Constructions for covering arrays

Chris Fisher and Karen Meagher

July 3, 2013

1 Introduction

Let n, r, k, t be positive integers with $t \leq r$. A *covering array* with strength t and alphabet size k is an $r \times n$ array with entries from $\{0, 1, \ldots, k-1\}$ and the property that any $t \times n$ subarray has all k^t possible t-tuples occurring at least once. A covering array with these parameters will be denoted by t-$CA(n, r, k)$. The number of columns in a covering array is called the *size* of the array. For most constructions the goal is to construct a covering array with few columns. We define

$$t\text{-}CAN(r, k) = \min\{n : \text{a } t\text{-}CA(n, r, k) \text{ exists}\}.$$

2 The First Construction

In [1] a construction for a 3-$CA((2q+1)(q^3-q)+(q+1),\ 2(q+1),\ q+1)$, where q is a prime power, is given. This construction uses a matrix, called the *starter matrix* and the group $PGL(2, q)$. The group $PGL(2, q)$ acts on $\mathbb{F}_q \cup \{\infty\}$, in this note we will denote the set $\mathbb{F}_q \cup \{\infty\}$ by $\{0, 1, \ldots, q\}$. The entries of the starter array are from the set $\{0, 1, \ldots, q\}$ and thus the elements of the group $PGL(2, q)$ act on the starter matrix.

The construction in [1] starts with a $(2q+2) \times (2q+1)$ starter matrix, which we will call M, with the entries from $0, 1, \ldots, q$. Then $q^3 - q$ matrices are constructed by having the elements from $PGL(2, q)$ act on the entries of M. These matrices are concatenated to form a $2(q+1) \times (2q+1)(q^3-q)$ matrix. This is called *developping* the matrix M. Finally this developped matrix is concatenated with a $2(q+1) \times (q+1)$ matrix to form a covering array.

To see how this construction forms a covering array, consider the orbits of $PGL(2,q)$ on the triples from $\{0,1,\ldots,q\}$. These orbits are:

1. Orbit 1: (x,y,z) where x,y,z are all distinct,
2. Orbit 2: (x,x,y) where x and y are distinct,
3. Orbit 3: (x,y,x) where x and y are distinct,
4. Orbit 4: (y,x,x) where x and y are distinct,
5. Orbit 5: (x,x,x).

The matrix M is selected so that for any triple of rows from M, there is at least one representative from each orbit, except the last orbit. Then developping the matrix M will produce a matrix in which for every three rows, every triple from $0,1,\ldots,q$ occurs in at least one column, except for the triples of the form (x,x,x). Finally adding a $2(q+1)\times(q+1)$-matrix in which the i-th column has all entires equal to $i-1$ produces a covering array.

To construct M consider a one factorization of the complete graph $K_{2(q+1)}$. For each one-factor in the factorization label the edges by the integers $0,1,\ldots,q$. Then construct a vector of length $2(q+1)$, with the entries indexed by the vertices in $K_{2(q+1)}$, and set the i-th entry to be the label of the edge in the one-factor that is adjacent to the i-th vertex. This is the characteristic vector of the one-factor. Set the columns of M to be the characteristic vectors of the one-factors in the one-factorization. The matrix M is the characteristic matrix of the one-factorization

In [1] it is shown that for any three rows of M there is exactly one column that contains a representative from each of orbit 2, orbit 3 and orbit 4. Thus there are $2q-4$ columns with representatives from oribt 1. This is enough to claim that this construction produces a covering array.

In this note, we construct a smaller covering array using this method with the group $PSL(2,q)$, rather than $PGL(2,q)$, and with a slightly different starter matrix.

The group $PSL(2,q)$ has two orbits over the distinct triples from $\{0,1,\ldots,q\}$. If (x,y,z) is in one of the orbits of $PSL(2,q)$ and a is not a square element of $\mathbb{F}_q$ then (ax,ay,az) is in the other oribt of the action of $PSL(2,q)$.

To construct the starter matrix for $PSL(2,q)$, take the first four columns of M (or any four columns of M) and multiply each entry in these columns by a non-square element from $\mathbb{F}_q$. Let M' be the matrix formed by concatenating these four new columns with M (the characteristic matrix of the one-factorization). We claim that for any three rows of M' there is a columns that contains at least one representative from each of the orbits of $PSL(2, q)$ acting on triples from $\mathbb{F}_q$ (except the orbit (x, x, x)). To show this, we only need to show that there is a representative of each of the two obrbits on triples with distinct entries between any three rows. This holds since for these three rows in the first four columns of M there must be at least one triple of the form (x, y, z) in which all the entries are distinct. Thus there is column in M' with the values (ax, ay, az) in these three rows. Thus there is a representative from each of the orbits of $PSL(2, q)$ acting on the distinct triples of $\{0, 1, \ldots, q\}$.

Lemma 1. *For q a prime power*

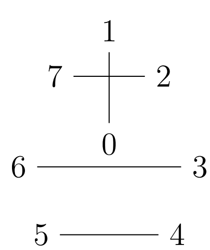
$$3\text{-}CAN(2(q+1), q+1)) \leq (2q+5)\frac{(q^3-q)}{2} + (q+1).$$

3 A Second Construction

The question we ask next, is for $q > 3$ does the matrix M contain a representative of every orbit from $PSL(2, q)$ acting on the distinct triples of $\{0, 1, \ldots, q\}$?

To start we will pick a specific one-factorization of the $K_{2(q+1)}$. We will describe how to build the first one factor in this one-factorization. Place the numbers $1, \ldots 2(q+1)$ in a circle and place the number 0 in the centre of the circle; these are the vertices of $K_{2(q+1)}$. The first one-factor includes the edge between 0 and 1, and the edges between the vertices $(i, 2(q+1)+1-i)$ for $i = 2, \ldots q+1$. To build the other one-factors in the one-factorization take this one-factor and rotate the edges while leaving the vertices in place.

The figure below gives the first one-factor.



Let M_q be the characteristic matrix for this one-factorization for q a prime power.

Lemma 2. *If for any triple of the form $(1, r, s)$ the rows 1, r, s of M_q contains representatives from all possible orbits, then M_q is a starter matrix.*

Lemma 3. *If $q \equiv 3$
pmod4 then any triple of rows that includes the final row of M_q will contain representatives from all orbits. Conversely, if $q \equiv 1 \pmod 4$ then any triple of rows that includes the final row will never contain representatives from both orbits of distinct triples.*

If $q \equiv 1 \pmod 4$ then we will remove the final row from M_q.

Lemma 4. *Let $q \equiv 3 \pmod 4$. Consider the rows $(1, i, j)$ where $q > j > i > 1$. Provided that $(j-1)(i-1)(j-1) \neq 0$ then the rows 1, i, j in M_q contain representatives from both orbits of triples with distinct elements.*

Proof. The entry in the first column of M_q for the rows $1, i, j$ is $(0, i-1, j-1)$. The entry in the j-th columns of M_q for these three rows is $(j-1, j-i, 0)$.

The orbit is determined by whether the value of

$$\theta_{p,q,r} := p^2(q-r) + q^2(r-p) + r^2(p-q).$$

is a square or non-square.

Since

$$\theta_{0,i-1,j-1} = (j-1)(i-1)(i-j) = -((i-1)(j-1)(j-i)) = -(\theta_{j-1,j-i,0})$$

then these triples are in different orbits, provided that $(j-1)(i-1)(j-1) \neq 0$. □

References

[1] M. A. Chateauneuf, C. J. Colbourn, and D. L. Kreher. Covering arrays of strength three. *Des. Codes Cryptogr.*, 16(3):235–242, 1999.