COMPOSITE COVERING SYSTEMS OF MINIMUM CARDINALITY

Scott Jenkin
8 Dargin Street, Mount Helena, WA 6082, Australia.
coveringsystems@iinet.net.au

Jamie Simpson
Department of Mathematics and Statistics, Curtin University of Technology, GPO Box U1987, Perth WA 6001, Australia
simpson@maths.curtin.edu.au

Received:3/17/03, Accepted: 9/23/03, Published:9/24/03

Abstract

We write $S(m,a)$ for the congruence class $\{n \in \mathbf{Z} : n \equiv a \pmod m\}$. A covering system of congruences is a collection

$$\{S(m_1,a_1), S(m_2,a_2), \ldots, S(m_n,a_n)\}$$

with the property that $\cup_{i=1}^{n} S(m_i,a_i) = \mathbf{Z}$. Such a system is composite and incongruent if the moduli $\{m_i : i = 1,\ldots,n\}$ are composite and distinct. We describe the composite incongruent covering systems of minimum cardinality, thus answering a question asked by Gerry Myerson.

1. Introduction

We write $S(m,a)$ for the congruence class $\{n \in \mathbf{Z} : n \equiv a \pmod m\}$. A *covering system of congruences* is a collection

$$\{S(m_1,a_1), S(m_2,a_2), \ldots, S(m_n,a_n)\}, \tag{1}$$

with the property that

$$\cup_{i=1}^{n} S(m_i,a_i) = \mathbf{Z}.$$

Thus, for example, the set $\{S(2,0), S(2,1)\}$ is a covering system. The set of integers $\{m_1, m_2, \ldots m_t\}$ is the *set of moduli* of the system. Strictly this is a multiset, since the moduli may be repeated but it will be convenient to occasionally abuse notation in this

way. Covering systems were introduced by Erdös in 1952 [3] and were the subject of some of his favorite problems. They have generated a large literature and there are a number of celebrated open questions concerning them. See the surveys [5] and [6]. We say the covering system (1) is *irredundant* if it has no proper subcollection which is a covering system. A covering system is *incongruent* if all its moduli are distinct, and *composite* if each modulus is composite. An example of an incongruent covering system is

$$\{S(2,0), S(3,0), S(4,1), S(6,1), S(12,11)\}.$$

The main concern of this paper is with systems that are both composite and incongruent, which henceforth we will call CICSs. Examples of these will be given later.

In 1996 Cochrane and Myerson [2] introduced a new type of system called a homogeneous covering system. To describe this we write $H(m,a,b)$ for the set

$$\{(x,y) \in \mathbf{Z}^2 : ax + by \equiv 0 \pmod{m}\}.$$

A *homogeneous covering system* is a collection $\{H(m_i,a_i,b_i) : i = 1 \ldots n\}$ with $m_1 < m_2 < \ldots < m_n$ which has the property that

$$\cup_{i=1}^{n} H(m_i,a_i,b_i) = \mathbf{Z}^2.$$

They showed how such a system could be constructed from a CICS. Later Boping Jin and Myerson [1] showed that *every* homogeneous cover of $\mathbf{Z}^2$ can be obtained from a CICS using the construction of [2].

The archetypal example of a homogeneous covering system is constructed using a CICS devised by John Selfridge which contains 20 moduli. This is shown in Table 1. At a meeting of the Australian Mathematical Society Gerry Myerson asked whether any CICS exists with fewer than 20 moduli. This question was repeated in [6] and [8]. In this paper we will answer Gerry's question in the negative, and also show that besides Selfridge's example there are five other sets of 20 moduli which can be used to construct a CICS.

The structure of the paper is as follows. We say that a set of integers that can be the set of moduli of a covering system is *good*. In Section 2 we describe how any good set can be reduced to a canonical good set. We then use known results about covering systems to show that if a CICS has the minimum cardinality then its moduli set can be reduced to one of a finite (but large) collection of candidate sets.

In Section 3 we present an algorithm for testing whether or not a set of integers is good. In the final section we present the results of applying the algorithm to the collection of candidate sets.

2. Finding candidate sets

Lemma 1 *If $\{m_1, m_2, \ldots, m_n\}$ is a good set and $\mu > 1$ divides m_i for some $1 \leq i \leq n$, then $\{m_1, m_2, \ldots, m_n, \mu\} \backslash \{m_i\}$ is also good.*

Proof. Since $\{m_1, m_2, \ldots, m_n\}$ is good there exists a covering system

$$\{S(m_1, a_1), S(m_2, a_2), \ldots, S(m_n, a_n)\}.$$

But $S(\mu, a_i) \supseteq S(m_i, a_i)$ so we get another covering system by replacing $S(m_i, a_i)$ with $S(\mu, a_i)$. □

We will write LCM for lowest common multiple throughout this paper.

Lemma 2 *Let $\{m_1, m_2, \ldots, m_n\}$ be a good set and suppose that the primes dividing the LCM of $m_1, m_2, \ldots, m_n$ are $q_1 < q_2 < \ldots < q_t$. For $i = 1, \ldots, n$ let*

$$m_i = \Pi_{j=1}^{t} q_j^{\alpha_{ij}}.$$

Then, writing $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$ we get that

$$\{\Pi_{j=1}^{t} p_j^{\alpha_{ij}} : i = 1, \ldots, n\}.$$

is also good.

We omit the proof which is essentially the same as that of the first theorem of [10] and its corollary.

These lemmas allow us to form a canonical CICS from any CICS by replacing the prime factors of its moduli with the lowest primes, and replacing moduli by composite divisors wherever possible. Thus a canonical CICS has the properties:

(a) If, for $i \geq 2$, p_i divides a modulus of the CICS then p_{i-1} divides some modulus.

(b) Any composite divisor of a modulus is also a modulus.

Recall that a covering system is *irredundant* if it ceases to be a covering system when one of its members is removed. We are seeking a CICS of minimum cardinality, which must necessarily be irredundant. The following theorem is from [7].

Theorem 3 *If the LCM of the moduli of an irredundant covering system has prime factorization $\Pi_{i=1}^{t} p_i^{\alpha_i}$ then*

$$n \geq \sum_{i=1}^{t} \alpha_i (p_i - 1) + 1, \tag{2}$$

where n is the cardinality of the covering system.

From this we obtain the following.

Corollary 4 *The LCM of the moduli of a canonical CICS of minimum cardinality has the form*

$$L = 2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}7^{\alpha_4} \tag{3}$$

where

$$\alpha_1 + 2\alpha_2 + 4\alpha_3 + 6\alpha_4 \leq 19. \tag{4}$$

Proof. Suppose that (3) does not hold, so that the LCM of the moduli is divisible by a prime greater than or equal to 11. By property (a) of a canonical CICS the LCM is also divisible by 2, 3, 5, and 7, so by the Theorem its cardinality is at least $\sum_{i=1}^{5}(p_i-1)+1 = 24$. However Selfridge's CICS contains only 20 congruences, so we have a contradiction and (3) follows. Substituting into (2) yields (4). □

Corollary 4 and property (a) of a canonical CICS allow us to construct a finite population of candidates for the LCM of a canonical CICS of minimum cardinality. We simply consider all sets of non-negative integers $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ which satisfy (4) and reject those for which one member of the set equals zero while another with higher subscript is positive. This leaves 204 candidates for the LCM. This set of candidates is reduced further with the following theorem (which will be used again later).

Theorem 5 *If* $\{m_1, m_2, \ldots, m_n\}$ *is a good set then*

$$\sum_{i=1}^{n} 1/m_i \geq 1.$$

This result is well-known (see, eg, [5] or [6]) and easily proved using density arguments. From it we get the following.

Corollary 6 *If L is the LCM of the moduli of a CICS of minimum cardinality then the sum of the reciprocals of the 20 smallest composite divisors of L is at least 1.*

Using this we reject 86 of our 204 candidates, leaving 118. Having found a candidate for the LCM of the moduli of a minimum cardinality canonical CICS we need to determine the sets of moduli which have this LCM and satisfy requirement (b) of a CICS. This gives us 77,196 sets of integers.

3. An Algorithm for Recognising the Set of Moduli of a Covering System

In this section we consider the following decision problem.

Covering System

Instance: A multiset of integers $\{m_1, m_2, \ldots, m_n\}$.

Question: Do there exist integers $a_1, a_2, \ldots, a_n$ such that

$$\{S(m_1, a_1), S(m_2, a_2), \ldots, S(m_n, a_n)\}$$

is a covering system?

We will call a Yes-instance of this question *good* and a No-instance *bad.* Covering System appears to be a difficult problem. The following, apparently easier, problem is known to be NP-complete [4],[11].

Simultaneous Incongruences

Instance: Collection $\{(m_1, a_1), (m_2, a_2), \ldots, (m_n, a_n)\}$ of ordered pairs of positive integers.

Question: Is there an integer x such that, for $1 \leq i \leq n$, there is no i for which $x \equiv a_i \pmod{m_i}$.

Note that the question is equivalent to asking whether

$$\{S(m_1, a_1), S(m_2, a_2), \ldots, S(m_n, a_n)\}$$

is *not* a covering system: one can demonstrate this by finding a single integer not contained in any of the congruence classes.

We present an algorithm for answering the first of these questions. Unfortunately this algorithm cannot give a positive answer to Covering System : its output is either "No" or "Don't know". An earlier version of the algorithm was given in [9]. Before presenting it we give some technical results.

Let $M = \{m_1, m_2, \ldots, m_n\}$. We say that m_i is *helpful* in M if $M \backslash \{m_i\}$ is bad but M is good. Similarly we say that m_i is *unhelpful* in M if either $M \backslash \{m_i\}$ is good (in which case M is also good) or M is bad (in which case $M \backslash \{m_i\}$ is also bad). That is, m_i is unhelpful if removing m_i from M does not change M from good to bad.

Let p be a prime and p^α be the greatest power of p dividing any member of M. We partition M as

$$M = M_0 \cup M_1 \cup \ldots \cup M_\alpha,$$

where $m \in M_j$ if and only if p^j is the greatest power of p dividing m.

Lemma 7 *Let $M = \{m_1, \ldots, m_n\}$. Using the notation of the previous paragraph, if there exists j, $0 < j \leq \alpha$, such that*

$$p^{\alpha-j}|M_j| + p^{\alpha-j-1}|M_{j+1}| + ... + |M_\alpha| < p^{\alpha-j+1} \tag{5}$$

then each member of $\cup_{i=j}^{\alpha} M_i$ is unhelpful.

Proof. If no covering system exists with set of moduli M then all integers in M are unhelpful and we are done. So we assume that M is good and let A be a covering system with set of moduli M . We partition A into $A_0 \cup A_1 \cup ... \cup A_\alpha$ where $S(m, a)$ belongs to A_i if and only if m belongs to M_i.

We now prove the contrapositive of the Lemma. That is, we'll choose an arbitrary j from $\{1, ..., \alpha\}$ and assume that some element of some M_i, $i \geq j$, is helpful and show that (5) does not hold.

We see from this assumption that $A_0 \cup A_1 \cup ... \cup A_{j-1}$is not a covering system. So there exists an integer, say x, that does not belong to any congruence class in this collection. Set $p^\alpha L$ to be the LCM of the members of M and obtain integers x_k, $k = 1, 2, ..., p^{\alpha-j+1}$ satisfying

$$\begin{aligned} x_k &\equiv x \pmod{L} \\ x_k &\equiv x + kp^{j-1} \pmod{p^\alpha}. \end{aligned} \tag{6}$$

Each of these integers must belong to a congruence class in A. We'll show first that none can belong to a class in $A_0 \cup A_1 \cup ... \cup A_{j-1}$, then that this implies that (5) does not hold.

Suppose $x_k \in S(mp^i, a)$ for some $i \in \{1, 2, \ldots, \alpha\}$ where $S(mp^i, a) \in A_i$ (so that p does not divide m). Then

$$x_k \equiv a \pmod{mp^i} \tag{7}$$

which implies $x_k \equiv a \pmod{m}$. From this and (6) we have

$$x \equiv a \pmod{m}.$$

¿From (7) we also have $x_k \equiv a \pmod{p^i}$, which by (6) implies

$$x + kp^{j-1} \equiv a \pmod{p^i}.$$

If $i < j$ then the last two displays imply that $x \equiv a \pmod{mp^i}$, that is, $x \in S(mp^i, a)$ contradicting the way x was chosen. Thus $i \geq j$, and

$$\{x_k : k = 1, 2, ..., p^{\alpha-j+1}\} \subseteq \cup_{i=j}^{\alpha} A_i. \tag{8}$$

We now show that if $S(mp^i, a) \in A_i$ then

$$|\{x_k : k = 1, 2, ..., p^{\alpha-j+1}\} \cap S(mp^i, a)| \leq p^{\alpha-i}|M_i|.$$

This follows on noting that

$$\begin{aligned} S(mp^i, a) &= S(m, a) \cap S(p^i, a) \\ &= S(m, a) \cap \{\cup_{k=1}^{p^{\alpha-i}} S(p^\alpha, a + kp^i)\}. \end{aligned}$$

Since the x_k's belong to different congruence classes modulo p^α, each $S(p^\alpha, a + kp^i)$ contains only one. Thus $S(mp^i, a)$ contains at most $p^{\alpha-i}$ of them. This applies to each congruence class in A_i so the number of the x_k covered by congruence classes in A_i is at most

$$p^{\alpha-i}|A_i| = p^{\alpha-i}|M_i|. \tag{9}$$

So the number in all congruence classes in $\cup_{i=j}^{\alpha} A_i$ is at most

$$p^{\alpha-j}|M_j| + ... + |M_\alpha|.$$

This with (8) implies

$$p^{\alpha-j}|M_j| + ... + |M_\alpha| \geq p^{\alpha-j+1}$$

which is the negation of (5) thus proving the contrapositive of the Lemma, and hence the Lemma. □

In the algorithm presented in Section 3 we'll use this lemma to remove unhelpful members of the set of integers which we are testing for goodness. The next lemma allows us to apply a recurrence in our algorithm: we show that M is good if and only if each set in a collection of smaller sets is good.

Theorem 8 *Let p be a prime and let M be a good set of moduli. Write $M = M_0 \cup M_1$ where the members of M_1 are divisible by p and those of M_0 are not. Then there exists a partition of M_1,*

$$M_1 = D_1 \cup D_2 \cup ... \cup D_p$$

such that $M_0 \cup \{d/p : d \in D_i\}$ is good for each choice of $i \in \{1, 2, \ldots, p\}$.

Proof. Since M is good there exists a covering system A with set of moduli M. Choose $i \in [1, p]$ and set

$$\begin{aligned} A_i &= \{S(m, a) \in A : S(m, a) \cap S(p, i) \neq \emptyset\} \\ D_i &= \{m : S(m, a) \in A_i, m \in M_1\}. \end{aligned}$$

It is shown in [7] that a covering system can be constructed using the set of moduli $M^* = \{m/\gcd(m, p) : S(m, a) \in A_i\}$. Thus M^* is good. Note that whenever $(m, p) = 1$

we have $S(m,a) \cap S(p,i) \neq \emptyset$ (by the Chinese Remainder Theorem) so $M_0 \subseteq M^*$. The other members of M^* have the form d/p where $d \in D_i$, thus $M_0 \cup \{d/p : d \in D_i\}$ is good.

It remains to show that the sets D_i are disjoint. This is obvious when we note that $S(mp,a) \cap S(p,i) \neq \emptyset$ implies $S(mp,a) \subseteq S(p,i)$ for any m, p, a and i, so each member of M_1 appears as a modulus of a congruence in exactly one of the collections A_i. □

In the application we use the contrapositive of this theorem, which we give as a corollary.

Corollary 9 *We use the notation of the theorem. If for some prime p there doesnot exist a partition for which $M_0 \cup \{d/p : d \in D_i\}$ is good for each choice of $i \in \{1, 2, \ldots, p\}$ then M is not good.*

This result allows us to test M for goodness by testing the sets $M_0 \cup \{d/p : d \in D_i\}$ for goodness which can in turn be checked recursively. Since all partitions of M_1 must be considered this leads to a combinatorial explosion, however one hopes that many of the candidate sets may be eliminated quickly using Lemmas 1 and 2. The process will terminate since with each iteration the lowest common multiple of the moduli is decreasing. Indeed, once all the moduli are powers of the same prime we can end the process using the next lemma.

Lemma 10 *If p is a prime and $M = \{m_1, \ldots, m_t\}$ is a set of (not necessarily distinct) powers of p then M is good if and only if*

$$\sum_{i=1}^{t} 1/m_i \geq 1. \tag{10}$$

Proof. Let M be ordered such that $m_1 \geq m_2 \geq ... \geq m_t$. Note that if $\alpha \geq \beta$ then the congruence classes $S(p^\alpha, a)$ and $S(p^\beta, b)$ are either disjoint or $S(p^\alpha, a) \supseteq S(p^\beta, b)$.

If (10) holds a covering system $\{S(m_1, a_1), S(m_2, a_2), ...S(m_t, a_t)\}$ can be constructed as follows. Set $a_1 = 0$, then for $j = 2$ to t set a_j to be the least positive integer not included in any of $S(m_1, a_1), S(m_2, a_2), ...S(m_{j-1}, a_{j-1})$. If there is no such integer we already have a covering system and M is good. Otherwise $S(m_j, a_j)$ will be disjoint from the other congruence classes. The proportion of integers in $\{1, \ldots, M\}$ covered by the system is $\sum_{i=1}^{j} 1/m_i$. Since (10) holds this will reach 1 for some $j \leq t$, and so M is good.

If (10) does not hold then M is bad by Lemma 1. □

Combining these results we construct an algorithm for testing a set of integers for goodness.

Algorithm Moduli

input M:={m(1),m(2),...m(t)};

{Apply Theorem 5}

If 1/m(1)+1/m(2)+...+1/m(t) < 1 **then output** "No", **stop**;
compute L:= lcm{m(1),...m(t)};
compute prime factorisation of L:=p(1)^a(1)*p(2)^a(2)*...*p(s)^a(s);

{Apply Lemma 10}

if s==1 **then output** "Don't know", **stop**;

{Apply Lemma 7}

for i=1 to s
sum:=0;
for j = a(i) to 1 step −1
compute sum:=sum + p(i)^(a(i)−j)|{$m \in$ M : p(i) ^ j | m, p(i)^(j+1) $\not|$ m}|
if sum < p(i)^(a - j + 1) **then call** Moduli(M \{$m \in$ M : p(i)^j | m}), **stop**;
end;
end;

{Apply Corollary 9}

for i:= 1 to s;
M0:= {m ∈ M : p(i) $\not|$ m}
M1:= {m ∈ M : p(i) | m}
Good_Partition_Found:=false;
for each p(i)-partition M1:= D(1) ∪ D(2) ∪ ...∪ D(p(i)) of M1
if Moduli(M0 ∪ {d/p(i) : d ∈ D(k)}) == "Don't know" for all k ∈ {1,...p(i)}
then Good_Partition_Found:=true;
end;
if Good_Partition_Found==false **then output** "No", **stop**;
end;
output "Don't know";
end;

The correctness of the algorithm follows easily from the lemmas.

4. Results

The algorithm from the last section was applied to each of the 77,196 candidate sets obtained in Section 2. It returned "No" for all but 6. These were investigated by hand and it was found in each case that it was possible to find residues a_i which produced covering systems. The sets of moduli and residues are shown in the following table.

I Selfridge's CICS has lowest common multiple 720

m_i	4	8	16	6	12	24	48	9	18	36	72	144	10	20	15	30	60	45	90	180
a_i	0	2	6	1	5	14	46	0	15	21	30	78	3	15	11	17	59	39	21	147

II has lowest common multiple 1440

m_i	4	8	16	32	6	12	24	48	96	9	18	36	72	144	288	10	20	15	30	60
a_i	0	2	6	14	1	5	21	14	94	0	15	3	57	30	222	3	15	11	17	59

III has lowest common multiple 1440

m_i	4	8	16	32	6	12	24	48	96	9	18	36	10	20	15	30	60	45	90	180
a_i	0	2	6	30	1	5	14	46	78	0	15	21	3	15	11	17	59	39	21	147

IV has lowest common multiple 2880

m_i	4	8	16	32	64	6	12	24	48	96	192	9	18	36	72	10	20	15	30	60
a_i	0	2	6	14	62	1	5	21	30	94	158	0	15	3	57	3	15	11	17	59

V has lowest common multiple 2160

m_i	4	8	16	6	12	24	48	9	18	36	72	144	27	54	108	10	20	15	30	60
a_i	0	2	6	1	5	14	46	0	15	3	30	78	21	3	93	3	15	11	17	59

VI has lowest common multiple 4320

m_i	4	8	16	32	6	12	24	48	96	9	18	36	27	54	108	10	20	15	30	60
a_i	0	2	6	30	1	5	14	46	78	0	15	3	21	3	93	3	15	11	17	59

Table 1: Six composite irredundant covering systems of cardinality 20, $\{S(m_i, a_i) : i = 1, \ldots, 20\}$. These have the only possible sets of moduli, but for each set of moduli there are many other possible sets of residues. The first system was discovered by John Selfridge, the others are original to this paper.

Our argument shows these are the only canonical CICS with 20 moduli. Suppose such a CICS exists which is not canonical, that is, one which does not satisfy both conditions (a) and (b). Then we'd be able to obtain a non-canonical CICS by taking one of the sets of moduli from the table and either (a) replacing the largest prime divisor of its LCM with the next largest prime from the set $\{2, 3, 5, 7\}$ or (b) replacing one of the moduli with a proper multiple of itself. For (b) we need only consider multiples formed by multiplying moduli by 2, 3, 5 or 7.

These possibilities were tested on the 6 sets and no other covering systems were found.

Finally we need to consider the possibility that there exists a CICS with less than 20 moduli. Such a CICS could be transformed into covering system with 20 moduli by adding one or more extra congruences. This new covering system would produce "Don't know" as output from the algorithm and so would have been found. Note that such a

covering system would not be irredundant, but the only place we used irredundancy was in Theorem 3 and Corollary 4. Inequality (4) would still apply in this case since we could remove the redundant congruences from the covering system to form a CICS and apply Theorem 3 to this.

We conclude that no composite incongruent covering systems exist with fewer than 20 moduli, and that the only such covering systems with 20 moduli use one of the sets in Table 1.

References

[1] Boping Jin and Myerson, G., Homogeneous Covering Congruences and Subgroup Covers, preprint.

[2] Cochrane, T. and Myerson, G., Covering congruences in higher dimensions, Rocky Mountain J. Math. 26(1996), 77-81.

[3] Erdös, P., On a problem concerning systems of congruences, Mat. Lapok 3(1952), 122-128.

[4] Garey, M.R., and Johnson, D.S., Computers and Intractability : A Guide to the Theory of NP-completeness, San Francisco, CA, Freeman (1979).

[5] Guy, R., Unsolved problems in Number Theory, 2nd edition, New York, Springer-Verlag (1994).

[6] Porubský, Š. and Schönheim, J., Covering Systems of Paul Erdős Past, Present and Future, Bolyai Soc. Math. Studies 11, Paul Erdős and his Mathematics, I, Budapest 2002, 581-627.

[7] Simpson, R.J., Regular coverings of the integers by arithmetic progressions, Acta Arith. 45(1985), 145-152.

[8] Simpson, R.J., Covering systems of homogeneous congruences, Rocky Mountain J. Math., 28(1998), 1125-1133.

[9] Simpson, R.J., Recognising the set of moduli of a covering system, in Proc. 9th Australasian Workshop on Combinatorial Algorithms, (1998), Curtin University of Technology, Australia, C.S. Iliopoulos (ed), 117-123.

[10] Simpson, R.J. and Zeilberger, D., Necessary conditions for distinct covering systems with square-free moduli, Acta Arith., 59(1991), 59-70.

[11] Stockmeyer, L.J., and Meyer, A.R., Word problems requiring exponential time, Proc. 5th Ann. ACM Symp. on Theory of Computing, Association for Computing Machinery, New York(1973), 1-9.