since the S_i's partition $\mathbb{Z}$, taking the sum of these terms over all k's gives $1+x+x^2+\ldots=1/(1-x)$. Hence, we have formally that

$$\sum_{k=1}^{m}\frac{x^{a_k}}{1-x^{d_k}}=\frac{1}{1-x}.$$

[1]we use k's instead of i's here as indices to avoid confusion with the imaginary number i

Analysis of this equation using derivatives is a common method for proving theorems about ECS's. Additionally, part (ii) of Theorem 1 is obtained by substituting $\omega_k = e^{2\pi i/d_k}$ into these functions and examining the convergence or divergence of each side. However, by instead looking at the ECS modulo the LCM D, and mapping each element x of $\mathbb{Z}/D\mathbb{Z}$ to x^{ω_k}, we obtain certain new relationships. For a given arithmetic sequence S_k in the ECS, we define a set A_k to consist of integers b so that $0 \leq b < D$ and b is in the arithmetic sequence S_k. Additionally, to each arithmetic sequence S_k, we assign the polynomial $f_k(x) = \sum_{b \in A_k} x^b$. Now, since the S_k's partition the integers from 0 to $D-1$, it follows that $\sum_{k=1}^{m} f_k(x) = \sum_{j=0}^{D-1} x^j = \frac{x^D-1}{x-1}$.

We now fix a particular index l. Since ω_l is a root of $\frac{x^D-1}{x-1}$, assuming that $D \geq 2$, it is also a root of $\sum_{k=1}^{m} f_k(x)$. We will now determine k's for which ω_l is also a root of $f_k(x)$. Since d_i divides D we have, from the definitions of $f_k(x)$ and S_k that

$$f_k(x) = \sum_{j=0}^{(D/d_k)-1} x^{a_k+jd_k} = x^{a_k} \sum_{j=0}^{(D/d_k)-1} x^{jd_k} = x^{a_k} \frac{x^D-1}{x^{d_k}-1}.$$

Now, $f_k(\omega_l) = 0$ for any k with d_l not dividing d_k, so if we sum over d_k with d_l divides d_k we obtain a polynomial with coefficients in $\{0,1\}$ with ω_l as a root, namely

$$h_l(x) = \sum_{k \text{ with } d_l | d_k} f_k(x).$$

Using the results of Appendix E, we see the link between these polynomials and ECS's since each such polynomial is a linear combination of polynomials corresponding to other arithmetic sequences, namely those of the form $\frac{x^{d_k}-1}{x^{d_k/p}-1}$ for primes p dividing d_k. Also, each IECS yields polynomials with specific properties. We conjecture that all polynomials having these properties yield IECS's. If this were true these polynomials would assist us in characterizing all IECS's. To further understand the connection between ECS's and these polynomials we must combine the polynomial method with the lattice parallelotope method

as we do in the following section.

2.7 Polynomials and Lattice Parallelotopes

In this section we will analyze those IECS's for which at least one d_i is actually the LCM, say $d_k = D$. Now, the polynomial $h_k(x)$ as defined in Section 2.6 is a sum of all those i for which $d_i = D$, since $d_k = D$ is maximal. Also, for $d_i = D$, the polynomial $f_i(x)$, as defined in Section 2.6, is a monic monomial. Hence, any polynomial of degree $D-1$ or lower with coefficients in $\{0, 1\}$ is a prospect for the $h_k(x)$ corresponding to some IECS. Now, for some fixed LCM D, we define an *IECS-inducing polynomial* and a *potential IECS-inducing polynomial* as follows.

Definition 2 *For a fixed integer D, a polynomial* $\sum_{v \in V} x^v$ *with coefficients in* $\{0, 1\}$ *is an* IECS-inducing polynomial *if there exists some IECS with LCM D such that there is an arithmetic sequence in the IECS with* $a_i = v$ *and* $d_i = D$ *if and only if* $v \in V$*.*

Definition 3 *For a fixed integer D, a polynomial with coefficients in* $\{0, 1\}$ $\sum_{v \in V} x^v$ *is a* potential IECS-inducing polynomial *if* $e^{2\pi i/D}$ *is a root of the polynomial and for any nonempty* $U \subset V$ *and prime p dividing D,* $\frac{x^D-1}{x^{D/p}-1}$ *does not divide* $\sum_{u \in U} x^u$*.*

All IECS-inducing polynomials are potential IECS-inducing polynomials since $\omega_k = e^{2\pi i/D}$ is a root of the IECS-inducing polynomial $h_k(x)$, and if any subset did yield a polynomial divisible by $\frac{x^D-1}{x^{D/p}-1}$ for some prime p dividing D that subset would be reducible to arithmetic sequences with $d_i = \frac{D}{p}$, an impossibility since the ECS under consideration is irreducible. If all potential IECS-inducing polynomials were also IECS-inducing polynomials we would have a good way of characterizing IECS's. However, we have the following non-trivial counter example showing that the link between IECS's and polynomials is not as strong as expected.

Theorem 6 *The polynomial* $f(x) = x^{104} + x^{103} + x^{97} + x^{94} + x^{92} + x^{91} + x^{89} + x^{88} + x^{83} + x^{82} + x^{79} + x^{76} + x^{74} + x^{73} + x^{68} + x^{67} + x^{62} + x^{61} + x^{59} + x^{58} + x^{53} + x^{52} + x^{50} + x^{47} + x^{46} + x^{44} + x^{38} + x^{37} + x^{34} + x^{32} + x^{31} + x^{29} + x^{23} + x^{21} + x^{19} + x^{17} + x^{16} + x^{15} + x^{13} + x^{8} + x^{4} + x^{2} + 1$ *is a potential IECS-inducing polynomial but not an IECS-inducing polynomial.*

Proof: See Appendix E.

3 Partitions of $\mathbb{Z}^n$ into Translates of Sublattices: The Case of General n

3.1 Extensions from the One Dimensional Case

Along with generalizing the integers to $\mathbb{Z}^n$ and replacing arithmetic sequences by translates of sublattices we must find the appropriate generalization of the a_i's and d_i's. One standard form of representing sublattices of $\mathbb{Z}^n$ involves placing n independent basis vector of the sublattice into the columns of a square $n \times n$ matrix. We then let the translate be represented by a column vector. Letting the matrix be D_i and the column vector A_i we find that the translate of the sublattice includes all elements of $\mathbb{Z}^n$ of the form $D_i x + A_i$ for column vectors $x \in \mathbb{Z}^n$.

In terms of the numerical value d_i from ECS's we see that these correspond to the inverses of the density of the arithmetic sequence within the integers. We therefore let $d_i = |\det D_i|$ be the value corresponding to the d_i's of the arithmetic sequences. In terms of the LCM we see that this is the modulus of the arithmetic sequence that is the intersection of all of the S_i's when centered at 0. We therefore define a *maximal common lattice* (MCL), L_0, as the intersection of all the sublattices when centered at the origin, which, by classical linear algebra, is known to be a sublattice itself. Using these correspondences we now give a generalization of a number of methods used to analyze ECS's. For brevity, we call these partitions of $\mathbb{Z}^n$ generalized exact covering systems (GECS's).

3.2 The General Inductive Method

We again define the concept of *simple substitution* for GECS's to explain our inductive method. In essence, we take one basis vector of a particular translated sublattice L and replace L with k new translated sublattices by partitioning L along this basis vector. With $n = 1$ this generalized simple substitution reduces to simple substitution for ECS's. See Appendix A for a formal definition of generalized simple substitution.

Now, we have the following analogue of Theorem 2. Again we let Q be some property of a GECS and let $Q(P)$ be true if property Q holds for the GECS P and false otherwise.

Theorem 7 (The Generalized Induction Method) *Let Q be some property of GECS's. If $Q(P) \Leftrightarrow Q(P')$ whenever P' is obtained from P by simple substitution, and Q holds for some particular GECS, then Q holds for all GECS's.*

Proof: The proof in entirely analogous to that for ECS's, reducing each GECS to that with all D_i's the maximal common lattice of two MCL's. See Appendix H for details.

As an example of this generalized inductive method we prove a result corresponding to part *(i)* of Theorem 1. This result also has the value of demonstrating that the d_i's defined for GECS's do indeed correspond well to the d_i's of ECS's.

Theorem 8 *If some GECS has m translated sublattices with corresponding d_i's for $i = 1, \ldots, m$ as defined in Section 3.1 then*

$$\sum_{i=1}^{m} \frac{1}{d_i} = 1.$$

Proof: When we replace one of the translated sublattices by k new ones using simple substitution the determinants of the new matrices we obtain are each kd_i. Therefore, the sum mentioned in the theorem is unaltered by simple substitution, and since the theorem holds for the trivial GECS of a single translated sublattice, namely $\mathbb{Z}^n$ itself, the theorem holds for all GECS's.

3.3 Generalization of the Generating Functions and Polynomials

It is difficult to generalize either the generating functions and polynomials used to analyze ECS's since there is no simple way to restrict the generating functions to those with positive exponents. However, by mapping each element of $\mathbb{Z}^n/L_0\mathbb{Z}^n$ to a root of unity, L_0 the MCL, we can again establish certain necessary relationships between the sum of the elements covered by each translated sublattice. For a given translated sublattice L in a GECS P let the n basis vectors, the columns of D, be B_k for $k = 1, \ldots, n$. We then have the following generalization of the method used for ECS's of corresponding integers to roots of unity. We call a GECS *trivial* is it consists of only one translated sublattice and *non-trivial* otherwise.

Theorem 9 *Let P be a non-trivial GECS and let L be one particular translated sublattice of P. If H is a horizontal vector with rational coordinates so that $HB_k \in \mathbb{Z}$ for $k = 1, \ldots, n$ then there exists another translated sublattice L' in P so that $HB'_k \in \mathbb{Z}$ for $k = 1, \ldots, n$.*

Proof: We let each element of $\mathbb{Z}^n/L_0\mathbb{Z}^n$ correspond to a complex number, where L_0 is the MCL. We then show that the sum of these numbers over all the elements is 0 but the sum over the elements of the given translated sublattice L is nonzero. So there must exist another translated sublattice with nonzero sum, which means that it must have the given property, completing the proof. See Appendix I for details.

In the following two sections we use the results of Theorem 9 to prove some results about GECS's for some specific cases, attempting to generalize the results obtained for ECS's.

3.4 The Case of Parallel Bases

We prove here some theorems regarding GECS's for which there exists some basis of $\mathbb{Z}^n$ so that every translated sublattice in the GECS has a basis with each of the n vectors parallel to one of the vectors of the basis of $\mathbb{Z}^n$.

Theorem 10 *If some non-trivial GECS has the parallel bases property as defined above then for any sublattice L with matrix D in the GECS there is another sublattice L' with matrix D' so that $D'\mathbb{Z}^n$ is a sublattice of $D\mathbb{Z}^n$.*

Proof: We first apply some elementary transformations to the GECS to write all the matrices D_i as diagonal matrices. We then apply Theorem 9 using as H the horizontal vector with entries that are the inverses of the entries along the diagonal of one particular D_i. This gives the desired proof. See Appendix J for details.

Theorem 11 *If all of the translated sublattices of some non-trivial GECS have bases parallel to a particular fixed basis of $\mathbb{Z}^n$ there are two translated sublattices in GECS that are translates of one another.*

Proof: Let L with matrix D be one translated sublattice in the GECS with maximal d_i. By Theorem 10 there is another translated sublattice in the GECS L' with matrix D' so that $D'\mathbb{Z}^n$ is a sublattice of $D\mathbb{Z}^n$. However, if D' were something other than D itself it would have a larger value of d_i' than d_i. Therefore, $D = D'$ and L and L' are translates of one another.

Note that when Theorem 10 is applied with $n = 1$ we find that all ECS's have the parallel bases property and the property shown in Theorem 10 is equivalent to d_i dividing d_j. Hence, Theorem 10 is a generalization of part *(ii)* or Theorem 1. For our final section we restrict our attention to the case of $n = 2$ to obtain a result for arbitrary GECS's.

3.5 The Case of $n = 2$

Although we are not able to show that there are two translated sublattices that are translates of one another in a general GECS with $n = 2$ we can prove a result that is almost as strong.

Theorem 12 *For any vector V in $\mathbb{Z}^2$ and non-trivial GECS with $n = 2$ we can find two translated sublattices of the GECS, L and L', with bases B_1, B_2 and B_1', B_2' respectively, so that $B_1 = B_1'$, both parallel to V, and B_2 is parallel to B_2'.*

Proof: We first apply some elementary transformations to the GECS and V so that $V = \binom{1}{0}$. We then write all the matrices D_i in the form $\left(\begin{smallmatrix} a_i & b_i \\ 0 & c_i \end{smallmatrix}\right)$ with $a_i, c_i > 0$ and $0 \leq b_i < a_i$. We then apply Theorem 9 to the matrix $D = \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ with maximal c_i of those with maximal a_i using $H = \left(\frac{1}{a} \ -\frac{b}{ac}\right)$ to find another translated sublattice with the required relationship, completing the proof. See Appendix K for details.

4 Conclusion

We have introduced the inductive and polynomial methods to analyze exact covering systems and applied the lattice parallelotope method to characterize and enumerate irreducible exact covering systems with least common modulus $p_1^2 p_2 p_3$. Remaining problems include characterizing general irreducible exact covering systems and determining more exactly the properties necessary for a polynomial to be IECS-inducing. We then generalized the problem to n dimensions and showed a few results towards the goal of proving that in arbitrary non-trivial generalized exact covering systems there are two translated sublattices that are translates of one another. It is still an open problem whether this is true, and if not what the appropriate generalization is.

5 Acknowledgments

I would like to thank Dr. Payman Kassaei, who recently graduated from the MIT graduate school in mathematics, for all his assistance and motivation in researching this field. I would also like to thank the Center for Excellence in Education and the Research Science Institute for providing me with the facilities to perform this research and the staff for their assistance in all parts of my project.

References

[1] Beebee, John, Some trigonometric identities related to exact covers, *Proceedings of the American Mathematical Society*. **112** (1991) 329–338.

[2] Berger, M.A. et al., Lattice parallelotopes and disjoint covering systems, *Discrete Mathematics*. **65** (1987) 23–46.

[3] Fabrykowski, J., Multidimensional covering systems of congruences, *Acta Arithmetica*. **43** (1984), no. 2, 191–208.

[4] Guy, Richard K., *Unsolved Problems in Number Theory*, Springer-Verlag, 1994.

[5] Korev, Ivan, Irreducible disjoint covering systems of Z with the common modulus consisting of three primes, *Acta Mathematica Universitatis Comenianae*, **47** (1986) 75–81.

A Definitions

Definition 4 *Let P be an ECS and k an integer, $k \geq 2$, and let P' be an ECS with $m+k-1$ arithmetic sequences so that*

(i) $d'_i = d_i, a'_i = a_i$ *for* $i = 1 \ldots m-1$

(ii) $d'_{m+j} = kd_m, a'_{m+j} = a_m + jd_m$ *for* $j = 0 \ldots k-1$

We say that P' is obtained from P by simple substitution.

Definition 5 *Given a positive integer t and t positive integers g_i for $i = 1 \ldots t$ we define a* lattice parallelotope L *to be*

$$L = \mathbb{Z}/g_1\mathbb{Z} \times \mathbb{Z}/g_2\mathbb{Z} \times \ldots \times \mathbb{Z}/g_t\mathbb{Z}.$$

Definition 6 *For a given lattice parallelotope L, some index set $I \subset \{1 \ldots t\}$, and $|I|$ integers u_i for $i \in I$ we define a* cell C *as the subset of L consisting of those elements of L whose i^{th} coordinates are u_i for all $i \in I$.*

Definition 7 *A* $p_1^2 p_2 p_3$ partitioning set *consists of*

- *any partition of $\{0, \ldots, p_1 - 1\}$ into three subsets, B_1, B_2, and B_3, B_1 nonempty*
- *$|B_1|$ partitions of $\{0, \ldots, p_1 - 1\}$ into two non-empty sets, C_{i2} and C_{i3} for $i \in B_1$*
- *and one subset of each of $\{0, \ldots, p_2 - 1\} \times B_1$ and $\{0, \ldots, p_3 - 1\} \times B_1$, D_2 and D_3 respectively, so that for $i = 2, 3$ if we view D_i as a subset of the entries in a matrix with $|B_1|$ rows and p_i columns appropriately indexed then D_i contains an entire column but doesn't contain all the elements in any one row.*

For this definition let e_i for $i = 1, \ldots, n$ be a column vector with all 0's except for one 1 in position i.

Definition 8 *Let P be a GECS, k an integer with $k \geq 2$, and l some integer with $1 \leq l \leq n$, and let P' be another GECS with the same sublattices as P except one, L, with matrix D and translate A, which is replaced by k new lattices with matrix D' and translates A'_i for $i = 0, \ldots, k-1$ so that*

(i) $D' = D((k-1)e_l + \sum_{i=1}^{n} e_i)$

(ii) $A'_i = A + iDe_l$

We say that P' is obtained from P by simple substitution.

B Proof of Induction Method

Let P_0 be the particular ECS that has property Q. Now, let P_1 be some arbitrary ECS. We will show that P_1 has property Q. Let $D_0 = [D, D']$ be the least common multiple of the LCM's of each ECS. Now, for each arithmetic sequence S_i with common difference d_i in P_0 use simple substitution to replace it by $\frac{D_0}{d_i}$ new arithmetic sequences, each with a common difference of D_0. At each step we obtain a new ECS for which property Q holds because it is invariant under simple substitution. Let the final ECS with D_0 arithmetic sequences be called P_2. Next, perform the same transformations on P_1, again arriving at P_2 and both being equivalent under property Q . We then have $Q(P_0) \Leftrightarrow Q(P_2) \Leftrightarrow Q(P_1)$, and since $Q(P_0)$ holds by assumption so does $Q(P_1)$, completing the proof.

C Applications of the Induction Method

We here prove parts *(ii)* and *(iii)* of Theorem 3. Again, we can check that *(ii)* holds for $m = 1$, $a_1 = 0$, and $d_1 = 1$. Now, when we substitute k arithmetic sequences for a given one we get k arithmetic sequences of the form $(a_i + ld_i, kd_i)$ for $l = 0, \ldots, k-1$. The new sum is then

$$\sum_{l=0}^{k-1} \frac{a_i + ld_i}{kd_i} = \frac{ka_i}{kd_i} + \frac{1}{k}\sum_{l=0}^{k-1} l = \frac{a_i}{d_i} + \frac{k-1}{2}.$$

Since we add $\frac{1}{2}$ for each of the $k-1$ new sequences to each side of the equation in *(ii)* the induction holds, and since we have found it true for one ECS, we have *(ii)* as desired.

The case of one arithmetic sequences in the ECS also yields truth for *(iii)*, so again we only need to check the inductive step. Now, we rely on the well known fact that

$$2\sin y = \prod_{l=0}^{k-1} \left(2\sin\left(\frac{y + l\pi}{k}\right)\right).$$

When we substitute k arithmetic sequences for one we replace one term of the product by k new ones which satisfy the following equality. We rely on the above equality for the last step of this equation.

$$\prod_{l=0}^{k-1} \sin\left(\frac{\pi}{kd_i}\left(a_i + ld_i - z\right)\right) = \frac{1}{2^k}\prod_{l=0}^{k-1}\left(2\sin\left(\frac{\left(\frac{\pi}{d_i}(a_i - z)\right) + l\pi}{k}\right)\right) = \frac{1}{2^k} 2\sin\left(\frac{\pi}{d_i}(a_i - z)\right).$$

Again, we see that the term is replaced by something equivalent, noting that the appropriate number of powers of 2 are added, and since we have shown the equation in *(iii)* true for one ECS, the induction method shows it true for all ECS's, completing the proof.

D Description of the Lattice Parallelotope Method

Write $D = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$, D the LCM, with p_i prime. Consider the lattice parallelotope L with $t = \sum_{i=1}^{s} r_i$ and $g_j = p_k$ for $\sum_{i=1}^{k-1} r_i < j \leq \sum_{i=1}^{k} r_i$. In other words, let there be one g_i in L for each prime divisor of D, counting multiplicities. Now, for each $x \in \mathbb{Z}/D\mathbb{Z}$ let b_i for $i = 1, \dots, s$ be the integers for which $x \equiv b_i \pmod{p_i^{r_i}}$ and $0 \leq b_i < p_i^{r_i}$, and let c_{ij} for $i = 1, \dots, s$ and $j = 0, \dots, r_i - 1$ be the integers for which $0 \leq c_{ij} < r_i$ and

$$b_i = \sum_{j=0}^{r_i-1} c_{ij} p_i^j.$$

Then the mapping

$$x \mapsto \left(c_{10}, \ldots c_{i(r_1-1)}, c_{20}, \ldots, c_{2(r_2-1)}, \ldots, c_{s0}, \ldots, c_{s(r_s-1)}\right)$$

is a bijection by the Chinese Remainder Theorem, so the images of the arithmetic sequences partition L. Now, since an arithmetic sequence consists of all those x satisfying $x \equiv a_i \pmod{d_i}$ its image is the set of all elements of L with some coordinate fixed and the others free. Formally, if $d_i = p_1^{r'_1} p_2^{r'_2} \ldots p_s^{r'_s}$ with $0 \leq r'_i \leq r_i$ for $i = 1, \ldots, s$, then $x \in S_i$ if and only if $x \equiv a_i \pmod{p_i^{r'_i}}$ for $i = 1, \ldots, s$. So the image of x is in the image of S_i if and only if exactly r'_i of the r_i coordinates with $g_k = p_i$ are some fixed value and the remaining $r_i - r'_i$ are arbitrary. Therefore, the images of arithmetic sequences are exactly those *cells* with index sets that contain only the first r'_i indices of each group of r_i coordinates with $g_k = p_i$ for arbitrary integers r'_i with $0 \leq r'_i \leq r_i$ (see Appendix A for a definition of *cells*).

E Polynomials Related to Exact Covering Systems

In this section we will analyze polynomials of the form $h_k(x)$ as defined in Section 2.6, and show that they can all be written as a linear combination of polynomials of the form $\frac{x^{d_k}-1}{x^{d_k/p}-1}$ for primes p dividing d_k.

Lemma 1 *$\Phi_{d_k}(x) \mid h_k(x)$ where the polynomials are viewed as polynomials in $\mathbb{Z}[x]$.*

Proof: As was shown in Section 2.6, $\omega_k = e^{2\pi i/d_k}$ is a root of $h_k(x)$. Also, since the coefficients of $h_k(x)$ are in $\mathbb{Z}$, all of the primitive d_k^{th} roots of unity must be solutions to $h_k(x) = 0$. Hence $\Phi_{d_k}(x)$, the fundamental cyclotomic polynomial whose roots are exactly the d_k^{th} primitive roots of unity, must satisfy $\Phi_{d_k}(x) \mid h_k(x)$, as was to be shown.

Lemma 2 *$\Phi_n(x)$ can be written as a linear combination of the polynomials $\frac{x^n-1}{x^{n/p}-1}$ for all primes $p \mid n$ using coefficients in $\mathbb{Q}[x]$.*

Proof: Let $\omega = e^{2\pi i/n}$ be a primitive n^{th} root of unity. The roots of $\frac{x^n-1}{x^{n/p}-1}$ are exactly those numbers of the form ω^l for which $p \nmid l$. Hence, the numbers that are the roots of all the polynomials under consideration are those numbers of the form ω^l where $p \nmid l$ for all primes $p \mid n$. In other words, the common roots are those numbers ω^l for which $(n, l) = 1$, the primitive n^{th} roots of unity. Since $\mathbb{Q}[x]$ is a euclidean domain, $\Phi_n(x)$, the least common multiple of the polynomials under consideration, can be written as a linear combination of these polynomials. Hence, the lemma is proven.

Theorem 13 *For any ECS and integer k with $1 \leq k \leq m$ the polynomial $h_k(x)$ as defined in Section 2.6, can be written as a linear combination of the polynomials $\frac{x^{d_k}-1}{x^{d_k/p}-1}$ for primes $p \mid d_k$ using polynomials in $\mathbb{Q}[x]$ as coefficients.*

Proof: From Lemma 1 we have $h_k(x) = q(x)\Phi_{d_k}(x)$ for some polynomial $q(x) \in \mathbb{Z}[x]$, and from Lemma 2, Φ_{d_k} can be written as a linear combination of the polynomials described above. Multiplying by $q(x)$ each of the polynomials used as coefficients for writing $\Phi_{d_k}(x)$, we get a representation for $h_k(x)$ as a linear combination under the conditions required, completing the proof.

F Proofs of Theorems regarding IECS's with LCM $p_1^2 p_2 p_3$

Before giving the actual proofs of the theorems we will discuss the lattice parallelotope method as applied to IECS's with LCM $p_1^2 p_2 p_3$ and prove a number of lemmas.

We view the lattice parallelotope L corresponding to the IECS as a stack of p_1 3-dimensional parallelepipeds with sides p_1, p_2, and p_3, where the p_1 axis in the parallelepiped is vertical and corresponds to c_{11} of Appendix D. Hence, based on the results of Appendix

D, the only restriction on the index sets of cells partitioning L is that if c_{10} is free to vary then so must c_{11} be. In other words, any cell that includes points in all p_1 parallelepipeds must also include entire vertical lines if it includes any point in the line. So, the valid cells, those that correspond to arithmetic sequences, are points, lines, and planes contained within specific parallelepipeds, entire parallelepipeds, and cells though all p_1 parallelepipeds with vertical lines or planes with vertical components as their image in each parallelepiped. We will now prove a number of lemmas regarding IECS's with LCM $p_1^2 p_2 p_3$. In each we use IECS to mean specifically an IECS with LCM $p_1^2 p_2 p_3$ for three distinct primes p_1, p_2, and p_3.

Lemma 3 *The IECS can not include any cells with three dimensions.*

Proof: Assume for contradiction that an IECS did include such a cell. Then, no cell can have a dimension along the fourth axis because it would then intersect the one with that coordinate fixed and the other three free. Hence, all the cells would be confined to three dimensional areas parallel to the given cell. Since it must be irreducible, this means that the partition consists of p_i parallel cells for some i. However, in the case all the d_i's would be p_i, a contradiction since the LCM is not a single prime.

We need a definition before giving the next lemma.

Definition 9 *Given two sets, X_1 and X_2, a subset of $X_1 \times X_2$ is called a* grid *if it equals $X_1' \times X_2'$ for some $X_1' \subset X_1$ and $X_2' \subset X_2$.*

Lemma 4 *In any one of the parallelepipeds the vertical lines and the images of the planes passing through all the parallelepipeds form a grid with respect to the p_2 and p_3 axes.*

Proof: Assume for contradiction that a parallelepiped exists where the lines and images are not a grid. This means there must be two vertical lines or images, say at positions (x_1, y_1) and (x_2, y_2) of $\{0 \ldots p_2 - 1\} \times \{0 \ldots p_3 - 1\}$, so that there is no line at (x_1, y_2). Now, the only other cells that could pass through this area are lines along the p_2 or p_3 axes or planes within the parallelepiped. However, all of these would intersect one of the vertical lines or

images at (x_1, y_1) and (x_2, y_2). Hence, the entire position must consist of p_1 points. Then, however, we can combine these into a single vertical line, violating the irreducibility of the ECS.

Lemma 5 *The images of the planes that pass through all the parallelepipeds form a grid with respect to the p_2 and p_3 axes.*

Proof: Assume, for contradiction, that there exists two pairs of coordinates (x_1, y_1) and (x_2, y_2) which contain the images of these planes but that there is no such plane at (x_1, y_2). Then, by Lemma 4, since the vertical lines and the images of the planes form a grid, there must be a vertical line at position (x_1, y_2) in each of the p_1 parallelepipeds. However, these p_1 vertical lines can be reduced to a plane through all the parallelepipeds, violating the irreducibility of the ECS, giving the contradiction we wanted.

Lemma 6 *Fixing the planes that pass through all p_1 parallelepipeds, there are only two possible ways for parallelepipeds themselves to contain planes.*

Proof: First of all, there must be at least one plane through all p_1 parallelepipeds because the entire ECS could be reduced to p_1 entire parallelepipeds instead. Also, from Lemma 5, these planes through all the parallelepipeds form a grid with respect to the p_2 and p_3 axes. Now, if any parallelepiped contains a plane it must have a vertical component to avoid intersecting the planes passing through all the parallelepipeds. Also, of the two types of planes with vertical components, if some of each type were present they would intersect violating the disjointness of the cells. We let these planes have direction vertically and along the p_2 (resp. p_3) axis. Then, for the fixed parallelepiped, they are defined by points along the p_3 (resp. p_2) axis. Since there is at least one plane the only remaining cells are lines not along the p_3 (resp. p_2) axis and points. Therefore, any planar region defined by a point on the p_3 (resp. p_2) axis not intersecting a plane passing through all the parallelepipeds must contain an entire plane since it could be simplified to one otherwise. For the planar regions

that do intersect planes passing through all the parallelepipeds the remaining area must be filled with vertical lines as the only other possibility is vertical stacks of points which could be simplified. So, any parallelepiped with a plane consists only of planes where possible and vertical lines otherwise with two possible orientations for the planes.

Lemma 7 *Given the grid of vertical lines and images of planes through all the parallelepipeds in a specific parallelepiped there are* $2^{p_1} - 2$ *choices for the remaining cells assuming there are no planes.*

Proof: Since the vertical lines and images of planes through all the parallelepipeds are given the only possible remaining cells are non-vertical lines and points. For each of the p_1 planar regions perpendicular to the vertical lines it can contain all points or points and lines in one of the two directions, since if it contained lines in both directions they would intersect. To avoid reducibility, each planar regions must contain lines in one direction every place possible and single points elsewhere. Now, of the p_1 planar regions, each can be one of the two possibilities, one for the lines in each direction. The only restriction is that there must be at least one of each for otherwise there would be p_1 lines all in the same direction right above one another that could be reduced to a plane, an impossibility since the ECS is irreducible.

Proof of Theorem 4: We will exhibit a mapping from IECS's of LCM $p_1^2 p_2 p_3$ to $p_1^2 p_2 p_3$ partitioning sets that we will then prove is a bijection.

Let each parallelepiped corresponding to one element of the set $\{0, \ldots, p_1 - 1\}$. Now, let B_1 be the set of all parallelepipeds that contain no planes, B_2 the set that contains planes positioned vertically and along the p_2 axis, and B_3 the set that contains planes positioned vertically and along the p_3 axis. Since we have shown each parallelepiped is of exactly one of these types, they partition $\{0, \ldots, p_1 - 1\}$. Also, if all the parallelepipeds contained planes and B_1 were empty, the LCM would be $p_1 p_2 p_3$, as all the cells would have lengths along the vertical p_1 axis. For each of the $|B_1|$ parallelepipeds included in the set B_1, number the

p_1 planes perpendicular to the vertical lines by the elements of $\{0, \ldots, p_1 - 1\}$. For each parallelepiped numbered in B_1 let C_{i2} be the set of planes with lines along the p_2 axis and C_{i3} the set of planes with lines along the p_3 axis. As shown in Lemma 7, these two sets must partition $\{0 \ldots p_1 - 1\}$ and neither can be empty. Finally, number the p_2 (resp. p_3) axis with the elements from $\{0 \ldots p_2 - 1\}$ (resp. $\{0 \ldots p_3 - 1\}$), and let D_2 (resp. D_3) be the set of all ordered pairs from $\{0 \ldots p_2 - 1\} \times B_1$ (resp. $\{0 \ldots p_3 - 1\} \times B_1$) for which the vertical plane with coordinate along the p_2 axis (resp. p_3 axis) fixed by the first element of the ordered pair and in the parallelepiped defined by the second contains a vertical line or the vertical line image of a plane that passes through all the parallelepiped. Clearly, for each of the two sets, there must be some element in all of them that is the image of a plane passing through all the parallelepipeds, satisfying the first condition on the sets D_2 and D_3 in the definition of $p_1^2 p_2 p_3$ partitioning sets. Also, if any one parallelepiped contained vertical lines or images of planes through all the parallelepipeds for every point along some axis, the parallelepiped would be forced to contain planes to avoid being reducible, as has been previously shown. Thus, the second constraint on D_2 and D_3 is also satisfied. Hence, this mapping yields a valid $p_1^2 p_2 p_3$ partitioning set. We will now show that this is a bijection.

We will first show the mapping to be injective. Assume that two IECS's yielded the same $p_1^2 p_2 p_3$ partitioning set. They would then have parallelepipeds with planes in the exact same places in an identical fashion since there is only one possibility for each of the two types of planes. Since the D_2 and D_3 sets specify the locations of the vertical lines and the planes passing through all the parallelepipeds those would be identical. This is true because the vertical lines with the planes passing through all the parallelepipeds along with such planes by themselves must be grids and are therefore uniquely determined by the images along the p_2 and p_3 axes. Finally, the C_{i2} and C_{i3} sets determine the location of all the non-vertical lines. The only remaining cells are points, and in both they must go in the same remaining regions. Therefore, the mapping defined is injective.

To complete the proof we will demonstrate the map to be surjective by finding a valid IECS corresponding to any $p_1^2p_2p_3$ partitioning set. First find all the points along the p_2 (resp. p_3) axis so that all the ordered pairs including that point are in the set D_2 (resp. D_3). Such points must exist by the definition of a $p_1^2p_2p_3$ partitioning set. At the locations with both coordinates points of this type place the planes that pass through all the parallelepipeds. Next, place planes in the unique way for the given direction in the parallelepipeds listed in B_2 and B_3. Place more vertical lines in a grid in each of the parallelepipeds in B_1 using the elements in D_2 and D_3 corresponding to that parallelepiped to determine the locations. Finally, use the sets C_{i2} and C_{i3} to determine the direction of the lines in each of the p_1 planes perpendicular to the vertical for each of the parallelepipeds without planes. The remaining region is naturally filled with point cells. Now, because we have points the LCM is $p_1^2p_2p_3$. So all we have to verify is that the ECS is truly irreducible. Any vertical line is either included, contained within a plane, or intersects a line along another axis. Any horizontal line is either already contained in the ECS or intersects the image of a plane passing through all the parallelepipeds. Any plane within a parallelepiped either intersects a plane passing through all the cubes, is a cell already, or intersects lines perpendicular to it. Since there are planes passing through all the parallelepipeds the parallelepipeds themselves can not be reduced. Finally, since B_1 is non-empty, any space whose image is a plane in all the parallelepipeds intersects a line perpendicular to it in each of the parallelepipeds not containing planes.

We have now shown that the mapping previously defined is a valid function from IECS's with LCM $p_1^2p_2p_3$ to $p_1^2p_2p_3$ partitioning sets. Additionally, we have shown this mapping to be both injective and surjective. Therefore we have a bijection, completing the proof of the Theorem.

For the second theorem we again prove a lemma before giving the actual proof.

Lemma 8 *If $f(a, b)$ is defined as in Theorem 5 then*

$$f(a,b) = \sum_{i=0}^{a}\sum_{j=0}^{b}(-1)^{i+j}\tbinom{a}{i}\tbinom{b}{j}2^{ab-ib-ja+ij}.$$

Proof: Let Q_{IJ} for $I \in \{1,\ldots,a\}$ and $J \in \{1,\ldots,b\}$ be the set of subset of $\{1\ldots a\} \times \{1\ldots b\}$ including every element of the form (i,j) for $i \in I$ or for $j \in J$. The number of subsets in this set is then $2^{ab-|I|b-|J|a+|I||J|}$ since $|I|b+|J|a-|I||J|$ of the points must be in the subset and the other may or may not arbitrarily. We then have by inclusion-exclusion that $f(a,b)$, the number of subsets in none of these sets, satisfies the following equalities.

$$\begin{aligned} f(a,b) &= \sum_{I\subset\{1,\ldots,a\}}\sum_{J\subset\{1,\ldots,b\}}(-1)^{|I|+|J|}|Q_{IJ}| \\ &= \sum_{I\subset\{1,\ldots,a\}}\sum_{J\subset\{1,\ldots,b\}}(-1)^{|I|+|J|}2^{ab-|I|b-|J|a+|I||J|} \\ &= \sum_{i=0}^{a}\sum_{j=0}^{b}(-1)^{i+j}\tbinom{a}{i}\tbinom{b}{j}2^{ab-ib-ja+ij} \end{aligned}$$

Proof of Theorem 5: Since there is a bijection between IECS's with LCM $p_1^2p_2p_3$ and $p_1^2p_2p_3$ partitioning sets we will count the latter which in turn counts the former. Assume that $B_1 = k$. Then we have 2^{p_1-k} choices for B_2 and B_3, as each remaining element of $\{0\ldots p_1-1\}$ can be in either of the two arbitrarily. Also, for this choice of k we have $\binom{p_1}{k}$ choices for B_1. For the sets C_{i2} and C_{i3} we have $2^{p_1}-2$ choices as each partitioning is valid except letting either one be empty. Finally, for D_2 (resp. D_3), we have $2^{p_2}-1$ (resp. $2^{p_3}-1$) choices for each of the k rows, anything but all of the points, and we must remove those with no column containing all points. This is exactly $f(p_2,k)$ (resp. $f(p_3,k)$). So, we subtract this from the earlier term and obtain the number of possibilities for D_2 (resp. D_3). Now, multiplying all these terms together and summing over all valid k we obtain the desired expression for the number of IECS's with LCM $p_1^2p_2p_3$, completing the proof.

G Potential IECS Inducing Polynomials that are not IECS Inducing Polynomials

Proof of Theorem 6: The three diagrams show the locations of the points defined by the polynomial in the lattice parallelotope with sides 3, 5, and 7. The rows run from 0 to 4 (mod 5) and the columns run from 0 to 6 (mod 7). The values (mod 3) are as written below the diagrams. From the diagram for 2 (mod 3) we see that there must be a line through all three layers through the points marked "a" since that point in the top layer cannot be in a line in any other direction. Then, the point marked "b" cannot be in a line in any direction since all three intersect existing cells. Therefore there is no IECS, indeed no ECS corresponding to the given polynomial. Therefore, it is not IECS-inducing. To show that the polynomial is potential IECS-inducing we merely need to show that $e^{2\pi i/105}$ is a root and that no subset of the terms is divisible by the polynomials described in the definition. However, the latter condition only occurs when the points in the lattice parallelotope determined by the polynomial form a line, and upon checking we see this is false. Finally, to show that $e^{2\pi i/105}$ is a root we merely show that $\Phi_{105}(x)$ is a factor of the polynomial.

X	X	a				
X		b				

Table 1: 0 (mod 3)

		a				
X		X	X	X	X	X
		X	X	X	X	X
		X	X	X	X	X
		X	X	X	X	X

Table 2: 1 (mod 3)

	X	a				
	X	X	X	X	X	X
	X	X	X	X	X	X
	X	X	X	X	X	X

Table 3: 2 (mod 3)

$$x^{104}+x^{103}+x^{97}+x^{94}+x^{92}+x^{91}+x^{89}+x^{88}+x^{83}+x^{82}+x^{79}+x^{76}+x^{74}+x^{73}+x^{68}+x^{67}+$$
$$x^{62}+x^{61}+x^{59}+x^{58}+x^{53}+x^{52}+x^{50}+x^{47}+x^{46}+x^{44}+x^{38}+x^{37}+x^{34}+x^{32}+x^{31}+x^{29}+$$
$$x^{23}+x^{21}+x^{19}+x^{17}+x^{16}+x^{15}+x^{13}+x^{8}+x^{4}+x^{2}+1=$$
$$(x^{56}-x^{54}+x^{53}+x^{50}+x^{49}-x^{48}+3x^{46}-2x^{45}+2x^{44}+2x^{43}-2x^{42}+3x^{41}+x^{39}+x^{38}+x^{37}+$$
$$2x^{36}+2x^{34}+2x^{32}+2x^{31}+2x^{29}+x^{28}+x^{27}+2x^{26}+x^{25}+x^{24}+x^{23}+x^{22}+2x^{21}+2x^{19}+$$
$$x^{18}+2x^{16}+x^{14}+x^{13}+x^{12}+x^{10}+2x^{7}-x^{6}+x^{5}+x^{2}-x+1)\times$$
$$(x^{48}+x^{47}+x^{46}-x^{43}-x^{42}-2x^{41}-x^{40}-x^{39}+x^{36}+x^{35}+x^{34}+x^{33}+x^{32}+x^{31}-x^{28}-x^{26}-$$
$$x^{24}-x^{22}-x^{20}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}-x^{9}-x^{8}-2x^{7}-x^{6}-x^{5}+x^{2}+x+1)=$$
$$(x^{56}-x^{54}+x^{53}+x^{50}+x^{49}-x^{48}+3x^{46}-2x^{45}+2x^{44}+2x^{43}-2x^{42}+3x^{41}+x^{39}+x^{38}x^{37}+$$
$$2x^{36}+2x^{34}+2x^{32}+2x^{31}+2x^{29}+x^{28}+x^{27}+2x^{26}+x^{25}+x^{24}+x^{23}+x^{22}+2x^{21}+2x^{19}+$$
$$x^{18}+2x^{16}+x^{14}+x^{13}+x^{12}+x^{10}+2x^{7}-x^{6}+x^{5}+x^{2}-x+1)\,\Phi_{105}(x)$$

H Proof of Generalized Induction Method

Let P_0 be the given GECS with property Q and let P_1 be an arbitrary GECS which we will show to have property Q. Let L_2 be the intersection of the two MCL's L_0 and L_1. Then, each translated sublattice in P_0 has bases parallel to one set of bases for L_2. By performing simple substitution along each of these basis vectors, that is, picking the appropriate value for l, we divide a given translated sublattice L of P_0 into translated sublattices that are translates of L_2. After doing this for each translated sublattice of P_0 we obtain a new GECS P_2 which consists entirely of translates of L_2. Since every step was an application of simple substitution and property Q is preserved under simple substitution, we have $Q(P_0) \Leftrightarrow Q(P_2)$. Performing the exact same procedure on P_1 we find $Q(P_1) \Leftrightarrow Q(P_2)$. Hence, $Q(P_0) \Leftrightarrow Q(P_2) \Leftrightarrow Q(P_1)$ and since Q hold for P_0, Q holds for P_1 as desired.

I Proof of Theorem 9

Let the components of H be h_k for $k = 1, \ldots, n$. Then, to each element $X \in \mathbb{Z}^n$ with components x_k for $k = 1, \ldots, n$ correspond the complex number $\prod_{k=1}^{n} e^{2\pi i h_k x_k} = e^{2\pi i \sum_{k=1}^{n} h_k x_k}$. Now, by the properties given for H, we see that the same complex number corresponds to all the elements in L. This implies that the same complex number corresponds to all the elements of the MCL, L_0, and since there is more than one translated sublattice in P when we sum over the complex numbers corresponding to all the elements of $\mathbb{Z}^n/L_0\mathbb{Z}^n$ we obtain 0. Since we see that the sum of the complex numbers corresponding to each element L is not 0 there must be another translated sublattice in the GECS which yields a nonzero sum. Now, for any translated sublattice L' where one basis vector, B'_i, does not satisfy $HB'_i \in \mathbb{Z}$ has the complex number corresponding to that basis vector some rational root of unity other than 1. Since the complex number corresponding to the bases of L_0 are all 1, when we sum over the numbers corresponding to the elements in L' of $\mathbb{Z}^n/L_0\mathbb{Z}^n$ we get 0. Therefore the other translated sublattice with nonzero sum of corresponding complex numbers shown to exist with basis vectors B'_i for $i = 1, \ldots, n$ must satisfy satisfy $HB'_i \in \mathbb{Z}$. This is the property we desired to show, completing the proof.

J Proof of Theorem 10

We use Theorem 9, but first we have to find an equivalent form of the GECS that is easier to work with. Let M be the matrix whose columns are the basis vectors of $\mathbb{Z}^n$ that are parallel to the basis vectors of each translated sublattice in the GECS. Now, it is a well known result of classical linear algebra that we can multiply the matrices D_i on the right by $n \times n$ matrices with integer entries and determinant ± 1 without changing the sublattice it describes. Therefore, we first multiply each d_i by the appropriate matrix with one 1 in each row and column and 0's elsewhere so that the k^{th} column of each D_i is parallel to the k^{th} column of M. No column of M can have all its entries divisible by an integer larger than 1

since $|\det M| = 1$. Therefore, we have that $D_i = MD'_i$ where D'_i is a diagonal matrix with entries in $\mathbb{Z}$. Now, in addition to multiplying any individual matrix D_i on the right be a matrix with determinant ± 1 we can multiply all the D_i's and A_i's on the left by a matrix with determinant ± 1 and obtain a new GECS. Also, we note that a translated sublattice L' of the GECS has its matrix D' related to the matrix D of another translated sublattice L of the GECS as in the Theorem only if this property holds for their corresponding translated sublattices in the new GECS defined above. Hence, if we multiply all the D_i's and A_i's on the left by M^{-1}, M the matrix defined above, we obtain a GECS all of whose matrices are diagonal, and the property we are trying to show holds in the new GECS if and only if it holds in the original GECS. We now apply Theorem 9.

Take an arbitrary translated sublattice L of the new GECS obtained above. Let its k^{th} entry along the diagonal of its matrix D be c_k for $k = 1, \ldots, n$. Let the horizontal vector of Theorem 9 H have as its k^{th} entry $h_k = \frac{1}{c_k}$. Then, for each of the n basis vectors of D, B_k for $k = 1, \ldots, n$, we have $HB_k = h_k c_k = 1 \in \mathbb{Z}$. Therefore, we have another translated sublattice L' with the same properties. Let the diagonal entries of the matrix for this translated sublattice D' be c'_k for $k = 1, \ldots, n$. We then have that for all k with $1 \leq k \leq n$ that $HB'_k = h_k c'_k = \frac{c'_k}{c_k} \in \mathbb{Z}$. Then $c_k \mid c'_k$, and each column of D' is a multiple of a column of D. Therefore, the matrix D' is related to the matrix D as desired, and we have the result that we wanted.

K Proof of Theorem 12

First, if the components of V are v_1 and v_2 with $[v_1, v_2] = g$, then $\frac{1}{g}V$ is one vector in some basis of $\mathbb{Z}^2$. Now, letting the matrix of these two vectors be M, we can multiply all the D_i's and A_i's of the GECS on the left by M^{-1} as in the proof of Theorem 10 to obtain a new GECS. We also note that two translated sublattices are related as in the give Theorem in the new GECS if and only if they are so related in the old, applying the same transformation

to the given vector V. Now, by the choice of the matrix M, the vector V maps to a vector V' with components v_1 and v_2 so that $v_2 = 0$. We therefore can solve the theorem in general by solving it in the case of $V = \binom{1}{0}$.

A well known result of classical linear algebra shows that for each translated sublattice in the GECS we can find a form of D_i that is an upper-triangular matrix. For each index of a translated sublattice in the GECS i let D_i be written in upper-triangular form with $D_i = \left(\begin{smallmatrix} a_i & b_i \\ 0 & c_i \end{smallmatrix}\right)$. We can restrict $a_i, c_i > 0$ by multiplying by the appropriate matrix of the form $\left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right)$. We can further restrict that $0 \leq b_i < a_i$ since we can multiply D_i on the right by $\left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right)$ for arbitrary integers r to add any multiple of a_i to b_i. Now, of the set of all translated sublattices in the GECS with maximal a_i, choose the one with maximal c_i and call the matrix for the translated sublattice $D = \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$.

We apply Theorem 9 with $H = \left(\frac{1}{a} \; -\frac{b}{ac}\right)$. We see that

$$\left(\tfrac{1}{a} \; -\tfrac{b}{ac}\right)\begin{pmatrix} a \\ 0 \end{pmatrix} = 1 \in \mathbb{Z} \text{ and } \left(\tfrac{1}{a} \; -\tfrac{b}{ac}\right)\begin{pmatrix} b \\ c \end{pmatrix} = \tfrac{b}{a} - \tfrac{b}{a} = 0 \in \mathbb{Z}$$

Hence the premise of Theorem 9 is satisfied. We now must have another translated sublattice with matrix $D' = \left(\begin{smallmatrix} a' & b' \\ 0 & c' \end{smallmatrix}\right)$ so that

$$\left(\tfrac{1}{a} \; -\tfrac{b}{ac}\right)\begin{pmatrix} a' \\ 0 \end{pmatrix} = \frac{a'}{a} \in \mathbb{Z} \text{ and } \left(\tfrac{1}{a} \; -\tfrac{b}{ac}\right)\begin{pmatrix} b' \\ c' \end{pmatrix} = \frac{b'}{a} - \frac{bc'}{ac} = \frac{b'c - bc'}{ac} \in \mathbb{Z}$$

Now, since a is maximal and $a' > 0$ we see that $\frac{a'}{a} \in \mathbb{Z} \Rightarrow a = a'$. The other condition we obtained is equivalent to $ac \mid b'c - bc'$. However, we choose the b_i's so that $0 \leq b < a$ and $0 \leq b' < a' = a$, so $0 \leq b'c < ac$ and $0 \leq bc' < ac' \leq ac$, since c was choose to be maximal of those matrices with $a_i = a$. Therefore, $ac > b'c \geq b'c - bc' \geq -bc' > -ac$, and since $ac \mid b'c - bc'$ we have $b'c - bc' = 0$, or $\frac{b}{c} = \frac{b'}{c'}$, since both c and c' are non-zero. The first basis vectors of D and D' are both $\binom{a}{0}$, which are equal and parallel to $\binom{1}{0}$. For the second basis vectors, we have that they are parallel as well since the ratio of their components are equal.

We have therefore found two translated sublattices with matrices satisfying the properties we wanted, completing the proof.