On the state of strength-three covering arrays

M. Chateauneuf
Center for Applied Cryptographic Research
University of Waterloo
Waterloo Ontario N2L 3G1
mchateau@cacr.math.uwaterloo.ca

D.L. Kreher
Department of Mathematical Sciences
Michigan Technological University
Houghton MI 49931 1295
kreher@mtu.edu

ABSTRACT

A *covering array* of *size* N, *strength* t, *degree* k, and *order* v is a $k \times N$ array on v symbols in which every $t \times N$ subarray contains every possible $t \times 1$ column at least once. We present explicit constructions, constructive upper bounds on the size of various covering arrays, and compare our results with those of a commercial product. Applications of covering arrays include software testing, drug screening, and data compression.

1. INTRODUCTION

This article focuses on constructing new covering arrays with strength $t = 3$, and establishing new bounds on the covering array numbers $\mathsf{CAN}(3, k, v)$. A *covering array*, $\mathsf{CA}(N; t, k, v)$, of *size* N, *strength* t, *degree* k, and *order* v, is a $k \times N$ array on v symbols such that every $t \times N$ subarray contains every $t \times 1$ column on v symbols **at least** once. A covering array is optimal if it has the smallest possible number N of columns. This number is the *covering array number*,

$$\mathsf{CAN}(t, k, v) = \min\{N : \exists \mathsf{CA}(N; t, k, v)\}.$$

Submitted to the Journal of Combinatorial Designs on Novebe r 30, 2000

In Figure 1 we display a $\mathsf{CA}(10;3,5,2)$. An example application of covering arrays appeared in the IEEE article [11] from research done at Bellcore™. It involved the employment of a covering array for testing a telephone switch system. Figure 2 displays four parameters and the possible values for each parameter. An assignment of each value to a symbol from the set $\{0,1\}$ has been made. Each test run of the switch system is a setting of the parameter values. Thus a test run may be represented as a vector in $\{0,1\}^4$. If 3-way coverage of the parameter value combinations is desired, then a covering array, $\mathsf{CA}(N;3,4,2)$, can be used by associating each column of the array with a setting of the parameter values. Thus each of the N columns represents a test run, and all possible combinations of any 3 parameter values are tested. The problem is to minimize N, reducing the testing cost.

$$\begin{array}{|cccccccccc|}\hline 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \hline \end{array}$$

FIG. 1. $\mathsf{CA}(10;3,5,2)$

parameters(k)	values(v)
Call Type	Local(0) Long Distance(1)

Billing	Caller(0)
	Collect(1)

Access	Loop(0)
	ISDN(1)

Status	Success(0)
	Busy(1)

FIG. 2. Four discrete parameters, each with 2 possible values.

There are 8 binary 3-vectors and 16 binary 4-vectors. If the test-set consists of all these 4-vectors, then certainly all 3-way combinations will be tested. Therefore, we know $8 \leq N \leq 16$. Fortunately, there is a collection of 8 tests which provides the desired 3-way coverage, see Figure 3. Since $N = v^t$ in this case, the array is an *orthogonal array*, see Section 2.

Other applications related to covering arrays include: authentication [29], block ciphers [20], data compression [26], intersecting codes [14], oblivious transfer [6]. pseudorandomness [21], resilient functions [2], span programs [16], universal hashing [7], and zero-knowledge [5],

Call Type	0	0	0	0	1	1	1	1
Billing	0	0	1	1	0	0	1	1
Access	0	1	0	1	0	1	0	1
Status	0	1	1	0	1	0	0	1

FIG. 3. Eight tests provide three-way coverage of four binary parameters.

2. BACKGROUND RESULTS

In this section, we present basic and previously established results which we cite in the tables of Section 6. Let A be a $\mathsf{CA}(N;t,k,v)$ with entries $a_{ij} \in V = \{0,\dots,v{-}1\}$.

Row-collapsing. If any row from A is deleted we obtain a $\mathsf{CA}(N;t,k-1,v)$. So

$$\mathsf{CAN}(t,k-1,v) \leq \mathsf{CAN}(t,k,v).$$

Symbol-collapsing. If each occurrence of the symbol x in the array A is replaced with a fixed different symbol in $V\backslash\{x\}$, then a $\mathsf{CA}(N;t,k,v-1)$ is formed. Thus

$$\mathsf{CAN}(t,k,v-1) \leq \mathsf{CAN}(t,k,v).$$

Derived array bound. Every $x \in V$ appears $M \geq v^{t-1}$ times in row i of A. The $(k-1) \times M$ array obtained by deleting row i of A and retaining only the columns with an x on row i forms a $\mathsf{CA}(M;t-1,k-1,v)$. Therefore,

$$\mathsf{CAN}(t,k,v) \geq v \cdot \mathsf{CAN}(t-1,k-1,v).$$

It was established by Stevens, Moura, and Mendelsohn [27] that

$$\mathsf{CAN}(2,k,v) \geq v^2 + 3$$

when $3 \leq v \leq k-3$. Therefore we have the nontrivial lower bound,

$$v(v^2+3) \leq \mathsf{CAN}(3,k,v),$$

when $3 \leq v \leq k-3$.

Product. Let B be a $\mathsf{CA}(M;t,k,w)$ with entries $b_{ij} \in W = \{0,\dots,w-1\}$. Form the $k \times N$ array C_ℓ with entries $(a_{ij}, b_{i\ell}) \in V \times W$ for all $i = 1,\dots,k$ and $j = 1,\dots,N$. Then $[\mathsf{C}_1,\dots,\mathsf{C}_M]$ is a $\mathsf{CA}(NM;t,k,vw)$ on symbol set $V \times W$. Therefore,

$$\mathsf{CAN}(t,k,vw) \leq \mathsf{CAN}(t,k,v)\mathsf{CAN}(t,k,w).$$

Construction D. Construct C in three parts as follows:

$$\begin{array}{|c|ccccc|ccccc|}
\multicolumn{1}{c}{\text{I}} & \multicolumn{5}{c}{\text{II}} & \multicolumn{5}{c}{\text{III}}\\
\hline
 & \vec{0} & \mathsf{B}_1 & \mathsf{B}_1 & & \mathsf{B}_1 & \vec{V'} & \vec{0} & \vec{0} & & \vec{0}\\
 & \mathsf{B}_1 & \vec{0} & \mathsf{B}_2 & & \mathsf{B}_2 & \vec{0} & \vec{V'} & \vec{0} & & \vec{0}\\
 & \mathsf{B}_2 & \mathsf{B}_2 & \vec{0} & & \mathsf{B}_3 & \vec{0} & \vec{0} & \vec{V'} & & \vec{0}\\
\mathsf{CA}(N;3,k,v-1) & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\
 & \mathsf{B}_{k-2} & \mathsf{B}_{k-2} & \mathsf{B}_{k-2} & & \mathsf{B}_{k-1} & \vec{0} & \vec{0} & \vec{0} & & \vec{0}\\
 & \mathsf{B}_{k-1} & \mathsf{B}_{k-1} & \mathsf{B}_{k-1} & & \vec{0} & \vec{0} & \vec{0} & \vec{0} & & \vec{V'}\\
\hline
\end{array}$$

In part I the symbol set is $V' = \{1, \ldots, v-1\}$, in part II, B_i is row i of a $\mathsf{CA}(M; 2, k-1, v-1)$ on symbol set V' and $\vec{0} = [0, 0, \ldots, 0]$, and in part III, $\vec{V'} = [1, 2, \ldots, v-1]$. We claim that C is a $\mathsf{CA}(N + kM + k(v-1); 3, k, v)$ on symbol set $V = V' \cup \{0\}$. Choose any 3 rows and consider the patterns of 3-tuples:

$$\begin{array}{ccccc}
x & x & x & y & x\\
x & x & y & x & y\\
x & y & x & x & z
\end{array}$$

All patterns on V' are covered in part I. All patterns on V can include 0 once, twice or three times. Those including 0 once are covered in part II, and those including 0 twice and three times are covered in part III. Therefore,

$$\mathsf{CAN}(3, k, v) \le \mathsf{CAN}(3, k, v-1) + k \cdot \mathsf{CAN}(2, k-1, v-1) + k(v-1).$$

There are many possible similar constructions which are generally only used to improve bounds in sporadic cases, since in most cases the constructed array is larger than the arrays produced by later constructions. For example, an upper bound on $\mathsf{CAN}(3, 6, 6)$ was 343, obtained from a test set generated by the $\mathsf{AETG}^{\mathsf{SM}}$ system, see Section 5. We used **construction D** to improve this bound to 305. Other reasonable applications of this idea are the cases where v is not a prime power, since the bounds usually come from the next largest prime power, $q \ge v$.

Squaring k. This result of Colbourn, Chateauneuf and Kreher [9] is a generalization of a construction due to Atici, Magliveras, Stinson, and Wei [1]. If $(\binom{t}{2}!, k) = 1$, and there is a $\mathsf{CA}(N; t, k, v)$, then for $j \ge 0$,

$$\mathsf{CAN}(t, k^{2^j}, v) \le N(\binom{t}{2} + 1)^j.$$

2.1 Orthogonal Arrays

An *orthogonal array* of index 1, $\mathsf{OA}(t, k, v)$, is a $k \times v^t$ array with entries from a set of v symbols such that every $t \times v^t$ subarray contains every possible $t \times 1$ column exactly once. Therefore, a $\mathsf{CA}(v^t; t, k, v)$ is an $\mathsf{OA}(t, k, v)$. A well-known family of orthogonal arrays is the sum-zero arrays, $\mathsf{OA}(t, t+1, v)$, obtained by taking all vectors of $\mathbb{Z}_v^{t+1}$ whose components sum to zero, see [18]. Therefore, we have:

Theorem 2.1. *For all t and v, $\mathsf{CAN}(t, t+1, v) = v^t$.*

Another well-known family of orthogonal arrays is due to Bush, Reed, and Solomon, see [18]. For any prime power $q \geq t-1$, there is an $\mathsf{OA}(t, q+1, q)$, and if q is even, then there is an $\mathsf{OA}(3, q+2, q)$. Therefore, we have:

Theorem 2.2. *For any prime power $q \geq t-1$, $\mathsf{CAN}(t, q+1, q) = q^t$, and if q is even, then $\mathsf{CAN}(3, q+2, q) = q^3$.*

The **derived array bound** and type **D** constructions show that strength 2 covering arrays are important to the constructions in this article. A closely related structure is a Latin square. A *Latin square* of *order* v is a $v \times v$ array on v symbols such that each symbol appears exactly once in each row and exactly once in each column. Two Latin squares L_1 and L_2 of order v are *orthogonal* if the set

$$\{(L_1[i,j], L_2[i,j]) : 1 \leq i, j, \leq v\}$$

contains all of the v^2 possible pairs of symbols. A collection of k pairwise orthogonal Latin squares of order v is said to be a set of *k mutually orthogonal Latin squares of order v*, $\mathsf{MOLS}(v)$. Two well-known facts, see [18], are

1. A set of $k-2$ $\mathsf{MOLS}(v)$ is equivalent to an $\mathsf{OA}(2, k, v)$, and
2. There exists a pair of $\mathsf{MOLS}(v)$, for every order v except $v = 2$ and $v = 6$.

Using these two facts, we have

Theorem 2.3. $\mathsf{CAN}(3, 5, 2) = 10$.

Proof. There is no $\mathsf{OA}(2, 4, 2)$, because there is no pair of $\mathsf{MOLS}(2)$. Thus $\mathsf{CAN}(2, 4, 2) \geq 5$. A $\mathsf{CA}(5; 2, 4, 2)$ is given in Figure 4, and so, $\mathsf{CAN}(2, 4, 2) = 5$. Applying the **derived array bound**, we have

$$\mathsf{CAN}(3, 5, 2) \geq 2 \cdot \mathsf{CAN}(2, 4, 2) = 10.$$

In Figure 4 we exhibit a $\mathsf{CA}(10; 3, 5, 2)$ and therefore, $\mathsf{CAN}(3, 5, 2) = 10$. □

$$\boxed{\begin{array}{ccccc} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{array}} \qquad \boxed{\begin{array}{cccccccccc} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{array}}$$

FIG. 4. Optimal covering arrays $\mathsf{CA}(5; 2, 4, 2)$ and $\mathsf{CA}(10; 3, 5, 2)$.

2.2 Bias and perfect hash families

Due to statistical analysis in many applications, constructions of small sample spaces in which chosen random variables are almost independent are of interest. Recent work of Bierbrauer and Schellwat relate this idea of limited-dependence to the notion of limited-bias. Their reason is that bias is easier to work with. The following terminology and notation is taken from their articles [3, 2].

Let A be a $k \times N$, p-ary array for some prime p. A is *t-wise ϵ-dependent* if for every set U of s rows, $s \leq t$, and every $u \in \mathbb{F}_p^s$, $\nu_U(u)$ satisfies

$$\left| \frac{\nu_U(u)}{N} - \frac{1}{p^s} \right| \leq \epsilon,$$

where $\nu_U(u)$ is the number of times u occurs as a column in the $s \times N$ subarray determined by U. For example, an orthogonal array of strength t is t-wise 0-dependent (t-wise independent), and a covering array of strength t has *limited* dependence.

For $v \in \mathbb{F}_p^N$, the *bias* of v is

$$\mathsf{bias}(v) = \frac{1}{N} \left| \sum_{x \in \mathbb{F}_p} \nu_v(x) \zeta^x \right|,$$

where $\nu_v(x)$ is the number of times x appears as an entry in v, and ζ is a primitive complex p^{th} root of unity. Notice that $0 \leq \mathsf{bias}(v) \leq 1$, and $\mathsf{bias}(v) = 1$ if and only if v is a constant vector. The ambiguity due to the choice of ζ when talking about vectors is lost when talking of linear spaces: take the bias of a linear space to be the maximum bias of its nonzero members. For some $0 \leq \epsilon < 1$, A is *ϵ-biased* if every nontrivial linear combination of its rows has bias $\leq \epsilon$, and A is *t-wise ϵ-biased* if every nontrivial linear combination of at most t rows has bias $\leq \epsilon$.

The following relationship, showing that ϵ-biased arrays are ϵ-dependent, is established in [3]. If A is t-wise ϵ-biased for some $\epsilon > 0$, then A is t-wise ϵ'-dependent for some $\epsilon' < \epsilon$. From this relationship we see that a $k \times N$, p-ary array which is t-wise p^{-t}-biased is a covering array, $\mathsf{CA}(N; t, k, p)$.

A general construction, given in [3], involves perfect hash families. A *perfect hash family*, $\mathsf{PHF}(N; t, k, m)$, is a collection of N functions called (k, m)-*hash functions*, $h_j : K \longrightarrow M$, $|K| = k, |M| = m$, such that for each t-subset $X \subset K$, there is a hash function h_j which is injective (*perfect*) on X. A perfect hash family can be depicted as a $k \times N$ array in which the rows are labeled by the elements of K, the columns are labeled by the functions, h_j, and the $[i, j]$-entry is $h_j(i)$.

Theorem 2.4. *If there is a $\mathsf{PHF}(N_1; t, k, m)$ and a $\mathsf{CA}(N_2; t, m, v)$, then there is a $\mathsf{CA}(N_1 N_2; t, k, v)$.*

Proof. Let $h_1, h_2, \ldots, h_{N_1}$ be a $\mathsf{PHF}(N_1; t, k, m)$, where $h_i : K \longrightarrow M$ and $|K| = k$ and $|M| = m$. Let A be a $\mathsf{CA}(N_2; t, m, v)$ and label the rows of A with the elements of M. The j-th column of A determines a function $f_j : M \longrightarrow V$, where V is the v-element set of symbols used in A and $f_j(x) = A[i, j]$ if $x \in M$ labels row i of A. The composition of the functions determines the array. That is we take as column (j_1, j_2) the k-tuple

$$[f_{j_1}(h_{j_2}(x)) : x \in M]^{\mathsf{T}}$$

To see that these $N_1 N_2$ columns form a $\mathsf{CA}(N_1 N_2; t, k, v)$ consider any t-tuple $[m_1, m_2, ... m_t]$ of entries from M. The properties of the perfect hash family ensures that there is a function h_{j_1} for which

$$h_{j_1}(m_1), h_{j_1}(m_2), ..., h_{j_1}(m_t)$$

are all distinct. Now because A is a covering array the t-tuples

$$[f_{j_2}(h_{j_1}(m_1), f_{j_2}(h_{j_1}(m_2), ..., f_{j_2}(h_{j_1}(m_t))]$$

$1 \leq j_2 \leq N_2$ must include all of the the t-tuples. Therefore the N_1N_2 chosen columns form a $\mathsf{CA}(N_1N_2; t, k, v)$ as claimed. □

Two notable bounds obtained from this theorem are:

$$\mathsf{CAN}(3, 27, 9) \leq 2187,$$

using the (optimal) $\mathsf{PHF}(3; 3, r^3, r^2)$ for $r \geq 2$ from [4], and

$$\mathsf{CAN}(3, 32, 8) \leq 1536,$$

using the $\mathsf{PHF}(3; 3, 32, 8)$ from [28].

For many recent results on perfect hash families, see Blackburn [4], Stinson, Wei, and Zhu [28], Atici, Magliveras, Stinson, and Wei [1], and Kurosawa, Johansson, and Stinson [20].

3. COVERING ARRAYS FROM GROUPS

In this section we build on a construction of Chateauneuf, Colbourn, and Kreher [9] that uses 2 and 3 transitive groups. Let M be a $k \times n$ array with entries from a set Ω of $v > 2$ symbols, let $\mathcal{G}$ be a subgroup of $\mathsf{S}ym(\Omega)$, the symmetric group of permutations on the symbols in Ω and let $m = |\mathcal{G}|$. For $g \in \mathcal{G}$, M^g is the $k \times n$ array whose $[i, j]$ entry is $\mathsf{M}[i, j]^g$, the image of $\mathsf{M}[i, j]$ under g. $\mathsf{M}^{\mathcal{G}}$ is the $k \times nm$ array, $[\mathsf{M}^g : g \in \mathcal{G}]$. Let $\mathsf{C} = \mathsf{C}(k, \Omega) = [xJ : x \in \Omega]$ be the $k \times v$ array whose columns are the *all-x* vectors xJ where

$$J = [\underbrace{1, 1, \ldots, 1}_{k \text{ times}}]^T.$$

If M has the property that every $t \times n$ subarray contains at least one representative from each non-constant orbit of $\mathcal{G}$ acting on t-tuples from Ω, $[\mathsf{M}^{\mathcal{G}}, \mathsf{C}]$ is a $\mathsf{CA}(nm + v; t, k, v)$. The array M is called a *starter array* with respect to $\mathcal{G}$, and

The following example illustrates the idea of using starter arrays and groups to construct covering arrays and shows that this construction *can* be optimal.

Example: Let $t = 3, \Omega = \{0, 1, 2\}$, and $\mathcal{G} = \mathcal{S}_\Omega$. The action of $\mathcal{G}$ on 3-tuples from Ω has five orbits:

Orbit No.	0	1	2	3	4
	0 1 2	0 0 1 1 2 2	0 0 1 1 2 2	0 0 1 1 2 2	0 0 1 1 2 2
Orbit	0 1 2	0 0 1 1 2 2	1 2 2 0 0 1	1 2 2 0 0 1	1 2 2 0 0 1
	0 1 2	1 2 2 0 0 1	0 0 1 1 2 2	1 2 2 0 0 1	2 1 0 2 1 0
pattern	$[xxx]^\mathsf{T}$	$[xxy]^\mathsf{T}$	$[xyx]^\mathsf{T}$	$[yxx]^\mathsf{T}$	$[xyz]^\mathsf{T}$

Brief inspection shows the following array, M, is an appropriate starter array to construct $[\mathsf{M}^{\mathcal{G}}, \mathsf{C}]$, a $\mathsf{CA}(27; 3, 4, 3)$. One can easily check that on each set of 3 rows there is a representative from each orbit $1-4$.

$$\mathsf{M} = \begin{array}{|cccc|}\hline 0&0&0&0\\ 0&1&1&1\\ 1&0&1&2\\ 2&1&0&2\\ \hline\end{array}$$

□

A $\mathsf{CA}(27;3,4,3)$ can also be constructed using Theorem 2.1.

Recall that the projective general linear group of dimension 2 may be seen as the "fractional linear group":

$$\mathsf{PGL}(2,q) = \left\{ x \mapsto \frac{ax+b}{cx+d} : a,b,c,d \in \mathbb{F}_q \cup \{\infty\}, ad-bc \neq 0 \right\},$$

in which we define $1/0 = \infty, 1/\infty = 0, 1-\infty = \infty - 1 = \infty$, and $\infty/\infty = 1$. Its action on $\mathbb{F}_q \cup \{\infty\}$ is sharply 3-transitive. Similarly, the affine group of dimension 2 may be seen as the "linear group":

$$\mathsf{AGL}(2,q) = \{x \mapsto ax+b : a,b \in \mathbb{F}_q, a \neq 0\}.$$

Its action on $\mathbb{F}_q$ is sharply 2-transitive.

Notice in the previous example, $\mathcal{G} = \mathsf{S}ym(\{0,1,2\}) \cong \mathsf{PGL}(2,2)$. The idea behind the construction is: if each (non–constant) pattern is found in any three rows of a starter array, then the 3-transitivity of the group action will ensure that all 3-tuples appear when the array is developed.

Theorems 3.1, 3.2, and 3.3 were established in [9], using one-factorizations of $\mathcal{K}_{2v}$ to construct appropriate starter arrays. An illustrative example can be found in [9].

Theorem 3.1. *For a prime power $q \geq v-1 > 1$,*

$$\mathsf{CAN}(3,2v,v) \leq (2v-1)(q^3-q)+v.$$

Theorem 3.2. *For a prime power $q \geq v \in \{3,4\}$,*

$$\mathsf{CAN}(3,2v,v) \leq (2v-1)(q^2-q)+v.$$

Theorem 3.3. $\mathsf{CAN}(3,6,3) = 33.$

Theorem 3.4 extends Theorem 3.2 to include the case $v=5$.

Theorem 3.4. $\mathsf{CAN}(3,10,5) \leq 185.$

Proof. There are 396 nonisomorphic one-factorizations of $\mathcal{K}_{10}$, see Section VI.4.4, Table 4.22, of [15]. Only one of these, found by Kreher and Radzisowski (unpublished) using a clever search, admits an appropriate starter array, see Figure 5. The desired covering array is $[\mathsf{M}^{\mathsf{AGL}(2,5)}, \mathsf{C}]$. □

The starter array in Figure 5 has an interesting symmetry which was studied with the hope of finding a clever search method for larger cases. Because $\mathcal{K}_{12}$ has

0	0	0	0	0	0	0	0	0
0	1	1	1	1	1	1	1	1
1	1	0	2	4	2	3	3	4
1	0	1	4	2	3	2	4	3
2	4	3	1	0	2	4	2	3
2	3	4	0	1	4	2	3	2
4	3	2	4	3	1	0	2	4
4	2	3	3	4	0	1	4	2
3	4	2	3	2	4	3	1	0
3	2	4	2	3	3	4	0	1

FIG. 5. The starter array developed with $\mathsf{AGL}(2,5)$ to construct a $\mathsf{CA}(185;3,10,5)$.

$526,915,620$ non-isomorphic one-factorizations and, in general, $\mathcal{K}_{2v}$ may have as many as $((2v-1)!)^{v-1}$ [15], narrower searches must be made. One such search was conducted for $v=7$, but none of the candidate starter arrays were appropriate.

A *set-system* is a pair $(V,\mathcal{B})$, where V is a v-element set of *points* and $\mathcal{B}$ a family of subsets of V, called *blocks*. A *t-wise balanced design* with parameters t-(v,K,λ), is a set-system $(V,\mathcal{B})$ such that each t-element subset of V is in exactly λ blocks. The parameter K is the set of block sizes and for each $k \in K$ we denote the set of blocks of size k by $\mathcal{B}_k$. A *parallel class* in a set-system $(V,\mathcal{B})$ is a collection of blocks that partition the points. A set-system is *resovable* if its collection of blocks can be divided into parallel classes $P_1, P_2, \ldots, P_\ell$. For example a one-factorization of K_{2n} is a resolvable 2-wise balanced design with parameters 2-$(2n,2,1)$. This type of resolvable design was used in Theorems 3.1, 3.2, 3.3 and 3.4. We use another type of resolvable design, the Near Resolvable Design, to construct the starter arrays in Theorems 3.5 and 3.6. A *Near Resolvable Design* $\mathsf{NRB}(v,k,k-1)$, is a resolvable pairwise balanced design $(V,\mathcal{B})$ of type 2-$(v,\{1,k\},k-1)$, with $|\mathcal{B}_1| = v$, in which the blocks are divided into v parallel classes $P_1, P_2, \ldots, P_v$, such that class P_i contains the block $\{i\}$. Results on Near Resolvable Designs can be found in [15, I.6.1]. Each block in $\mathcal{B}_k$ contains $\binom{k}{2}$ t-element subsets of V and each element appears in exactly $k-1$ non-singleton blocks. Thus it is clear that the number of non-singleton blocks is

$$|\mathcal{B}_k| = (k-1)\cdot\frac{\binom{v}{2}}{\binom{k}{2}} = \frac{v(v-1)}{k}.$$

A *labeling* of a resolvable set-system $(V,\mathcal{B})$ having parallel classes $P_1, P_2, \ldots, P_\ell$ with a set Ω is a mapping

$$\mathsf{Label} : \mathsf{B} \longrightarrow \Omega$$

such that $\mathsf{Label}(B) \neq \mathsf{Label}(B')$ whenever B and B' belong to the same parallel class P_j. The *point-by-class incidence matrix* of an Ω labeled resolvable set-system $(V,\mathcal{B})$ with parallel classes $P_1, P_2, \ldots, P_\ell$ is the $|V|$ by ℓ array M given by

$$M[i,j] = \mathsf{label}(B) \text{ if } i \in B \text{ and } B \in P_j$$

for $i \in V$, $j = 1,2,\ldots,\ell$. An example is given in Figure 6.

Theorem 3.5. $\mathsf{CAN}(3,7,3) \leq 45$.

Proof. Develop the blocks $\{\{0\},\{1,2,4\},\{3,5,6\}\}$ mod 7, to form an $\mathsf{NRB}(7,3,2)$ with 7 parallel classes. Use any method to label the three blocks in each class with the symbols from $\Omega = \{0,1,2\}$ and form the 7×7 starter array, M, by constructing the *point-by-class* incidence matrix corresponding to the chosen labeling. See for example Figure 6. Let $\mathcal{G} = \mathsf{S}ym(\Omega)$ and consider the array $[M^{\mathcal{G}}, \mathsf{C}]$. To see why this array is a $\mathsf{CA}(45;3,7,3)$, consider any 3 rows a,b,c. These are points in $\mathbb{Z}_7$. So, either $\{a,b,c\}$ occurs as a block of the NRB, or it doesn't. If $\{a,b,c\}$ is a block, then the three pairs, $\{\{a,b\},\{a,c\},\{b,c\}\}$ occur once more each, accounting for four classes. But each point must still occur in each of the remaining three classes, and it must occur independently of the others. If the block $\{a,b,c\}$ does not occur, then the three pairs from it occur twice, accounting for six classes, leaving the seventh with the requirement that none of the pairs occur. Therefore, if we look at any 3 rows of M, we see each of the following patterns of 3-tuples: $\{(x,y,z),(x,x,y),(x,y,x),(y,x,x)\}$. Consequently, because $\mathcal{G}$ is 3-transitive on Ω, $[\mathsf{M}^{\mathcal{G}}, \mathsf{C}]$ is a $\mathsf{CA}(45;3,7,3)$. □

0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{5\}$	$\{6\}$
1	$\{1,2,4\}$	$\{2,3,5\}$	$\{3,4,6\}$	$\{0,4,5\}$	$\{1,5,6\}$	$\{0,2,6\}$	$\{0,1,3\}$
2	$\{3,5,6\}$	$\{0,4,6\}$	$\{0,1,5\}$	$\{1,2,6\}$	$\{0,2,3\}$	$\{1,3,4\}$	$\{2,4,5\}$
0	0	2	2	1	2	1	1
1	1	0	2	2	1	2	1
2	1	1	0	2	2	1	2
3	2	1	1	0	2	2	1
4	1	2	1	1	0	2	2
5	2	1	2	1	1	0	2
6	2	2	1	2	1	1	0

FIG. 6. A point-by-class incidence matrix of an $\mathsf{NRB}(7,3,2)$ is a starter array for a $\mathsf{CA}(45;3,7,3)$.

Theorem 3.6. $\mathsf{CAN}(3,8,3) \leq 45$.

Proof. The starter array is constructed as in Theorem 3.5, but with $\{i,\infty\}$ replacing block $\{i\}$ in class i, for each $i \in \mathbb{Z}_7$, and ∞ added to the row labels so the starter array has 8 rows. Figure 7 shows the starter array M and $[\mathsf{M}^{\mathcal{G}}, \mathsf{C}]$ is easily checked in a manner similar to Theorem 3.5 to be a $\mathsf{CA}(45;3,8,3)$. □

Theorem 3.7 is based on a pair of disjoint Steiner Triple System, $\mathsf{S}(2,3,9)$, which make a resolvable 2-$(9,\{3\},2)$ design.

Theorem 3.7. $\mathsf{CAN}(3,9,3) \leq 51$.

Proof. The starter array is the *point-by-class* incidence matrix of two block-disjoint $\mathsf{S}(2,3,9)$. The number of blocks in each $\mathsf{S}(2,3,9)$ is $b = 12$, and there are $b/k = 4$ classes. Figure 8 shows the starter array M, and $[\mathsf{M}^{\mathcal{G}}, \mathsf{C}]$ is a $\mathsf{CA}(51;3,9,3)$. The first 4 columns are from one $\mathsf{S}(2,3,9)$ and the last 4 columns are from another. □

0	$\{0,\infty\}$	$\{1,\infty\}$	$\{2,\infty\}$	$\{3,\infty\}$	$\{4,\infty\}$	$\{5,\infty\}$	$\{6,\infty\}$
1	$\{1,2,4\}$	$\{2,3,5\}$	$\{3,4,6\}$	$\{0,4,5\}$	$\{1,5,6\}$	$\{0,2,6\}$	$\{0,1,3\}$
2	$\{3,5,6\}$	$\{0,4,6\}$	$\{0,1,5\}$	$\{1,2,6\}$	$\{0,2,3\}$	$\{1,3,4\}$	$\{2,4,5\}$
0	0	2	2	1	2	1	1
1	1	0	2	2	1	2	1
2	1	1	0	2	2	1	2
3	2	1	1	0	2	2	1
4	1	2	1	1	0	2	2
5	2	1	2	1	1	0	2
6	2	2	1	2	1	1	0
∞	0	0	0	0	0	0	0

FIG. 7. A starter array for a $\mathsf{CA}(45;3,8,3)$.

0	$\{0,1,2\}$	$\{0,3,6\}$	$\{0,4,8\}$	$\{1,3,8\}$	$\{0,1,8\}$	$\{0,2,5\}$	$\{0,3,7\}$	$\{3,5,8\}$
1	$\{3,4,5\}$	$\{1,4,7\}$	$\{1,5,6\}$	$\{2,4,6\}$	$\{2,3,4\}$	$\{1,3,6\}$	$\{1,4,5\}$	$\{0,4,6\}$
2	$\{6,7,8\}$	$\{2,5,8\}$	$\{2,3,7\}$	$\{0,5,7\}$	$\{5,6,7\}$	$\{4,7,8\}$	$\{2,6,8\}$	$\{1,2,7\}$
0	0	0	0	2	0	0	0	1
1	0	1	1	0	0	1	1	2
2	0	2	2	1	1	0	2	2
3	1	0	2	0	1	1	0	0
4	1	1	0	1	1	2	1	1
5	1	2	1	2	2	0	1	0
6	2	0	1	1	2	1	2	1
7	2	1	2	2	2	2	0	2
8	2	2	0	0	0	2	2	0

FIG. 8. A starter array for a $\mathsf{CA}(51;3,9,3)$.

Next, we exploit the 3-transitivity of $\mathsf{PGL}(2,q-1)$ and the relatively small size of $\mathsf{AGL}(2,q)$, which is 2-transitive, when both $q-1$ and q are prime powers. This is reasonable because the construction using $\mathsf{AGL}(2,q)$ presented difficulties for $q>5$. Since $\mathsf{PGL}(2,q-1)$ is quite large, but is sufficiently transitive, we consider using it on a small part of the starter array, while using $\mathsf{AGL}(2,q)$ on the rest. Rosa and Wallis [23] establish the following:

Lemma 3.8. *For $v \geq 4$, any 3 disjoint one-factors of $\mathcal{K}_{2v}$ can be extended to a one-factorization.*

We use Lemma 3.8 to establish the following:

Lemma 3.9. *For $v \geq 4$, there is a one-factorization of $\mathcal{K}_{2v}$ which contains a triangle-free triple of one-factors.*

Proof. $\mathcal{K}_{v,v}$ has the following one-factorization:

$$\{\mathcal{F}_i = \{\{0,i\}+j : j \in \mathbb{Z}_v\} : i \in \mathbb{Z}_{v-1}\}.$$

The union of any three of these one-factors of $\mathcal{K}_{v,v}$ is triangle-free. Because one-factors of $\mathcal{K}_{v,v}$ are also one-factors of $\mathcal{K}_{2v}$ and $v \geq 4$, any three of the above one-factors can be extended to a one-factorization of $\mathcal{K}_{2v}$, by Lemma 3.8. □

We apply the appropriate groups to the appropriate parts of a starter array and find the following:

Theorem 3.10. *When $q-1$ and q are prime powers, and $v \leq q$, there is a* $\mathsf{CA}(N; 3, k, v)$ *with*

$$N = 3q(q-1)(q-2) + (2v-4)q(q-1) + v \approx 5v^3.$$

Proof. Let $\mathcal{F}$ be a one-factorization of $\mathcal{K}_{2v}$ which by Lemma 3.9 contains a triple $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ of triangle-free one-factors. Construct M_3, the $2v \times 3$ array, as in the construction in Theorem 3.1, using $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$. Let M_2 be the $2v \times (2v-4)$ array corresponding to the remaining one-factors, and let $\mathsf{M}_1 = \mathsf{C}(2v, \mathbb{Z}_v)$. On any 3 rows of M_3 there must be at least one column which has 3 distinct entries. By arguments similar to those in the proof of Theorem 3.1, the remaining patterns of 3-tuples occur in M_2 and M_1. Therefore, the desired covering array is:

$$[\mathsf{M}_3^{\mathsf{PGL}(2,q-1)}, \mathsf{M}_2^{\mathsf{AGL}(2,q)}, \mathsf{M}_1].$$

□

4. GENERALIZATIONS OF ROUX'S THEOREM

The following theorem appeared in Sloane [25], and was taken from Roux's PhD dissertation [24].

Theorem 4.1. $\mathsf{CAN}(3, 2k, 2) \leq \mathsf{CAN}(3, k, 2) + \mathsf{CAN}(2, k, 2)$.

The construction is simple and instructive. First append a $\mathsf{CA}(N_2; 2, k, 2)$ to a $\mathsf{CA}(N_3; 3, k, 2)$, making a $k \times (N_3 + N_2)$ array. Then copy it below itself, producing a $2k \times (N_3 + N_2)$ array, and replace the copied strength 2 array by its bit-complement array (switch 0 to 1 and 1 to 0).

We cannot simply double the $\mathsf{CA}(N_3; 3, k, 2)$ for then it would be possible to choose three rows in the constructed array in which a row of the original covering array is repeated. The additional columns arising from the appended $\mathsf{CA}(N_2; 2, k, 2)$ are needed to neutralize this problem.

The constructions in this section were inspired by this idea. First we construct strength two covering arrays using ordered designs, and then we generalize Roux's theorem. An *ordered design*, $\mathsf{OD}(t, k, v)$, is a $k \times \binom{v}{t} t!$ array with entries from a v-element set V such that in any t-tuple of rows, every t-tuple of t distinct entries occurs exactly once. A v by v Latin square L is *idempotent* if $L[i, i] = i$ for all i and they exist when $v \geq 3$. It is easy to see that an $\mathsf{OD}(2, 3, v)$ is equivalent to an idempotent Latin square of order v and so they exist for all $v \geq 3$. Also for all prime powers q the group $\mathsf{AGL}(2, q)$ is sharply 2-transitive. Thus, the $q \times q(q-1)$ array whose columns are the permutation representations of elements of $\mathsf{AGL}(2, q)$ forms an $\mathsf{OD}(2, q, q)$, see [15, IV.30.2].

Theorem 4.2. *For $v \geq 3$, $\mathsf{CAN}(2, 3k, v) \leq \mathsf{CAN}(2, k, v) + v(v-1)$*

Proof. Let A be a $\mathsf{CA}(N_2; 2, k, v)$, let B be an $\mathsf{OD}(2, 3, v)$, and let B_i be row i of B, repeated k times. We claim the following array, C, is a $\mathsf{CA}(N_2 + v(v-1); 2, 3k, v)$:

$$\mathsf{C} = \begin{array}{|ll|}\hline \mathsf{A} & \mathsf{B}_1 \\ \mathsf{A} & \mathsf{B}_2 \\ \mathsf{A} & \mathsf{B}_3 \\ \hline \end{array}$$

Choose any two rows of C. If they include distinct rows of A then all 2-tuples are covered. Otherwise, suppose 2 rows of A are repeated. Then by construction, two distinct rows of B are included. Therefore, all 2-tuples with repeated symbols are covered by the first N_2 columns of C, all 2-tuples with distinct symbols are covered by the last $v(v-1)$ columns of C, and C is the desired covering array. □

Using an $\mathsf{OD}(2, q, q)$ we have

Corollary 4.3. *For $v \leq q$, $\mathsf{CAN}(2, qk, v) \leq \mathsf{CAN}(2, k, v) + q(q-1)$.*

Theorem 4.4. *If there is an $\mathsf{OD}(2, m, u)$ then for $v \leq u$ and $2 \leq k \leq m$,*

$$\mathsf{CAN}(2, m(m-1)k, v) \leq \mathsf{CAN}(2, k, v) + 2u(u-1).$$

Proof. Let A be a $\mathsf{CA}(N_2; 2, k, v)$, let B be an $\mathsf{OD}(2, m, u)$, and let B_i be row i of B, repeated k times. For $i = 1, \ldots, m-1$, and subscripts $\in \mathbb{Z}_m$, construct $mk \times (N_2 + 2u(u-1))$ arrays as follows:

$$\mathsf{C}_i = \begin{array}{|lcc|}\hline \mathsf{A} & \mathsf{B}_1 & \mathsf{B}_{i+1} \\ \mathsf{A} & \mathsf{B}_2 & \mathsf{B}_{i+2} \\ \vdots & \vdots & \vdots \\ \mathsf{A} & \mathsf{B}_{m-1} & \mathsf{B}_{i+m-1} \\ \mathsf{A} & \mathsf{B}_m & \mathsf{B}_{i+m} \\ \hline \end{array}$$

Let $\mathsf{C} = [\mathsf{C}_1, \mathsf{C}_2, \ldots, \mathsf{C}_m - 1]^{\mathsf{T}}$ be the concatenation of these arrays, top to bottom. Any two rows of C include either a repeated row of A and two distinct rows of B, or just the opposite. Either way, all 2-tuples with distinct entries appear in one half, and those with repeated entries appear in the other. Thus, C is a

$$\mathsf{CA}(N_2 + 2u(u-1); 2, m(m-1)k, v).$$

□

Using an $\mathsf{OD}(2, q, q)$, we have for $2 \leq k, v \leq q$:

$$\mathsf{CAN}(2, q(q-1)k, v) \leq \mathsf{CAN}(2, k, v) + 2q(q-1).$$

The following constructions for strength 3 arrays are similar. Using only two copies of a $\mathsf{CA}(3, k, v)$ is an easier construction than using three due to the fact that tripling allows a single row of the covering array to be chosen three times, thus covering *only* pattern $[x, x, x]^T$. Interchanging bits in Roux's theorem is the binary form of deranging the symbols: instead of merely ensuring that $0 \mapsto 1$ and $1 \mapsto 0$, we show that supplying all possible maps $x \mapsto y$ for $x \neq y$ is sufficient for doubling the number of rows.

Theorem 4.5. $\mathsf{CAN}(3, 2k, v) \leq \mathsf{CAN}(3, k, v) + (v-1)\mathsf{CAN}(2, k, v)$.

Proof. Let A be a $\mathsf{CA}(N_3; 3, k, v)$, and B be a $\mathsf{CA}(N_2; 2, k, v)$, both on the symbol set $\{1, 2, 3, \ldots, v\}$. Let C_v be the cyclic group of permutations generated by

$$\pi = (1, 2, 3, \ldots, v).$$

Construct C as follows:

$$\mathsf{C} = \boxed{\begin{array}{ccccc} \mathsf{A} & \mathsf{B} & \mathsf{B} & \cdots & \mathsf{B} \\ \mathsf{A} & \mathsf{B}^{\pi^1} & \mathsf{B}^{\pi^2} & \cdots & \mathsf{B}^{\pi^{v-1}} \end{array}}$$

where B^g is the array obtained by applying the permutation g to each of the symbols in B. Consider three rows of C, $a, b, c \in \{1, \ldots, 2k\}$, and all patterns of 3-tuples:

$$\begin{array}{ccccc} x & x & x & y & x \\ x & x & y & x & y \\ x & y & x & x & z \end{array}$$

If a, b, c include 3 distinct rows of A, then all triples on these rows occur among the first N_3 columns. If $a < b \leq k < c = a + k$, then the triples with patterns $[x, y, x]^{\mathsf{T}}$ or $[x, x, x]^{\mathsf{T}}$ occur in the first N_3 columns of C. For pattern $[x, x, y]^{\mathsf{T}}$ we observe that there is a permutation, $\pi^j \in C_v$, which maps x to y. Hence the triples with this pattern are covered in the corresponding section of C, Similarly, patterns $[y, x, x]^{\mathsf{T}}$ and $[x, y, z]^{\mathsf{T}}$ are covered since there is a permutation $\pi^{j'}$ mapping y to x and permutation $\pi^{j''}$ which maps x to z. Checking the case $c = b + k$ is similar. The other cases $a \leq k < b < c$ are easily checked, using the inverse permutations. Therefore, C is a covering array, $\mathsf{CA}(N_3 + (v-1)N_2; 3, 2k, v)$. □

Theorem 4.5 and the result

$$\lim_{k \to \infty} \frac{\mathsf{CAN}(2, k, v)}{\log_2 k} = \frac{v}{2}$$

proven in [17] give us our next theorem:

Theorem 4.6.

$$\lim_{k \to \infty} \frac{\mathsf{CAN}(3, k, v)}{\log k} = \binom{v}{2}.$$

5. COMPARISON WITH A COMMERCIAL TESTING TOOL

The $\mathsf{AETG}^{\mathsf{SM}}$ Web (AETG is a service mark of Telcordia$_{\mathsf{TM}}$ Technologies, Inc.) is an online commercial system which generates test sets based on a model of a system. The system is located at `http://aetgweb.argreenhouse.com`. The tester can input names of parameters, create relations between the parameters, define levels for each parameter, specify coverage, omit certain combinations from the test set or require the occurrence of certain combinations, and more. The details are discussed in [12, 10, 11]. The covering arrays constructed using algebraic techniques such as those introduced in this article provide complete three-way coverage of discrete parameters, all with the same number of levels, and are smaller than the

TABLE I. Relative sizes of $\mathsf{CA}(N;3,k,v)$: entries are (AETG,algebraic methods).

$k\backslash v$	3	4	5	6	9	10
6	47,33	105,64		343,305		1508,1331
7	50,45	116,88	229,185			1664,1331
8	56,45	131,88	249,185			1832,1331
9	60,51	141,112	272,185			1998,1331
10	63,55	150,112	287,185			2145,1331
11	65,57	157,121	308,225			2283,1331
12	71,57	166,127	319,225	548,510		2414,1331
27					?,2187	0,2541

corresponding test sets generated by the AETG system. We expect our methods to improve results on other types of test sets such as adaptive and mixed-level.

Table I compares the sizes of a few test sets developed in this article with those generated by AETG. When we attempted to construct a covering array with 27 factors at 9 levels, the system ran for several hours and returned no result, so we aborted the computation. Our next attempt involved 27 factors at 10 levels. After a few seconds the system returned a test set of size 0, which seems to indicate system failure. Generation of 4-way covering test sets was attempted and the system failed to produce any results.

6. TABLES

Tables III, IV, V, and VI show current bounds on the covering array numbers, $\mathsf{CAN}(3,k,v)$ and $\mathsf{CAN}(2,k,v)$. The $[k,v]$-entry is either N, when $\mathsf{CAN}(t,k,v)=N$, or $[N_\ell, N_u]$, when only $N_\ell \leq \mathsf{CAN}(t,k,v) \leq N_u$ is known. The superscripts are decoded in the Table II. When an entry has no superscript, it is due to **row-collapsing**.

TABLE II. Key for covering array tables.

a	No OA	Bush
b		Sloane[25]
c	$\mathsf{PHF}(N_1;t,k,m) \times \mathsf{CA}(N_2;t,m,v)$	Theorem2.4, bias[3, 2]
d	$\mathsf{CAN}(t,k,v-1) \leq \mathsf{CAN}(t,k,v)$	**symbol-collapsing**
e	$\mathsf{CAN}(t,k,v) \geq \mathsf{CAN}(t-1,k-1,v)$	**derived array bound**
f	$\mathsf{CA}(M;t,k,w) \times \mathsf{CAN}(N;t,k,v)$	**product**
g	No $\mathsf{MOLS}(2)$	Theorem1
h	$[\mathsf{M}^{\mathsf{AGL(2,q)}}, C]$	Theorems3.2 and 3.4
i		Nurmela[22]
j		**squaring** k[9]
k		**construction D**
l	$\mathsf{CAN}(3,2k,v) \leq \mathsf{CAN}(3,k,v) + (v-1)\mathsf{CAN}(2,k,v)$	Theorem 4.5
m	OA	Sloane[18]
n		Katona[19]
o		Östergård-Mallows[9, 25]
s		Stevens[26]
t	$\mathsf{CAN}(2,3k,v), \mathsf{CAN}(2,qk,v)$	Theorem 4.2,Corollary4.3
y	AETG	Cohen, et.al.[13]

TABLE III. $\mathsf{CAN}(2,k,v)$

$k\backslash v$	2	3	4	5	6	7	8	9	10	11
3	4^m	9	16	25	36^m	49	64	81	100	121
4	5^g	9^m	16	25	37^s	49	64	81	100^m	121
5	6	11^o	16^m	25	37 ,39^i	49	64	81	100 ,101	121
6	6	12	19^s	25^m	37 ,41^i	49	64	81	100 ,101^s	121
7	6	12	19,21^s	29^s	37 ,42^i	49	64	81	100 ,120	121
8	6	12 ,13	19,23^s	29,33^i	39^s,42^i	49^m	64	81	100 ,120	121
9	6	12 ,13^s	19,24	29,35^i	39 ,48^t	52^s,63	64^m	81	100 ,120	121
10	6^n	12 ,14^i	19,24^i	29,37^i	39 ,52^i	52 ,63^s	67^s,80	81^m	100 ,120	121
11	7	12 ,15	19,25^i	29,38^i	39 ,55^i	52 ,73^i	67 ,80^s	84^s,120	100 ,120	121
12	7	12 ,15	19,26	29,40^i	39 ,57^i	52 ,76^i	67 ,99^i	84 ,120	103^s,120	121^m
13	7	12 ,15	19,26^i	29,41^i	39 ,58^i	52 ,79^i	67 ,102^i	84 ,120^d	103 ,120^s	124^s,231
14	7	12 ,15	19,27	29,42^i	39 ,60^i	52 ,81^i	67 ,104^i	84 ,131^i	103 ,162^i	124 ,231
15	7^n	12 ,15	19,27^i	29,43^i	39 ,61^i	52 ,83^i	67 ,107^i	84 ,135^i	103 ,166^i	124 ,231
16	8	12 ,15	19,28	29,45	39 ,69^s	52 ,91	67 ,120	84 ,153	103 ,180	124 ,231
17	8	12 ,15	19,28	29,45	39 ,76	52 ,91	67 ,120	84 ,153	103 ,180	124 ,231
18	8	12 ,15	19,28	29,45	39 ,76	52 ,91	67 ,120	84 ,153	103 ,180	124 ,231
19	8	12 ,15^i	19,28	29,45	39 ,76	52 ,91	67 ,120	84 ,153	103 ,180	124 ,231
20	8	12 ,17	19,28^s	29,45	39 ,76	52 ,91	67 ,120	84 ,153	103 ,180	124 ,231
21	8	12 ,17	19,31	29,45	39 ,76	52 ,91	67 ,120	84 ,153	103 ,180^y	124 ,231
22	8	12 ,17	19,31	29,45	39 ,76	52 ,91	67 ,120	84 ,153	103 ,202	124 ,231
23	8	12 ,17	19,31	29,45	39 ,76	52 ,91	67 ,120	84 ,153	103 ,202	124 ,231
24	8	12 ,17^i	19,31	29,45	39 ,76	52 ,91	67 ,120	84 ,153	103 ,202	124 ,231
25	8	12 ,18	19,31^s	29,45^x	39 ,76	52 ,91	67 ,120	84 ,153	103 ,202	124 ,231
26	8	12 ,18	19,32	29,49	39 ,76	52 ,91	67 ,120	84 ,153	103 ,202	124 ,231
27	8	12 ,18	19,32	29,49	39 ,76	52 ,91	67 ,120	84 ,153	103 ,202	124 ,231
28	8	12 ,18	19,32	29,49	39 ,76	52 ,91	67 ,120	84 ,153	103 ,202	124 ,231
29	8	12 ,18	19,32	29,49	39 ,76	52 ,91	67 ,120	84 ,153	103 ,202	124 ,231
30	8	12^n,18^i	19,32^s	29,49^s	39 ,76^s	52 ,91^s	67 ,120^t	84 ,153^t	103 ,202	124 ,231

TABLE IV. $\mathsf{CAN}(2, k, v)$

$k\backslash v$	12	13	14	15	16	17	18	19
3	144	169	196^m	225	256	289	324^m	361
4	144	169	196 ,225	225	256	289	324 ,333^f	361
5	144	169	196 ,225	225	256	289	324 ,360	361
6	144	169	196 ,225^d	225^m	256	289	324 ,360	361
7	144^m	169	196 ,255	225 ,255	256	289	324 ,360	361
8	144 ,169	169	196 ,255	225 ,255	256	289	324 ,360	361
9	144 ,169	169	196 ,255	225 ,255	256	289	324 ,360	361
10	144 ,169	169	196 ,255	225 ,255	256	289	324 ,360	361
11	144 ,169	169	196 ,255	225 ,255	256	289	324 ,360	361
12	144 ,169	169	196 ,255	225 ,255	256	289	324 ,360	361
13	144 ,169	169	196 ,255	225 ,255	256	289	324 ,360	361
14	147^s,169^d	169^m	196 ,255	225 ,255	256	289	324 ,360	361
15	147 ,255	172^s,255	196 ,255	225 ,255	256	289	324 ,360	361
16	147 ,255	172 ,255	199^s,255	225 ,255	256	289	324 ,360	361
17	147 ,255	172 ,255	199 ,255	228^s,255	256^m	289	324 ,360	361
18	147 ,255^d	172 ,255^d	199 ,255^d	228 ,255^s	259^s,288	289^m	324 ,360	361
19	147 ,276	172 ,325	199 ,360	228 ,288^d	259 ,288^s	292^s,360	324 ,360	361
20	147 ,276	172 ,325	199 ,360	228 ,360	259 ,360	292 ,360	327^s,360	361^m
21	147 ,276^t	172 ,325	199 ,360^d	228 ,360^d	259 ,360^d	292 ,360^d	327 ,360^s	364^s,529
22	147 ,288	172 ,325	199 ,437	228 ,450	259 ,496	292 ,561	327 ,529	364 ,529
23	147 ,288	172 ,325	199 ,437	228 ,450	259 ,496	292 ,561	327 ,529	364 ,529
24	147 ,288	172 ,325	199 ,437^l	228 ,450	259 ,496	292 ,561	327 ,529^d	364 ,529^d
25	147 ,288	172 ,325	199 ,437	228 ,450	259 ,496	292 ,561	327 ,600^d	364 ,600^d
26	147 ,288	172 ,325	199 ,437	228 ,450	259 ,496	292 ,561	327 ,625^d	364 ,625^d
27	147 ,288	172 ,325	199 ,437^l	228 ,450	259 ,496	292 ,561	327 ,666	364 ,703
28	147 ,288	172 ,325	199 ,437	228 ,450	259 ,496	292 ,561	327 ,666	364 ,703
29	147 ,288	172 ,325	199 ,437	228 ,450	259 ,496	292 ,561	327 ,666	364 ,703
30	147 ,288^t	172 ,325^t	199 ,437^t	228 ,450^j	259 ,496^t	292 ,561^t	327 ,666^t	364 ,703^t

TABLE V. CAN$(3, k, v)$

$k\backslash v$	2	3	4	5	6	7	8	9
4	8^m	27^m	64	125	216^m	343	512	729
5	10^g	28^a,33	64	125	222^e,275^k	343	512	729
6	12	33^h	64^m	125^m	222 ,305^k	343	512	729
7	12	36^e,45	76^e,88	125 ,185	222 ,343	343	512	729
8	12	36 ,45^l	76 ,88^h	145^e,185	222 ,343^v	343^m	512	729
9	12	36 ,51^h	76 ,112	145 ,185	234^e,470	343 ,512	512	729
10	12	36 ,55^l	76 ,112^l	145 ,185^h	234 ,470^l	364^e,512^v	512^m	729^m
11	12^b	36 ,57	76 ,121	145 ,225	234 ,510	364 ,637	536^e,960	729 ,1331
12	14^e,15^i	36 ,57^l	76 ,121^l	145 ,225^l	234 ,510^l	364 ,637	536 ,960	756^e,1331^d
13	14 ,16	36 ,69	76 ,151	145 ,301	234 ,553	364 ,637	536 ,960	756 ,1377
14	14 ,16^b	36 ,69^l	76 ,151^l	145 ,301^l	234 ,553	364 ,637	536 ,960	756 ,1377
15	14 ,17	36 ,74	76 ,159	145 ,317	234 ,553	364 ,637	536 ,960	756 ,1377
16	14 ,17^b	36 ,74^l	76 ,159^l	145 ,317^l	234 ,553^l	364 ,637^l	536 ,960	756 ,1377
17	16^e,18	36 ,77	76 ,184	145 ,325	234 ,710	364 ,890	536 ,960	756 ,1377
18	16 ,18	36 ,77^l	76 ,184	145 ,325^l	234 ,710^l	364 ,890	536 ,960^l	756 ,1377
19	16 ,18	36 ,83	76 ,184	145 ,333	234 ,730	364 ,890	536 ,1072	756 ,1377
20	16 ,18^l	36 ,83^l	76 ,184^l	145 ,333^l	234 ,730^l	364 ,890^l	536 ,1072^l	756 ,1377^l
21	16 ,18	36 ,87	76 ,196	145 ,377	234 ,785	364 ,1029	536 ,1520	756 ,2187
22	16 ,18^l	36 ,87	76 ,196^l	145 ,377^l	234 ,785^l	364 ,1029	536 ,1520^l	756 ,2187
23	16 ,22	36 ,87	76 ,199	145 ,385	234 ,795	364 ,1029	536 ,1536	756 ,2187
24	16 ,22^i	36 ,87^l	76 ,199^l	145 ,385^l	234 ,795^l	364 ,1029	536 ,1536	756 ,2187
25	16 ,23	36 ,99	76 ,229	145 ,465	234 ,843	364 ,1029	536 ,1536	756 ,2187
26	16 ,23	36 ,99	76 ,229^l	145 ,465^l	234 ,843^l	364 ,1029	536 ,1536	756 ,2187
27	16 ,23	36 ,99	76 ,232	145 ,469	234 ,853	364 ,1029	536 ,1536	756 ,2187
28	16 ,23^l	36 ,99	76 ,232^l	145 ,469^l	234 ,853^l	364 ,1029	536 ,1536	756 ,2187
29	16 ,24	36 ,104	76 ,238	145 ,473	234 ,858	364 ,1029	536 ,1536	756 ,2187
30	16 ,24^l	36 ,104^l	76 ,238^l	145 ,473^l	234 ,858^l	364 ,1029^l	536 ,1536^c	756 ,2187^c

TABLE VI. $\mathsf{CAN}(3,k,v)$

$k\backslash v$	10	11	12	13	14	15
4	1000^m	1331	1728^m	2197	2744^m	3375^m
5	1000 ,1250^f	1331	1728 ,2112^f	2197	2744 ,3430^f	3375 ,4096
6	1000 ,1331	1331	1728 ,2112^f	2197	2744 ,4096	3375 ,4096
7	1010^e,1331	1331	1728 ,2197	2197	2744 ,4096	3375 ,4096
8	1010 ,1331	1331	1728 ,2197	2197	2744 ,4096	3375 ,4096
9	1010 ,1331	1331	1728 ,2197	2197	2744 ,4096	3375 ,4096
10	1010 ,1331	1331	1728 ,2197	2197	2744 ,4096	3375 ,4096
11	1010 ,1331	1331	1728 ,2197	2197	2744 ,4096	3375 ,4096
12	1010 ,1331^d	1331^m	1728 ,2197	2197	2744 ,4096	3375 ,4096
13	1030^e,2197	1331 ,2197	1728 ,2197	2197	2744 ,4096	3375 ,4096
14	1030 ,2197^d	1364^e,2197^d	1728 ,2197^d	2197^m	2744 ,4096	3375 ,4096
15	1030 ,2411	1364 ,2541	1764^e,3696	2197 ,4096	2744 ,4096	3375 ,4096
16	1030 ,2411	1364 ,2541	1764 ,3696	2236^e,4096	2744 ,4096	3375 ,4096
17	1030 ,2411	1364 ,2541	1764 ,3696	2236 ,4096	2786^e,4096	3375 ,4096
18	1030 ,2411	1364 ,2541	1764 ,3696^l	2236 ,4096^d	2786 ,4096^d	3420^e,4096^d
19	1030 ,2411	1364 ,2541	1764 ,3781	2236 ,4225	2786 ,6859	3420 ,6859
20	1030 ,2411	1364 ,2541	1764 ,3781	2236 ,4225	2786 ,6859^d	3420 ,6859^d
21	1030 ,2411	1364 ,2541	1764 ,3781^l	2236 ,4225	2786 ,7411	3420 ,7666
22	1030 ,2411	1364 ,2541	1764 ,4056	2236 ,4225	2786 ,7411	3420 ,7666
23	1030 ,2411	1364 ,2541	1764 ,4056	2236 ,4225	2786 ,7411	3420 ,7666
24	1030 ,2411^l	1364 ,2541	1764 ,4056	2236 ,4225	2786 ,7411	3420 ,7666
25	1030 ,2541	1364 ,3993	1764 ,4056	2236 ,4225	2786 ,7411	3420 ,7666
26	1030 ,2541	1364 ,3993	1764 ,4056	2236 ,4225	2786 ,7411	3420 ,7666
27	1030 ,2541	1364 ,3993	1764 ,4056	2236 ,4225	2786 ,7411	3420 ,7666
28	1030 ,2541^d	1364 ,3993	1764 ,4056^l	2236 ,4225^l	2786 ,7411	3420 ,7666
29	1030 ,3905	1364 ,3993	1764 ,6501	2236 ,6591	2786 ,7411	3420 ,7666
30	1030 ,3905^l	1364 ,3993	1764 ,6501	2236 ,6591	2786 ,7411	3420 ,7666

ACKNOWLEDGEMENTS

We thank Kari Nurmela and Brett Stevens for helpful discussions, and Charles Colbourn for encouragement. Many of the results in this paper are presented in the first author's dissertation [8]. He is grateful to the Department of Mathematical Sciences at Michigan Technological University for its support. Specifically, thanks to his advisor, Don Kreher, and to his committee, Alphonse Baartmans, Konrad Heuvers, and Linda Ott. He is also grateful to the Center for Applied Cryptographic Research at the University of Waterloo for its support.

REFERENCES

[1] M. Atici and S. S. Magliveras and D. R. Stinson and W.-D. Wei, Some recursive constructions for perfect hash functions. *J. Combinat. Designs* (4):353-363, 1996.

[2] J. Bierbrauer and H. Schellwat, Almost independent and weakly biased arrays: efficient constructions and cryptologic applications. *Advances in Cryptology*, CRYPTO 2000, *Lecture Notes in Computer Science*, 533-543, 2000.

[3] J. Bierbrauer and H. Schellwat, Weakly biased arrays, almost independent arrays, and error-correcting codes. DIMACS, 2000, to appear.

[4] S.R. Blackburn, Perfect hash families: probabilistic methods and explicit constructions, *J. Combinat. Theory, A*, 2000, to appear.

[5] J. Boyar, G. Brassard, and R. Peralta, Subquadratic zero-knowledge. *JACM* 42(6):1196-1193, 1995.

[6] G. Brassard, C. Crépeau, and M. Santha, Oblivious transfers and intersecting codes. *IEEE Trans. on Information Theory*, 42(6):1769-1780, 1996.

[7] J. Carter and M. Wegman, Universal classes of hash functions. *J. Computer and System Sci.*, 18:143-154, 1979.

[8] M. Chateauneuf, *Covering arrays.* PhD thesis, Michigan Technological University, 2000.

[9] M.A. Chateauneuf, C.J. Colbourn, and D.L. Kreher, Covering arrays of strength 3. *Designs, Codes and Cryptography*, 16:235-242, 1999.

[10] D.M. Cohen, S.R. Dalal, M.L. Fredman, and G.C. Patton, The AETG system: a new approach to testing based on combinatorial design. Technical Report TM-25261, Bell Communications Research, Morristown NJ, 1995.

[11] D. M. Cohen, S. R. Dalal, M. L. Fredman, and G. C. Patton, The AETG system: an approach to testing software based on combinatorial design. *IEEE Trans. Software Engineering* 23:437-444, 1997.

[12] D.M. Cohen and S.R. Dalal and A. Kajla and G.C. Patton, The automatic efficient test generator. In *Proc. 5th Int'l Symp. Software Reliability Eng.*, pages 303-309, Los Alamitos CA, 1994. IEEE CS Press.

[13] D. M. Cohen, S. R. Dalal, J. Parelius, and G. C. Patton, The combinatorial design approach to automatic test generation. *IEEE Software* 13:83-88, 1996.

[14] G. Cohen and G. Zémor, Intersecting codes and independent families. *IEEE Trans. on Information Theory*, (40):1872-1881, 1994.

[15] C. J. Colbourn and J. H. Dinitz (editors), *The CRC Handbook of Combinatorial Designs.* CRC Press, Boca Raton, 1996.

[16] A. Gal, A characterization of span program size and improved lower bounds for monotone span programs. In *13th Symposium of the Theory of Computing*, pages 429-437, 1998.

[17] L. Gargano, J. Körner, and U. Vaccaro, Sperner capacities. *Graphs and Combinatorics* (9):31-46, 1993.

[18] A.S. Hedayat, N.J.A. Sloane, and John Stufken, *Orthogonal Arrays, Theory and Applications*. Springer, 1999.

[19] G.O.H. Katona, Two applications (for search theory and truth functions) of Sperner type theorems. *Periodica Math. Hung.*, 3:19-26, 1973.

[20] K. Kurosawa, T. Johansson, and D. Stinson, Almost k-wise independent sample spaces and their cryptologic applications. *Advances in Cryptology, Eurocrypt 97*, Lecture Notes in Computer Science, (1233):409-421, 1997.

[21] M. Naor and O. Reingold, On the construction of pseudo-random permutations: Luby-Rackoff revisited. *STOC*, (29):189-199, 1997. (complete version: `http://theory.lcs.mit.edu/tcryptol/homepage.html`)

[22] K. Nurmela, Upper bounds for covering arrays by tabu search. *submitted.*

[23] A. Rosa and W.D. Wallis, Premature sets of one-factors or how not to schedule round robin tournaments. *J. Combinat. Designs*, 4(4):291-297, 1982.

[24] G. Roux, *k-propriétés dans des tableaux de n colonnes; cas particulier de la k-surjectivité et de la k-permutivité*. PhD thesis, University of Paris, 1987.

[25] N. J. A. Sloane, Covering arrays and intersecting codes, *J. Combinat. Designs* 1:51-63, 1993.

[26] B. Stevens, *Transversal covers and packings*. PhD thesis, University of Toronto, 1998.

[27] B. Stevens, L. Moura, and E. Mendelsohn, Lower bounds for transversal covers. *Designs, codes and cryptography*, 15(3):279-299, 1998.

[28] D.R. Stinson, R. Wei, and L. Zhu, New constructions for perfect hash families and related structures using combinatorial designs and codes. *J. Combinat. Designs*, 8(3):189-200, 2000.

[29] M. Wegman and J. Carter, New hash functions and their use in authentication and set equality. *J. Computer and System Sci.*, 22(3):265-279, 1981.

Received Nov 29, 2000
Accepted ??