Covering Arrays and Intersecting Codes

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, New Jersey 07974

September 18, 1992

ABSTRACT

A t-covering array is a set of k binary vectors of length n with the property that, in any t coordinate positions, all 2^t possibilities occur at least once. Such arrays are used for example in circuit testing, and one wishes to minimize k for given values of n and t. The case $t = 2$ was solved by Rényi, Katona, and Kleitman and Spencer. The present paper is concerned with the case $t = 3$, where important (but unpublished) contributions were made by Busschbach and Roux in the 1980's. One of the principal constructions makes use of intersecting codes (linear codes with the property that any two nonzero codewords meet). This paper studies the properties of 3-covering arrays and intersecting codes, and gives a table of the best 3-covering arrays presently known. For large n the minimal k satisfies $3.21256 < k/\log n < 7.56444$.

Covering Arrays and Intersecting Codes

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, New Jersey 07974

1. Introduction

Before shipping those new machines off to your customers, you want to run some final tests. There are sixteen switches on the back of each machine that have to be set, each with two positions. Since there are $2^{16} = 65536$ possible combinations, you can't test them all. Instead, you would like to find a small number of test settings for the sixteen switches such that every subset of three switches gets exercised in all 2^3 possible ways. In other words, you would like a minimal set of binary vectors of length 16 with the property that the projection onto any three coordinates includes all 2^3 possibilities. How many test vectors do you need? The answer is not more than 17: you could for example use the vectors

$$\begin{array}{c} 0000000000000000 \\ (0000101101110111) \end{array} \tag{1}$$

where the parentheses indicate that all sixteen cyclic shifts of this vector are to be used. This is a *3-covering array*. It is not known if 17 is minimal (the best lower bound is 14).

More generally, a *t-covering array* with alphabet size q, length n and size k consists of k vectors of length n with entries from $\{0, 1, \ldots, q-1\}$ with the property that the projection onto any t coordinates contains all q^t possibilities. Other names are *t-surjective array*, or (for the transposed array) a *qualitatively t-independent family* of vectors. The problem, apparently first studied by Rényi [48], is to minimize k for given values of q, t, n, or equivalently to maximize n for given values of q, t, k. As the bibliography shows, there is an extensive body of literature related to this problem.

In the case $t = q = 2$ the problem was completely solved by Rényi [48] (for k even) and independently by Katona [30] and Kleitman and Spencer [34] (for all k). The answer is that for any k, the maximal length of a binary 2-covering array of size k is

$$n = \binom{k-1}{\lceil \frac{k}{2} \rceil} . \tag{2}$$

Such an array may be constructed as follows. The names of the symbols in any column of the array may be permuted, so we may assume the first row is the zero vector $\mathbf{0}$. The columns of the remaining $k-1$ rows are then taken to be the characteristic vectors of all $\lceil \frac{k}{2} \rceil$-subsets of a $(k-1)$-set. The proof that this is optimal uses Sperner's lemma [53], [26], [31] (if k is even) and the Erdös-Ko-Rado theorem [21] (if k is odd).

For large n, (2) implies that the minimal k satisfies

$$k = \log n + \frac{1}{2} \log \log n \ \cdots \tag{3}$$

(all logs are to base 2).

In the case $t = 2$, $q > 2$, the rate of growth of k with n was recently determined by Gargano, Körner and Vaccaro [24], [25], who show that for large n the minimal k satisfies

$$k = \frac{q}{2} \log n \ (1 + o(1)) \ . \tag{4}$$

However, they do not give an explicit construction of 2-covering arrays that achieve (4), and not much seems to be known about exact values of k for small n.

For example, let us briefly discuss the case $t = 2$, $q = 3$ (the "ternary Spernery" problem). In an earlier paper Gargano, Körner and Vaccaro [23] gave an explicit construction achieving $k = 2.07 \log n \ (1 + o(1))$. Other constructions were given by Poljak, Pultr and Rödl [46] and Poljak and Tuza [47]. For $n = 2, 3, 4$ the codewords of the tetracode ([17], p. 81) show that the minimal k is 9. For $n = 5$, Östergård [45] showed that $k \leq 11$, and Applegate [2] recently used integer programming to show that $k = 11$. Applegate's solution may be transformed to read $\mathbf{0}$, $\pm(01112)$. For $n = 6$ Cook [18] also used integer programming to show that $k \leq 12$. His solution may be written as 0(01221), 111000, 100110, 120201, 102022, 202202, 210011, 221120. For slightly larger values of n reasonably good arrays can be formed by taking three copies of the array that solves the $q = t = 2$ problem (see (2)), removing the $\mathbf{0}$ row from each, then writing one copy in terms of 0's and 1's, one copy in terms of 1's and 2's, and one copy in terms of 2's and 0's. This produces an array of size $k = 3a$ and length

$$n = \binom{a}{\lceil \frac{a+1}{2} \rceil} \ . \tag{5}$$

(A similar but slightly less efficient construction was given in [47].) In summary, for $t = 2$, $q = 3$ the smallest known values of k for given values of n are

$$\begin{array}{lcccccccccccc} n: & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & \cdots \\ k: & 9 & 9 & 9 & 11 & 12 & 15 & 15 & 15 & 15 & 18 & 18 & \cdots . \end{array}$$

The values for $n \leq 5$ are optimal, while it seems likely that those for $n \geq 8$ can be improved. It would be nice to have a more extensive table.

Applegate's integer programming formulation [2] is worth recording, since it can be applied to the general problem of finding a t-covering array of minimal size. Let V be the set of all q^n possible vectors that can be used in the array, let S be the set of all $\binom{n}{t}$ t-tuples of coordinates, and let P be the set of all q^t q-ary vectors of length t. A t-covering array $D \subseteq V$ is specified by setting $x_v = 1$ if $v \in D$, $x_v = 0$ if $v \notin D$. Then finding a minimal array is equivalent to the integer program: choose $x_v \in \{0, 1\}$ for $v \in V$ so as to

$$\text{minimize} \qquad k = \sum_{v \in V} x_v \tag{6}$$

subject to the constraints

$$\sum x_v \geq 1 \quad \text{for all} \quad s \in S, \quad p \in P \ , \tag{7}$$

where the sum in (7) is over all $v \in V$ such that the projection of v onto s is p.

The main purpose of the present paper is to study the case $t = 3$, $q = 2$. Important results were obtained by Busschbach in an unpublished technical report in 1984 [8], and by Roux in an unpublished thesis in 1987 [50]. However, as we shall see, their results can be somewhat improved. The main results of this paper are contained in Theorem 5 and Table 3 in Section 3.

One of the best constructions for 3-covering arrays (due to Busschbach [8]) makes use of "intersecting codes", and Section 2 is devoted to these codes.

The cases $t \geq 4$ (and $q \geq 2$) will not be discussed here. Some results on these problems can be found in [1], [8], [11], [13], [29], [34], [47], [50], [51], [54], [55], [56]. Applications of these covering arrays and related structures to circuit testing, digital communication, network design, etc., are discussed in [4], [8], [12], [15], [19], [44], [51], [52], [54], [55]. The survey article by Körner and Lucertini [35] gives an overview of these and several related problems. Honkala [28] uses t-covering arrays in the construction of codes with small covering radius. Sherwood [52] describes a computer program CATS ("Constrained Array Test System"), which attempts to find small covering arrays for a large class of problems, including ones in which the alphabet size q varies from coordinate to coordinate. Seroussi and Bshouty [51] show that a generalized version of the problem of finding a minimal t-covering array is NP-complete.

2. Intersecting codes

A linear code $\mathcal{C}$ of length N, dimension K and minimal Hamming distance D, i.e. an $[N, K, D]$ code, over a field of order Q is called *intersecting* (or *linked*) if any two nonzero codewords have at least one coordinate where they are both nonzero. Such codes have been studied by several authors [14], [32], [38], [43], [49]. Given K, the problem is to determine $f_Q(K)$, the minimal length N of any $[N, K, D]$ intersecting code. In view of Theorem 2(i), finding $f_2(K)$ may be regarded as a "linear Sperner" problem.

The main properties of intersecting codes are the following. $D_{\max}$ denotes the maximal distance between codewords. Most of the results assembled in Theorems 1 and 2 are elementary.

Theorem 1. *(i) If $\mathcal{C}$ is intersecting then $D \geq K$ [38]. (ii) If $D_{\max} < 2D$ then $\mathcal{C}$ is intersecting [14]. (iii) If $\mathcal{C}$ is an $[N, K, D]$ intersecting code with generator matrix $[A\ I]$ then*

$$\begin{bmatrix} A & I & I & 0 \\ 00\ldots0 & 11\ldots1 & 00\ldots0 & 1 \end{bmatrix}$$

generates an $[N+K+1, K+1, K+1]$ intersecting code [14]. (iv) The direct product ([40], p. 568) of $[N_1, K_1, D_1]$ and $[N_2, K_2, D_2]$ intersecting codes is an $[N_1N_2, K_1K_2, D_1D_2]$ intersecting code [14]. (v) If $N = 2K - 1$ then an $[N, K, D]$ MDS code ([40], p. 317) is intersecting (since $D = (N+1)/2$). Such codes exist if $N \leq Q + 1$ ([40], p. 323).

Proof of (i). Let $u_1 = 11\ldots10\ldots0 \in C$ have weight D, and choose a basis $u_1, u_2, \ldots, u_K$ for C in which $u_2, \ldots, u_K$ begin with a 0. Since $u_2, \ldots, u_K$ must intersect u_1, $K - 1 \leq D - 1$.

Theorem 2. *Let $\mathcal{C}$ be a binary intersecting code. (i) For any two nonzero codewords u and v there is a coordinate where u is 0 and v is 1 [8]. (ii) $D_{\max} \leq N - K + 1$ [6]. (iii) $N \geq 3(K-1)$ [6].*

Proof of (iii). Let u be a minimal weight codeword, and choose another word v that has at least $K - 1$ 0's in the support of u. This is possible since $D \geq K$. Then $N - K + 1 \geq wt(u + v) \geq 2D - 2(D - K + 1)$.

The application to the construction of 3-covering arrays given in the next section is based on the following property.

Theorem 3. *Let u, v, w be distinct codewords of an intersecting code. Then either (i) there is a coordinate where u, v, w are distinct, or (ii) there is a coordinate where u and v agree and w*

is different, another coordinate where v and w agree and u is different, and a third coordinate where w and u agree and v is different.

Of course possibility (i) cannot occur for binary codes.

Proof. We will show that $\mathbf{0}$, $x = v - u$, $y = w - u$ have the stated property. Then u, v, w do also. Either there is a coordinate i such that $x_i \neq 0$, $y_i \neq 0$, $y_i \neq x_i$ (and (i) holds), or, for all i, $x_i \neq 0 \Rightarrow y_i = 0$ or $y_i = x_i$. In the latter case there must be a coordinate j such that $x_j = 0$, $y_j \neq 0$ (or else $x - y$, y do not intersect), a coordinate k such that $x_k \neq 0$, $y_k = 0$ (or else $y - x$, x do not intersect), and a coordinate l such that $x_l \neq 0$, $y_l = x_l$ (or else x, y do not intersect); and (ii) holds.

In the nonbinary case, MDS codes provide good examples of intersecting codes (see Theorem 1(v)). Other examples are given by codes with few weights, cf. [9], but these do not seem to produce efficient 3-coverings. S. Litsyn [39] has pointed out that for large N, algebraic-geometric codes provide good examples of intersecting codes. Let Q be an even power of a prime. Then there are algebraic-geometric codes over the field of order Q with

$$D = \left\lceil \frac{N+1}{2} \right\rceil , \quad \liminf_{N \to \infty} \frac{K}{N} \geq \frac{1}{2} - \frac{1}{\sqrt{Q} - 1} \tag{8}$$

and having a polynomial-time construction [33], [57, Theorem 3.4.15]. These codes are intersecting.

Rather more is known in the binary case.

Theorem 4. *The minimal length $f_2(K)$ of an $[N, K, D]$ binary intersecting code satisfies*

$$c_1 K(1 + o(1)) \leq f_2(K) \leq c_2 K - 2 , \tag{9}$$

where $c_1 = 3.53\ldots$, $c_2 = \frac{2}{2 - \log 3} = 4.8188\ldots$.

Sketch of proof. The lower bound, obtained by Katona and Srivastava [32], follows immediately from Theorem 1(i) and the McEliece-Rodemich-Rumsey-Welch bound for linear codes ([42], [40] Chap. 17). This version of the upper bound is due to Blokhuis and Metsch [5], although essentially equivalent bounds had been given earlier by Komlós (see [14]) and Retter [49]. Blokhuis and Metsch observe that $1 + f_2(K)$ is the minimal number of points needed to block all affine subspaces $AG(K-2, 2)$ in an $AG(K, 2)$. Since each point blocks one quarter of all $AG(K-2, 2)$, we can make sure that after choosing i points at most a fraction $(3/4)^i$ of all $AG(K-2, 2)$ are not blocked. Since the total number of $AG(K-2, 2)$ is less than 4^K, it suffices to take c_2K points, where $c_2 = \log 4/\log(4/3)$. Therefore $1 + f_2(K) < c_2K$. Retter [49] shows that $f(K) = c_2K(1+o(1))$ can be achieved by Goppa codes (although his argument is also nonconstructive).

Table 1 gives the best upper bounds presently known on $f_2(K)$ for small values of K. For $K \leq 6$ the values of $f_2(K)$ are easily proved to be optimal, using Theorems 1(i), 2(ii), 2(iii), and the bounds on the minimal distance of binary linear codes given in [58]. For example, $f_2(5)$ cannot be less than 13 since no $[12, 5, 5]$ linear code exists [6]. The values of $f_2(1), \ldots, f_2(5)$ were first determined in [32]. Conway [16] has shown that $f_2(7) \geq 19$.

Table 1: Minimal length $f_2(K)$ of any $[N, K, D]$ binary intersecting code. The entries for $K \leq 6$ are exact while the remaining entries give upper bounds on $f_2(K)$. Explicit codes are known in every case.

K	$f(K)$	Code
1	1	$\{0, 1\}$
2	3	$[3, 2, 2]$ even weight code
3	6	$[6, 3, 3]$ shortened Hamming code
4	9	Use Theorem 1(iv)
5	13	Omit coordinates 1, 6 from following code
6	15	$[15, 6, 6]$ BCH code [14]
7	21	See Table 2
8	25	See Table 2
9	29	Omit coordinates 1, 2 from following code
10	31	Dual of $[31, 21, 5]$ BCH code [14]
11	41	See Table 2
12	46	
13	51	
14	56	
17	63	Dual of $[63, 46, 7]$ BCH code

Two of the best codes in Table 1 are duals of BCH codes. It seems likely that the duals of some longer BCH codes will also provide good intersecting codes. The obvious approach is to use the Carlitz-Uchiyama bound ([40], p. 280) to guarantee that the weights satisfy condition (iii), but unfortunately the resulting codes are quite weak.

Generator matrices for some of the other codes mentioned in Table 1 are given in Table 2. If the generator matrix has the form $[A\ I]$ then Table 2 gives the rows of A in hexadecimal. The remaining codes in Table 1 may be obtained from the author.

Table 2: Generator matrices $[A\ I]$ for binary intersecting codes.

N	K	D	Rows of A in hexadecimal
21	7	7	35ED, 216E, 38B8, 1389, 2E5D, 339E, 2FF7
25	8	9	001FF, 01FF0, 0333A, 07C3C, 0B996, 0D6B7, 13A77, 14A9D
41	11	11	3C8DF41E, 33EC23BF, 22543C8B, 112FD46A, 14FF5B3D, 2ED72BF9, 3EE1EF78, 0C6EFF07, 357CC3AD, 3D75FADE, 2FFFD2BB

3. Binary 3-covering arrays

In this section we study binary 3-covering arrays, beginning with the asymptotic results. Let $g_t(n)$ denote the minimal size of a binary t-covering array of length n. Then $g_1(n) = 2$, and $g_2(n)$ is determined by (2).

Theorem 5. *As $n \to \infty$,*

$$3.21256\ldots \log n\ (1 + o(1)) < g_3(n) < 7.56444\ldots \log n\ (1 + o(1))\ . \tag{10}$$

Remarks. The lower bound is due to Kleitman and Spencer [34]. The constant is equal to $(H(1/4) - 1/2)^{-1}$, where $H(x) = -x\log x - (1-x)\log(1-x)$. There has been some confusion in the literature concerning this bound. An unfortunate misprint in Eq. (11) of [34] misleadingly suggests that a stronger lower bound has been established, and this error was repeated in [8] and [12].

Kleitman and Spencer also obtain an upper bound of $15.5726 \log n$ by considering random arrays. By using the main result of the Erdös-Frankl-Füredi paper [20] this can be reduced to $11.02 \log n$. A further reduction to $9.6377 \log n$ can be obtained by using the binary intersecting codes whose existence is guaranteed by the right-hand side of (9) in the construction of Theorem 7(i) below. The bound of $7.56444 \log n$ uses an argument due to Roux [50]. Roux actually claims an upper bound of $6.294 \log n$, but this seems to be an arithmetic error. The following is a corrected version of his argument.

Roux defines a $k \times n$ binary array A to be an $\mathcal{E}$*-bad* t-covering array if the number of bad t-tuples, that is, t-tuples of coordinates such that the projection of A onto those coordinates does not include all 2^t possibilities, is at most $\mathcal{E}\binom{n}{t}$.

Proof of upper bound (after Roux [50]). Let $n' = 3n/2$, $k = 2r$. We consider the collection of $k \times n'$ arrays A formed by choosing the columns to be random vectors of length $2r$ and weight r. For any triple $s = s_1 s_2 s_3$ of coordinates and any binary vector $v = v_1 v_2 v_3$, define the random variable $Q_{s,v}(A)$ to be 0 if the projection of A onto s includes v, and to be 1 otherwise. Also let

$$Q(A) = \sum_{s,v} Q_{s,v}(A) \ .$$

If $Q(A) = 0$ then A is 3-covering array, while if $Q(A) < b$ then A is an $\mathcal{E}$-bad 3-covering array with $\mathcal{E} = b/\binom{n'}{3}$.

The probability that $Q_{s,v}(A) = 1$ is equal to

$$\binom{2r}{r}^{-2} \sum_{u=0}^{r} \binom{r}{u}^2 \binom{2r-u}{r} \ .$$

To see this, take for example $s = 123$, $v = 111$, and suppose the first column consists of r 1's followed by r 0's. The number of choices for columns 2 and 3 is $\binom{2r}{r}^2$. Let u be the number of common 1's in columns 1 and 2. $Q_{s,v}(A) = 1$ if and only if the 1's in column 3 are disjoint from these common 1's, an event which can happen in $\binom{r}{u}^2\binom{2r-u}{r}$ ways. The expected value of $Q(A)$ is then

$$8\binom{n'}{3}\binom{2r}{r}^{-2} \sum_{u=0}^{r} \binom{r}{u}^2 \binom{2r-u}{u} \ . \tag{11}$$

We choose r to be the largest integer so that this quantity is less than $n/2$. It follows that there exists a $2r \times n'$ array A which contains at most $n/2$ bad triples. By deleting at most $n/2$ coordinates we can eliminate these bad triples, producing a 3-covering array of size $2r \times n$. The sum in (11) is dominated by the terms near $u = \alpha r$, where $\alpha = (3 - \sqrt{5})/2 = .3819\ldots$, and we find $k = 2r = 7.56444\ldots \log n \ (1 + o(1))$, as claimed. The constant is

$$\frac{4}{4 - 2H(\alpha) - (2-\alpha)H(1/(2-\alpha))} \ .$$

The upper bound in Theorem 5 is nonconstructive. Alon [1] gave an explicit construction of t-covering arrays with $k \le c \log n$, but his constant is extremely large. In the case $t = 3$, Cohen [12] found that the constant in Alon's construction is about 10^{656}. Roux [50] was able to reduce the constant to 10^{256}. The construction using nonbinary intersecting codes given in Theorem 7(ii) produces arrays with a polynomial-time construction and $k \le 12.347 \log n$, as well as explicit arrays with a small constant for a wide range of values of n.

Before leaving the asymptotic theory we mention another result from Roux's thesis that is at first glance quite surprising. For any t and any $\mathcal{E} > 0$ there is a constant k_0 such that $\mathcal{E}$-bad

t-covering arrays of size k_0 exist for all lengths n. The size is independent of the number of columns. For example, at most 68 vectors are needed for an 0.001-bad 3-covering array with any number of columns. The result is easily established by choosing arrays at random and using a probabilistic argument.

Roux also gives two useful bounds.

Theorem 6. (Roux [50])

$$g_{t+1}(n+1) \geq 2g_t(n) \ , \tag{12}$$

$$g_3(2n) \leq g_3(n) + g_2(n) \ . \tag{13}$$

Proof. (12) is clear. (13) Let A, B be arrays achieving $g_3(n)$, $g_2(n)$. Then it is easy to check that

$$\begin{matrix} A & A \\ B & \overline{B} \end{matrix}$$

is a 3-covering array (where the bar indicates the complementary array).

We now give some constructions for 3-covering arrays. The rows of I_n and $\overline{I}_n$ show that $g_3(n) \leq 2n$ for $n \geq 4$. It is also trivial to verify (by computer) that a normalized Hadamard matrix (H_{12}) of order 12 yields a 3-covering array with $n = 11$ and $k = 12$ when the initial column of 1's is deleted and -1's are replaced by 0's. None of the five Hadamard matrices of order 16 produces a 3-covering of length 15 in this way. However, Mallows [41] found that if the first and ninth columns are omitted from the fourth Hadamard matrix of order 16 (B_3 in the notation of Assmus and Key [3]), a 3-covering array is obtained with length 14 and size 16. Kreher and Tonchev [37] observed that the incidence matrix of the nicest 2-$(16,6,2)$ biplane ([10]; [22], Table XVII, No. 5; [27], Table I.1, No. 10), supplemented by $\mathbf{0}$, forms a 3-covering with $n = 16$, $k = 17$. Another array with the same parameters is given in (1).

Theorem 7. *(i) If an* $[N, K, D]$ *binary intersecting code* $\mathcal{C}$ *exists then*

$$g_3(2^K) \leq 2N + 2 \ . \tag{14}$$

(ii) If a 3-surjective array A *exists of size* k_0 *and length* n_0*, where* n_0 *is a prime power, then*

$$g_3(n_0^K) \leq k_0(2K-1) \tag{15}$$

holds for all K *with* $1 \leq K \leq {}^1/_2 n_0 + 1$.

Remark. This is a strengthening of some constructions introduced by Busschbach [8] and also used by Roux [50]. [8] has $2^K - 1$ rather than 2^K in (14), and establishes (15) only under the stricter hypothesis that

$$K \leq \left[\frac{4n_0}{9} \right] + 1 \ . \tag{16}$$

Proof. For part (ii) we let $\mathcal{C}$ be an $[N = 2K-1, K, K]$ MDS intersecting code over the field of order n_0. Such a code exists by Theorem 1(v). For part (i) we set $n_0 = k_0 = 2$, $A = \binom{0\ 1}{1\ 0}$. Then for both parts we arbitrarily label the columns of A by the elements of the field of order n_0, form the $N \times n_0^K$ array whose columns are the codewords of $\mathcal{C}$, and replace every entry of this array by the corresponding column of A. This produces a $k_0 N \times n_0^K$ array. For part (i) we further adjoin the all-0's and all-1's rows. Theorem 3 now implies that the resulting array is a 3-covering.

For example, let us apply Theorem 7(ii) with $n_0 = 11$, $k_0 = 12$. We may take $K = 6$ in (13), and deduce that $g_3(11^6) \leq 132$. This array was also given by Roux, but his claim that it is a 3-covering is unjustified since $K = 6$ violates (16). A second iteration gives

$$g_3(11^{3 \times 11^6}) \leq 132 \times 11^6 \ ,$$

and so on. This sequence of 3-coverings has $k/\log n \approx 6.4$ for $n \leq 10^6$, ≈ 12.719 for $n \leq 10^{5000000}$ (compare with (10)), while, for large n, $k/\log n$ grows as constant $\times \log^* n$, where $\log^* n$ is the number of logarithms needed to reduce n to a number less than 1.

If instead of MDS codes we use the algebraic-geometric codes mentioned in (8), we obtain the following result.

Theorem 8 ([39].) *If there exists a 3-covering array of size k_0 and length n_0, where n_0 is an even power of a prime, then there is an infinite sequence of 3-covering arrays of size k and length n with*

$$\liminf_{n \to \infty} \frac{k}{\log n} \leq \frac{1}{\frac{1}{2} - \frac{1}{\sqrt{n_0} - 1}} \frac{k_0}{\log n_0} \ .$$

The complexity of constructing these arrays grows as a polynomial in n.

For example, using $n_0 = 14641$, $k_0 = 84$ we obtain $k \leq 12.347 \log n \ \ (1 + o(1))$.

The final theorem is due to Kreher [36] and the author.

Theorem 9. *(i) If a binary constant weight code with length N, constant weight W, minimal distance D and containing M codewords exists with $N > 3W$ and $D > W$, then $g_3(M) \leq 2N$.*

(ii) If a Steiner system $S(T,K,V)$ containing $M = \binom{V}{T}/\binom{K}{T}$ blocks exists with $V > 3K$ and $K > 2(T-1)$, then $g_3(M) \le 2V$.

Proof. (i) Let A be the $N \times M$ array whose columns are the codewords. Any two distinct codewords intersect in at most $W - D/2$ coordinates, and since $W > 2(W - D/2)$ this means that in any three columns all of 100, 010, 001 occur. Since $N > 3W$, 000 also occurs. Therefore the rows of A and $\overline{A}$ form a 3-covering array. (ii) is a special case of (i).

The maximal number of codewords in a constant weight code of length N, weight W and minimal distance D is usually denoted by $A(N,D,W)$, and [7] gives extensive tables of lower bounds on this quantity. An entry marked $A(N,D,W)$ or $S(T,K,V)$ in Table 3 indicates an array obtained by applying Theorem 9.

Table 3 summarizes all these results, giving upper bounds on $g_3(n)$ for $n \le 11^6$. If n is missing, the following entry should be used. Explicit arrays are known in every case. It follows from (12) that the entries in Table 3 for $n \le 11$ are exact. However, the author expects that most of the other entries (as well as those in Table 1) can be considerably improved, and offers these tables as a challenge to the reader.

Acknowledgements

I should like to thank David Applegate, Aart Blokhuis, Andries Brouwer, Gérard Cohen, John Conway, Bill Cook, János Körner, Donald Kreher, Simon Litsyn, Colin Mallows, Klaus Metsch and Vladimir Tonchev, all of whom have contributed to this paper.

Table 3: Upper bounds to $g_3(n)$, the minimal number of vectors in a binary 3-covering array of length n. If n is missing, use the following entry.

n	$g_3(n)$	Construction
3	8	$\{0,1\}^3$
4	8	$(1000), (0111)$
5	10	$(10000), (01111)$
11	12	H_{12}
14	16	$H_{16} - 2$ columns
16	17	2-$(16, 6, 2)$ biplane or (1)
20	18	(13)
22	19	(13)
28	23	(13)
30	24	(13)
32	25	(13)
40	26	(13)
44	27	(13)
56	31	(13)
64	32	(14)
70	34	(13)
80	35	(13)
121	36	(15)
128	42	(13)
176	44	$A(22, 8, 7)$
253	46	$S(4, 7, 23)$
254	50	$A(25, 8, 7)$
256	51	(15)
260	52	$S(3, 5, 26)$
361	54	(15)
420	57	(13)
506	58	(13)
1331	60	(15)
1584	73	(13)
2662	74	(13)
14641	84	(15)
22880	101	(13)
29282	102	(13)
161051	108	(15)
184756	128	(13)
322102	129	(13)
1771561	132	(15)

References

[1] N. Alon, "Explicit construction of exponential-sized families of k-independent sets," *Discr. Math.* **58** (1986), 191–193.

[2] D. Applegate, personal communication.

[3] E. F. Assmus, Jr. and J. D. Key, "Hadamard matrices and their designs: a coding theoretic approach," *Trans. Amer. Math. Soc.* to appear.

[4] B. Becker and H.-U. Simon, "How robust is the n-cube?," *Info. Computation* **77** (1988), 162–178.

[5] A. Blokhuis and K. Metsch, personal communication.

[6] A. E. Brouwer, personal communication.

[7] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane and W. D. Smith, "A new table of constant weight codes," *IEEE Trans. Inform. Theory* **36** (1990), 1334–1380.

[8] P. Busschbach, "Constructive methods to solve the problems of s-surjectivity, conflict resolution, coding in defective memories," Report 84D005, École Nationale Supér. Télécomm., Paris, 1984.

[9] A. R. Calderbank and W. M. Kantor, "The geometry of two-weight codes," *Bull. London Math. Soc.* **18** (1986), 97–122.

[10] P. J. Cameron, "Biplanes," *Math. Z.* **131** (1973), 85–101.

[11] A. K. Chandra, L. T. Kou, G. Markowsky and S. Zaks, "On sets of Boolean n-vectors with all k-projections surjective," *Acta. Inform.* **20** (1983), 103–111.

[12] G. D. Cohen, "Applications of coding theory to communication combinatorial problems," *Discr. Math.* **83** (1990), 237–248.

[13] G. D. Cohen, P. Godlewski and M. Karpovsky, "Test exhaustif de circuits combinatoires," *Traitment de Signal* **1** (1984), 223–226.

[14] G. D. Cohen and A. Lempel, "Linear intersecting codes," *Discr. Math.* **56** (1985), 35–43.

[15] G. D. Cohen and G. Simonyi, "Coding for write-directional memories and conflict resolution," *Discr. Appl. Math.* **24** (1989), 103–114.

[16] J. H. Conway, personal communication.

[17] J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups*, Springer-Verlag, NY, 2nd ed., 1992, to appear.

[18] W. Cook, personal communication.

[19] I. I. Dumer, "Asymptotically optimal codes correcting memory defects of fixed multiplicity," *Problemy Peredachi Informatsii* **25** (No. 4, 1989), pp. 3–10. English translation, *Problems of Information Transmission* **25** (1989), 259–265.

[20] P. Erdös, P. Frankl and Z. Füredi, "Families of finite sets in which no set is covered by the union of two others," *J. Combin. Theory*, Ser. A **33** (1982), 158–166.

[21] P. Erdös, C. Ko and R. Rado, "Intersection theorems for systems of finite sets," *Quart. J. Math. Oxford* **12** (1961), 313–318.

[22] R. A. Fisher and F. Yates, *Statistical Tables for Biological, Agricultural, and Medical Research*, Hafner, NY, 6th ed., 1963.

[23] L. Gargano, J. Körner and U. Vaccaro, "Sperner theorems on directed graphs and qualitative independence," *J. Combinatorial Theory* (submitted).

[24] L. Gargano, J. Körner and U. Vaccaro, "Sperner capacities," *Graphs and Combinatorics* (submitted).

[25] L. Gargano, J. Körner and U. Vaccaro, "Capacities: from information theory to extremal set theory," *J. Amer. Math. Soc.* (submitted).

[26] C. Greene, "Sperner families and partitions of a partially ordered set," in *Combinatorics*, ed. M. Hall, Jr. and J. H. van Lint, Reidel, Dordrecht, Holland, 1975, pp. 277–290.

[27] M. Hall, Jr., *Combinatorial Theory*, Wiley, NY, 2nd ed., 1986.

[28] I. S. Honkala, "Modified bounds for covering codes," *IEEE Trans. Information Theory* **37** (1991), 351–365.

[29] I. S. Honkala, "A Graham-Sloane type construction for s-surjective matrices," preprint, 1991.

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

[31] G. O. H. Katona, "Extremal problems for hypergraphs," in *Combinatorics*, ed. M. Hall, Jr. and J. H. van Lint, Reidel, Dordrecht, Holland, 1975, pp. 215–244.

[32] G. O. H. Katona and J. Srivastava, "Minimal 2-coverings of a finite affine space based on $GF(2)$," *J. Stat. Planning Inference* **8** (1983), 375–388.

[33] G. L. Katsman, M. A. Tsfasman and S. G. Vladuts, "Modular curves and codes with a polynomial construction," *IEEE Trans. Information Theory* **30** (1984), 353–355.

[34] D. J. Kleitman and J. Spencer, "Families of k-independent sets," *Discr. Math.* **6** (1973), 255–262.

[35] J. Körner and M. Lucertini, "Compressing inconsistent data," preprint, 1992.

[36] D. L. Kreher, personal communication.

[37] D. L. Kreher and V. D. Tonchev, personal communication.

[38] A. Lempel and S. Winograd, "A new approach to error-correcting codes," *IEEE Trans. Inform. Theory* **23** (1977) 503–508.

[39] S. N. Litsyn, personal communication, 1992.

[40] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[41] C. L. Mallows, personal communication.

[42] R. J. McEliece, E. R. Rodemich, H. C. Rumsey, Jr., and L. R. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Trans. Inform. Theory* **23** (1977) 157–166.

[43] D. Miklós, "Linear binary codes with intersection properties," *Discr. Appl. Math.* **9** (1984), 187–196.

[44] J. Naor and M. Naor, "Small-bias probability spaces: efficient constructions and applications," in *Proc. 20th Annual ACM Symp. Theory of Computing*, ACM Press, 1990, pp. 213–223.

[45] P. R. J. Östergård, "Constructions of mixed covering codes," Report 18, Digital Systems Laboratory, Helsinki Univ. Technology, Dec. 1991.

[46] S. Poljak, A. Pultr and V. Rödl, "On qualitatively independent partitions and related problems," *Discr. Appl. Math.* **6** (1983), 193–205.

[47] S. Poljak and Z. Tuza, "On the maximum number of qualitatively independent partitions," *J. Combin. Theory, Ser.* **A 51** (1989), 111–116.

[48] A. Rényi, *Foundations of Probability*, Wiley, New York, 1971.

[49] C. T. Retter, "Intersecting Goppa codes," *IEEE Trans. Inform. Theory* **35** (1989), 822–828.

[50] G. Roux, "k-propriétés dans des tableaux de n colonnes; cas particulier de la k-surjectivité et de la k-permutivité," Ph.D. Dissertation, University of Paris 6, March 1987.

[51] G. Seroussi and N. H. Bshouty, "Vector sets for exhaustive testing of logical circuits," *IEEE Trans. Information Theory* **34** (1988), 513–522.

[52] G. B. Sherwood, "Constrained Array Test System (CATS) User's Guide," AT&T Bell Laboratories, Middletown, NJ, 1992.

[53] E. Sperner, "Ein Satz über Untermengen einer endlicher Menge," *Math. Z.* **27** (1928), 544–548.

[54] D. T. Tang and C.-L. Chen, "Logic test pattern generation using linear codes," *IEEE Trans. Computers* **33** (1984), 845–850.

[55] D. T. Tang and C.-L. Chen, "Iterative exhaustive pattern generation for logic testing," *IBM J. Res. Dev.* **28** (1984), 212–219.

[56] D. T. Tang and L. S. Woo, "Exhaustive test pattern generation with constant weight vectors," *IEEE Trans. Computers* **32** (1983), 1145–1150.

[57] M. A. Tsfasman and S. G. Vladuts, *Algebraic-Geometric Codes*, Kluwer, Dordrecht, Holland, 1991.

[58] T. Verhoeff, "An updated table of minimum-distance bounds for binary linear codes," *IEEE Trans. Inform. Theory* **33** (1987), 665–680.