The number of linearly independent binary vectors with applications to the construction of hypercubes and orthogonal arrays, pseudo (t, m, s)-nets and linear codes.

S. B. Damelin*, G. Michalski*, G. L. Mullen** and D. Stone*

4 February 2003

Abstract

We study formulae to count the number of binary vectors of length n that are linearly independent k at a time where n and k are given positive integers with $1 \leq k \leq n$. Applications are given to the design of hypercubes and orthogonal arrays, pseudo (t, m, s)-nets and linear codes.

1991 AMS(MOS) Classification: Primary: 11T30; secondary: 05B15.

Keywords and Phrases: Binary Vector, Linear Code, Linear independence, (t, m, s)-net, pseudo (t, m, s)-net, Orthogonal Array, Hypercube, Orthogonal Structure.

1 Introduction

Let $n \geq 1$ be an integer and denote by V_n the n dimensional vector space F_2^n of binary vectors of length n, i.e., those vectors with n entries consisting of 0s and 1s and where arithmetic is performed mod 2. Given a positive integer $k \leq n$, what is the maximum number of vectors we can choose from V_n that are linearly independent k at a time? Before proceeding further, let us pause for a moment to fully appreciate what this question means. It is not hard to see that no matter how we choose our vectors, as long as we avoid the null vector $\overrightarrow{0}$, the chosen vectors will be linearly independent one at a time and in fact, if $n \geq 2$, two at a time as well because our arithmetic is performed mod 2. So the answer to our question for $k = 1, 2$ is $2^n - 1$. What about $k \geq 3$? A nonempty subset of any linearly independent set is by definition itself linearly independent, so in this paper we are interested in studying supersets of maximal lineary independent sets. More precisely, we study closed formulae for the **maximum** number of vectors linearly independent k at a time. We also present several interesting applications of our main result to the construction of hypercubes and orthogonal arrays, pseudo (t, m, s)-nets and linear codes. In order to proceed, we find it necessary to introduce some needed notation. In what follows n and k are integers with $1 \leq k \leq n$.

Definition 1 We will say that a nonempty set $A \subseteq V_n$ is *k-independent*, if every nonempty subset of A that has at most k elements is linearly independent. The family of all k-independent subsets of V_n will be denoted by $V_n(k)$. Our earlier discussion shows that $V_n(1) = \left\{ A \subseteq V_n : \overrightarrow{0} \notin A \right\}$, for $n \geq 1$, and $V_n(2) = V_n(1)$, for $n \geq 2$. Also, it is clear from Definition 1 that $V_n(k_1) \supseteq V_n(k_2)$, whenever $k_1 \leq k_2 \leq n$; i.e., for $n \geq 2$, we have

$$V_n(1) = V_n(2) \supseteq ... \supseteq V_n(n).$$

Note that the least family in this hierarchy, $V_n(n)$, includes all linearly independent subsets of V_n.

In this paper, we are interested in maximum possible sizes of elements of $V_n(k)$, and, to this end, let us define

$$Ind\,(n, k) := \max \{|A| : A \in V_n\,(k)\}\,.$$

We have that $Ind\,(n, 1) = 2^n - 1$ if $n \geq 1$, $Ind\,(n, 2) = Ind\,(n, 1)$ if $n \geq 2$, and for every $n \geq 3$

$$2^n - 1 \geq Ind\,(n, 3) \geq ... \geq Ind(n, n) \geq n + 1. \tag{1.1}$$

(By using the n unit vectors along with the all-ones vector, it is easy to see that $Ind(n, n) \geq n+1$.) In Theorem 2 below we give formulae for $Ind\,(n, 3)$, and for $Ind\,(n, k)$, where $k = n - m$, for some m with $0 \leq m \leq n/3$.

Our main result can be stated as follows.

Theorem 2 The following formulae hold:

(a)
$$Ind\,(n, 3) = 2^{n-1}, \text{ for } n \geq 3. \tag{1.2}$$

(b)
$$Ind\,(n, n - m) = n + 1, \text{ for } n \geq 3m + 2,\ m \geq 0. \tag{1.3}$$

(c)
$$Ind\,(n, n - m) = n + 2, \text{ for } n = 3m + i,\ i = 0, 1,\ m \geq 2. \tag{1.4}$$

Remark 3 We note that it is indeed easy to construct sets of vectors satisfying Theorem 2. For the case $n = 3m + 2$ from (1.3), one can construct the required $n+1$ vectors by simply using the n unit vectors of length n along with the all ones vector of length n to give the required $n + 1$ vectors.

In the cases from (1.4) where $n = 3m$ and $n = 3m + 1$, we start with the set of n unit vectors of length n. In the $n = 3m$ case, we add the two vectors $(1, ..., 1, 0, , ..., 0)$ and $(0, ..., 0, 1, ..., 1)$ where we use $2m$ ones in each case, along with m zeros. The resulting set will then be $n - m$ independent. In the $n = 3m+1$ case, we add the two vectors $(1, ..., 1, 0, ..., 0)$ and $(0, ..., 0, 1, ..., 1)$ where we now use $2m + 1$ ones, and the rest zeros. In this case the set will also be $n - m$ independent.

Remark 4 In [13], Tallini has studied a problem, slightly different to ours, namely counting the maximum number of vectors of length n over F_q, where q is a prime, which are linearly independent k at a time but not $k + 1$ at a time. Let us denote this number by $Ind_q(n, k)$. Clearly, $Ind_2(n, k) \leq Ind(n, k)$. We also refer the interested reader to the detailed survey of Hirschfeld, see [3], for further bounds on $Ind_q(n, k)$ for any prime q.

The remainder of this paper is organized as follows. In Section 2 we present the proof of Theorem 2, and in Section 3 we present some applications of Theorem 2 to the construction of hypercubes and orthogonal arrays, pseudo (t, m, s)-nets and linear codes.

2 The Proof of Theorem 2

In this section, we present the proof of Theorem 2. Throughout n and k are integers with $2 \leq k \leq n$. For any $X \subseteq V_n$, the notation $\sum X$ will denote $\sum_{x \in X} x$, if $X \neq \emptyset$, and $\overrightarrow{0}$ otherwise. Let us also define for $A \subseteq V_n$ and an integer l

$$A^l := \left\{ \sum X : X \subseteq A \,\text{and}\, |X| = l \right\};$$

i.e. $A^0 = \left\{ \overrightarrow{0} \right\}$, $A^l = \emptyset$ if $l < 0$ or $l > |A|$, and if $1 \leq l \leq |A|$, A^l consists of all vectors of the form $a_1 + ... + a_l$, where $a_1, ..., a_l \in A$ are all distinct. Finally, for any set of integers U, let

$$A^U = \bigcup_{l \in U} A^l.$$

In what follows, U will typically be an interval with respect to the natural ordering of the integers.

2.1 The Proof of Theorem 2(b)

In this subsection, we present the proof of Theorem 2(b). Throughout, $\text{span}(A)$ denotes the linear subspace generated by $A \subseteq V_n$.

Lemma 5 Let $A \subseteq V_n$. Then the following statements hold:

(a) $\text{span}(A) = A^{[0,|A|]}$.

(b) A is k-independent if and only if $\overrightarrow{0} \notin A^{[1,k]}$.

(c) If A is a <u>maximal</u> k-independent subset of V_n, then A contains a basis of V_n.

Proof As (a) and (b) are self evident, it suffices to show (c). Consider a maximal linearly independent $B \subseteq A$. Then it follows that $\mathrm{span}\,(B) = V_n$, and thus that B is a basis of V_n, because we have

$$V_n \subseteq A^{[0,k)} \subseteq \mathrm{span}\,(A) \subseteq \mathrm{span}\,(B) \subseteq V_n,$$

where the first inclusion follows from the maximality of A, and the third one from the maximality of B. $\square$

Note that since the property of being k-independent is preserved under isomorphisms, Lemma 5(c) says that in the study of $Ind(n,k)$ one can restrict one's attention to supersets of the canonical basis.

In what follows, we will use the symbol Δ to denote the set-theoretic operation of *symmetric difference*; i.e. for sets X and Y,

$$X\Delta Y := (X - Y) \cup (Y - X) = (X \cup Y) - (Y \cap X)\,.$$

Note that, due to the mod 2 arithmetic, for any $X, Y \subseteq V_n$, we have

$$\sum X + \sum Y = \sum (X\Delta Y)\,. \tag{2.1}$$

Lemma 6 Let $A \subseteq V_n$ and suppose that $k \leq |A|$. Then the following statements are equivalent:

(i) A is k-independent.

(ii) For every $X, Y \subseteq A$, with $1 \leq |X\Delta Y| \leq k$, we have $\sum X \neq \sum Y$.

(iii) Suppose that integers r and l are given with $0 \leq r < l \leq |A|$ and satisfying in addition (1) $l + r \leq k$ or (2) $l + r \geq 2\,|A| - k$. Then

$$A^r \cap A^l = \emptyset.$$

Proof We first show (i) $\Rightarrow$ (ii): We proceed by way of contradiction. Suppose that X and Y are as above but $\sum X = \sum Y$. Then by (2.1), we have

$$\overrightarrow{0} = \sum X + \sum Y = \sum (X\Delta Y) \in A^{|X\Delta Y|} \subseteq A^{[1,k]}.$$

But this, by Lemma 5b, contradicts (i).
(ii) $\Rightarrow$ (iii): Let $X, Y \subseteq A$, $|X| = r < l = |Y|$, where r and l satisfy the hypothesis of (iii). Part (iii) will follow if we can show that $\sum X \neq \sum Y$. To see this, we employ (ii). Clearly, $|X\Delta Y| \geq 1$, so it is enough to show that $|X\Delta Y| = |X - Y| + |Y - X| \leq k$. This is clear if $l + r = |X| + |Y| \leq k$. Moreover if $l + r \geq 2\,|A| - k$ then

$$\begin{aligned} &|X - Y| + |Y - X| \leq |A - Y| + |A - X| = \\ &= |A| - |Y| + |A| - |X| = 2\,|A| - (|X| + |Y|) \leq k. \end{aligned}$$

Thus (iii) holds.
(iii) $\Rightarrow$ (i): Let $1 \leq l \leq k$. By assumption we have

$$\left\{\overrightarrow{0}\right\} \cap A^l = A^0 \cap A^l = \emptyset.$$

But then (i) follows from Lemma 5(b). Lemma 6(iii) is proved. $\Box$

We now record three corollaries of Lemma 6. The first one, a basic fact from linear algebra, allows us to introduce the notion of weight. The other two, interesting in themselves, are needed in the proof of Theorem 2.

Corollary 7 If $A \subseteq V_n$ is linearly independent, then for every $p \in span\,(A)$, there is a $\underline{\text{unique}}$ $P \subseteq A$ so that $p = \sum P$. In particular, the sets $A^0, \ldots, A^{|A|}$ are pairwise disjoint.

Proof This follows from Lemma 6(ii) with $k = |A|$. $\Box$

The unique $P \subseteq A$ as above will be called the A-*support* of p, denoted by $supp_A\,(p)$. The cardinality of $supp_A\,(p)$ will be called the A-*weight* of p, denoted by $|p|_A$. Observe that, by (2.1), we have $supp_A\,(p+q) = supp_A\,(p)\,\Delta supp_A\,(q)$ and, in particular,

$$|p+q|_A = |p|_A + |q|_A - 2\,|supp_A\,(p) \cap supp_A\,(q)|\,. \tag{2.2}$$

Corollary 8 Suppose $B \subseteq W \subseteq V_n$ for some k-independent set W and B with $\text{span}(B) = V_n$. Then, for each $r = 1, \ldots, |W - B|$,

$$(W - B)^r \subseteq B^{(k-r,|B|]}. \tag{2.3}$$

Proof By Lemma 5(a), we know that $V_n = B^{[0,|B|]}$. Suppose first that $r > k$. Then

$$B^{(k-r,|B|]} = B^{[0,|B|]} = V_n.$$

Thus we may assume without loss of generality that $r \leq k$. (2.3) will follow if we can show that for every integer l with $0 \leq l \leq k - r$ we have

$$(W - B)^r \cap B^l = \emptyset. \tag{2.4}$$

If $l \neq r$, (2.4) follows from Lemma 6(iii). Indeed, $l + r \leq k$ and so

$$(W - B)^r \cap B^l \subseteq W^r \cap W^l = \emptyset.$$

If $l = r \leq k - r$, then $2r \leq k$ and we have

$$(W - B)^r \cap B^r = \emptyset$$

by Lemma 6(ii), since if $X \subseteq W - B$, $Y \subseteq B$, and $|X| = |Y| = r \geq 1$, then $1 \leq |X \Delta Y| \leq 2r \leq k$. This completes the proof. $\Box$

Corollary 9 Suppose W contains a basis B of V_n. Then W is k-independent if and only if for each $r = 1, \ldots, |W - B|$,

$$(W - B)^r \subseteq B^{(k-r,|B|]}.$$

Proof Necessity: This is Corollary 8.
Sufficiency: Suppose to the contrary that X is a nonempty subset of W with $|X| \leq k$ and $\sum X = \overrightarrow{0}$. Let $X_1 = X \cap B$ and $X_2 = X - B$. Then $\sum X_1 = \sum X_2$ and since $|X_2| \geq 1$ (B is linearly independent), we have

$$\sum X_1 = \sum X_2 \in (W - B)^{|X_2|} \subseteq B^{(k-|X_2|,|B|]}$$

(the last inclusion follows from the right hand side of the equivalence being proved). In particular, using Corollary 7, we have $|X_1| > k - |X_2|$ and therefore $|X| = |X_1| + |X_2| > k$, which is a contradiction. We have proved Corollary 9. $\square$

We need one final preparatory lemma in order to present the proof of Theorem 2(b). Recall that if $B \subseteq V_n$ is linearly independent, and $p \in span(B)$, then $|p|_B$ and $supp_B\,(p)$ denote, respectively, B-weight and the B-support of p.

Lemma 10 Suppose $B \subseteq V_n$ is linearly independent, and $p, q \in B^{[|B|-m,|B|]}$ for some $m \leq |B|$. Then $|p+q|_B \leq 2m$.

Proof Let p,$q \in B^{[|B|-m,|B|]}$, $P = supp_B\,(p)$ and $Q = supp_B\,(q)$. We then have

$$\begin{aligned} |p+q|_B &= |P \Delta Q| \leq (|B| - |P|) + (|B| - |Q|) \\ &= 2\,|B| - (|P| + |Q|) \leq 2\,|B| - 2\,(|B| - m) = 2m \end{aligned}$$

as required. $\square$

We are ready for the

Proof of Theorem 2(b) We first establish that $Ind(n, n-m) \leq n+1$. Suppose that $n \geq 3m+2$ and W is a maximal $(n-m)$-independent subset of V_n. By maximality, W contains a basis B of V_n (cf. Lemma 5(c)). On the other hand by Corollary 8 (with $r = 1$), we have $(W - B) \subseteq B^{[n-m,|B|]}$. Thus to complete the proof, it is enough to show that

$$\left| W \cap B^{[n-m,|B|]} \right| < 2. \tag{2.5}$$

Suppose $p, q \in W \cap B^{[n-m,|B|]}$. Let $A = supp_B\,(p+q)$. By Lemma 10, $|A| \leq 2m$. Therefore, either $p = q$, or else $A \cup \{p, q\}$ is a linearly dependent subset of W with no more than $2m+2$ elements. However, the latter cannot happen since W is $(n-m)$-independent, and

$$2m + 2 = (3m+2) - m \leq n - m.$$

This proves (2.5) and so $Ind(n, n-m) \leq n+1$. To prove $Ind(n, n-m) \geq n+1$, let B be a basis for V_n. By Corollary 7, $W := B \cup \{\sum B\}$ is n-independent and thus $(n-m)$-independent. This completes the proof of Theorem 2(b). $\square$

2.2 The Proof of Theorem 2(c)

In this subsection we present the proof of Theorem 2(c). In what follows, we present two further auxiliary results which we require for our proof.

Lemma 11 Suppose $B \subseteq V_n$ is linearly independent and p and q are elements of *span* (B) with $|p|_B = r \leq s = |q|_B$. Then

$$|p+q|_B = 2j + (s-r), \tag{2.6}$$

for some j with $0 \leq j \leq \min\{r, |B| - s\}$.

In particular:

(a) If $r = s = 2m + i$, then

$$p + q \in B^{2m} \text{ if and only if } |P \cap Q| = m + i. \tag{2.7}$$

(b) If $r = 2m$ and $s = 2m + 1$, then

$$p + q \in B \text{ if and only if } |P \cap Q| = 2m. \tag{2.8}$$

Proof Let $P = supp_B(p)$ and $Q = supp_B(q)$. Then by (2.2)

$$|p+q|_B = |P \Delta Q| = r + s - 2|P \cap Q| = 2(r - |P \cap Q|) + (s - r).$$

Moreover, $\max\{0, r + s - |B|\} \leq |P \cap Q| \leq r$, which implies that $0 \leq r - |P \cap Q| \leq \min\{r, |B| - s\}$. This establishes the result. The statements (2.7) and (2.8) follow from (2.6) where $j = r - |P \cap Q|$. $\square$

Lemma 12 Suppose that $n = 3m + i, m \geq 2$, and $i = 0, 1$. Let $W \subseteq V_n$ be $(n-m)$-independent and suppose that $B \subseteq W$ is a basis for V_n. Then the following statements hold:

(a) If x and y are two distinct elements of W such that $2m + i \leq |x|_B \leq |y|_B$, then:

 (I) $|x|_B = |y|_B = 2m + i$ and $|x + y|_B = 2m$ or

 (II) $|x|_B = 2m$, $|y|_B = 2m + 1$ and $|x + y|_B = 2m - 1$.

 Moreover, (II) is possible *only* if $i = 0$.

(b) If x and y are as in (a), then $|supp_B(y) - supp_B(x)| = m$.

(c) $\left|W \cap B^{[2m+i,|B|]}\right| \leq 2$.

Proof We first prove Lemma 12(a). Let x and y be as in the hypothesis. We can write $|x|_B = 2m + i_x$ and $|y|_B = 2m + i_y$, for some $i_x, i_y \leq m + i$ such that

$$i \leq i_x \leq i_y. \tag{2.9}$$

By Lemma 11 we deduce that

$$|x+y|_B = 2j + (i_y - i_x) \tag{2.10}$$

for some $j \le \min\{|x|_B, 3m+i-|y|_B\} = m+i-i_y$. In particular, we have

$$|x+y|_B \le 2(m+i-i_y) + (i_y - i_x) = 2(m+i) - (i_x + i_y). \tag{2.11}$$

On the other hand, using Corollary 8, we have $|x+y|_B > 2m+i-2$ (since $x+y \in (W-B)^2$) and therefore combining this last observation with (2.11), we learn that

$$2m+i-2 < |x+y|_B \le 2(m+i) - (i_x+i_y). \tag{2.12}$$

In particular, we deduce that

$$i_x + i_y < i+2. \tag{2.13}$$

Suppose first that $i_x = i_y$. Then by (2.9) and (2.13), $i \le i_x < \frac{i}{2}+1$, so we have $i_x = i_y = i$, which together with (2.12) yields (I) (note that by (2.10), $|x+y|_B$ is even). On the other hand, if $i_x < i_y$, then (2.9) and (2.13) imply that $i \le i_x < i_y < 2$; i.e. $i = i_x = 0$ and $i_y = 1$, which implies (II). We have also demonstrated that (II) is possible only if $i=0$. Lemma 12(a) is thus proved.

We now proceed with the proof of Lemma 12(b). Let $X = supp_B(x)$ and $Y = supp_B(y)$. By Lemma 12(a), $|X| = 2m+i$ and

$$|Y| + |X\Delta Y| = |y|_B + |x+y|_B = 4m+i.$$

We deduce that

$$\begin{aligned}4m+i &= |Y| + |X\Delta Y| = |Y| + |X| + |Y| - 2|X\cap Y| = \\ &= 2|Y| + 2m + i - 2|X \cap Y|.\end{aligned}$$

Thus

$$2m = 2(|Y| - |X\cap Y|) = 2|Y-X|.$$

This last statement establishes Lemma 12(b).

Finally, we prove Lemma 12(c). We proceed by way of contradiction. Suppose, to the contrary, that p, q, r are three distinct elements of $W \cap B^{[2m+i,|B|]}$. It suffices to show that

$$|r+p+q|_B \le 1. \tag{2.14}$$

Indeed, this will yield a contradiction, since, by Corollary 8, $|r+p+q|_B > 2m+i-3 \ge i+1 \ge 1$ ($m \ge 2$). Thus we establish (2.14). Firstly, by Lemma 10(a), at least two of the three vectors, say p and q are in B^{2m+i}, and the other one, r, is in $B^{[2m+i,2m+1]}$. Let $P = supp_B(p)$, $Q = supp_B(q)$ and $R = supp_B(r)$. By Lemma 12(a)

$$|P\Delta Q| = |p+q|_B = 2m, \tag{2.15}$$

so by Lemma 11(a), $|P \cap Q| = m+i$. This implies that $S := \{P - Q, Q - P, P \cap Q\}$ forms a partition of B, in which the first two sets have m elements each. Since by Lemma 12(a), $|R - P| = |R - Q| = m$, this means that the first two elements of S are subsets of R; i.e.

$$(P \Delta Q) \subseteq R. \tag{2.16}$$

Also, by (2.15), since $|R| \leq 2m+1$, R has at most one element in $P \cap Q$. Therefore, using (2.16), we get

$$|r + p + q|_B = |R \Delta (P \Delta Q)| = |R - (P \Delta Q)| = |R \cap (P \cap Q)| \leq 1.$$

(The third equality follows from the fact that S covers V_n.) This establishes (2.14), and completes the proof of Lemma 8. □

We are ready for:

The Proof of Theorem 2(c) We first prove that $Ind(n, n-m) \leq n+2$. Suppose that W is a maximal $(n-m)$-independent subset of V_n. By maximality, W contains a basis B of V_n (cf. Lemma 5(c)). Moreover, by Corollary 8, $(W - B) \subseteq B^{[2m+i, |B|]}$, so the required inequality follows from Lemma 12.

To prove $Ind(n, n-m) \geq n+2$, consider a basis B of V_n, with $p, q \in B^{2m+i}$ such that $p + q \in B^{2m}$. Corollary 9, then, will imply that $W = B \cup \{p, q\}$ is $(2m+i)$-independent. To see that p and q as above exist, take any partition $\{X, Y, Z\}$ of B, with $|X| = |Y| = m$ and $|Z| = m+i$. Let $p = \sum (X \cup Z)$ and $q = \sum (Y \cup Z)$. [For example, working with the canonical basis, we can let $p = (1, \ldots, 1, 0, \ldots, 0)$ and $q = (0, \ldots, 0, 1, \ldots, 1)$, where either block of 1's is of length $2m+i$.] □

2.3 The Proof of Theorem 2(a)

We complete this section with the proof of Theorem 2(a). We remark that although this result follows from [13, 4], we provide a full independent proof for the reader's convenience.

Proof of Theorem 2(a) Let E denote the set of binary vectors in V_n of even weight. It is easy to see that E is an additive subgroup of V_n. Thus if $a \in V_n$ is of odd weight, an easy application of Lagrange's theorem gives that

$$|E| = |a + E| = \frac{2^n}{2} = 2^{n-1}.$$

Thus in V_n, there are 2^{n-1} vectors of even weight and 2^{n-1} vectors of odd weight. Now let

$$W := \{u \in V_n : u \text{ has odd weight}\}.$$

We claim that W is 3-independent. Let a, b and c be in W. If these are not independent, then $c = a + b$, but this would make c have even weight (c.f (2.2)) which is an obvious contradiction. This shows that $Ind(n, 3) \geq 2^{n-1}$. Now we show that indeed we have equality. It suffices to show the following:

Suppose that $G \subseteq V_n$ contains one more than half of V_n, i.e. $|G| = 2^{n-1} + 1$. Then G contains 3 elements which are dependent. To see this, first observe that G has at least one element of odd weight and one of even weight. Let $G = E \cup \theta$ be a partition of G into even and odd weight vectors. Let a be an element of θ and write $|E| = t$ and $|\theta| = s$ so that $|G| = |E| + |\theta| = t + s = 2^{n-1} + 1$. Now consider the set

$$A = \{a + e \mid e \in E\}.$$

Because A has the same cardinality as E, $|A| = |E| = t$. Moreover, each element of A has odd weight. If some $a + e \in \theta$, then a, $a + e$ and e are in G and we are done. However if no element of A is in θ, then $A \cap \theta = \emptyset$ and so we conclude that

$$|A \cup \theta| = |A| + |\theta| = t + s = 2^{n-1} + 1.$$

But $A \cup \theta$ is a subset of all vectors in V_n of odd weight which means that $|A \cup \theta| \leq 2^{n-1}$ which is a contradiction. Thus indeed $Ind(n, 3) = 2^{n-1}$. □

3 Applications

A classic 1938 result of R. C. Bose in the theory of mutually orthogonal latin squares (MOLS), see [1], demonstrated an equivalence between complete sets of MOLS of a given order and affine planes of the same order; also see [6] for further related results. This result has inspired much research on generalizations to other combinatorial objects with applications in areas as diverse as coding theory, combinatorial designs, numerical integration and random number generation. We refer the interested reader to the survey [6] and the references cited therein for a detailed account of this fascinating subject. In this section, we will give an application of the results of Theorem 2 to the construction of hypercubes and orthogonal arrays, pseudo (t, m, s)-nets and linear codes.

3.1 Orthogonal Arrays and Hypercubes.

A *hypercube* of dimension n and order b is an array containing b^n cells, based upon b distinct symbols arranged so that each of the b symbols appears the same number of times, namely $b^n/b = b^{n-1}$ times. For $2 \leq k \leq n$, a set of k such hypercubes is said to be k-*orthogonal* if upon superpositioning of the k hypercubes, each of the b^k distinct ordered k-tuples appears the same number of times, i.e $b^n/b^k = b^{n-k}$ times. Finally a set of $r \geq k$ such hypercubes is said to be k-*orthogonal* if any subset of k hypercubes is k-orthogonal. When $k = 2$ this reduces to the usual notion of pairwise or mutually orthogonal latin squares of order b. See [8], [9] and [10] for further discussion related to sets of orthogonal hypercubes, and in particular, sets of k-orthogonal hypercubes.

Using our constructions for a set of k independent binary vectors of length n, we can build sets of k-orthogonal hypercubes of dimension n. Assume that $Ind(n, k) = s$, and let $a_1x_1 + \cdots + a_nx_n$ denote a vector of length n in $B_n(k)$, a set of k-independent vectors of length n. One can then construct a binary hypercube C of dimension n by placing the F_2 field element $a_1b_1 + \cdots + a_nb_n$ in the cell of the cube C labelled by $(b_1, \ldots, b_n)$, where each $b_i \in F_2$. Since each vector in $B_n(k)$ has at least one nonzero coefficient $a_i = 1$, and since the equation $x_i = b$ has exactly 2^{n-1} solutions in F_2^n, it is clear that each such vector represents a binary hypercube of dimension n. Moreover, given k such vectors from $B_n(k)$, the corresponding hypercubes will be k-orthogonal. Since the k vectors are k-independent, this follows from the fact that the $k \times n$ matrix obtained from the coefficients of the k vectors will have rank k. Hence each element of F_2^n will be obtained exactly 2^{n-k} times, so that the k hypercubes of dimension n are indeed k-orthogonal.

We remind the reader that an *orthogonal array* of size N, s constraints, b levels, strength k and index λ is an $s \times N$ array A with entries from a set of b distinct elements with the property that any $k \times N$ subarray of A contains all possible $k \times 1$ columns with the same frequency λ. Such an array will be denoted by $OA(N, s, b, k)$. In Theorem 13 of [8] the following result is given. Let $b \geq 2, s \geq k \geq 2$, and $t \geq 0$ be integers. Then there exists an orthogonal array $OA(b^{t+k}, s, b, k)$ of index b^t if and only if there exist s, k-orthogonal hypercubes of dimension $t + k$ and order b.

Hence if $n = 3m+2, m \geq 0$, from Theorem 2 we can construct an $OA(2^n, n+1, 2, n-m)$ of index 2^m. Similarly if $n = 3m+i, i = 0, 1, m \geq 2$, we can construct an $OA(2^n, n+2, 2, n-m)$ of index 2^m.

3.2 Pseudo (t, m, s)-nets

In this subsection we briefly discuss a connection between sets of k-independent vectors and (t, m, s)-nets and pseudo (t, m, s)-nets. For a fixed integer $s \geq 1$, an *elementary interval in base* $b \geq 2$ is an interval of the form

$$E = \prod_{i=1}^{s} [a^{(i)} b^{d_i}, (a^{(i)} + 1) b^{d_i})$$

with integers $d_i \geq 0$ and integers $0 \leq a^{(i)} < b^{d_i}$ for $1 \leq i \leq s$. Given an integer m with $m \geq t \geq 0$, a (t, m, s)*-net in base* b is a point set of b^m points in $[0, 1)^s$ such that every elementary interval E of volume b^{t-m} contains exactly b^t points. It is well known, see for example [11], that (t, m, s)-nets are useful in numerical analysis; in particular in the approximation of multi-dimensional integrals.

As shown in [10] and stated again in [8], if $k = 2$, an orthogonal array $OA(b^{t+2}, s, b, 2)$ of index b^t is equivalent to a $(t, t + 2, s)$-net in base b. As indicated in [4] for $k \geq 3$, orthogonal arrays are however, not equivalent to $(t, t + k, s)$-nets. Orthogonal arrays are in fact equivalent to so called pseudo nets which are structures with less uniformity in the distribution of the points than in a (t, m, s)-net. A pseudo net in base b has the same definition as a (t, m, s)-net in base b except that only a restricted subset of the elementary intervals is required to contain the proper share of points.

More specifically, as defined in [4], a point set of b^m points in $[0,1)^s$ is a *pseudo* (t,m,s)*-net in base* b if every elementary interval of volume b^{t-m} satisfying either

(i) all $d_i \in \{0,1\}$, or

(ii) $d_i \neq 0$ for exactly one $i, 1 \leq i \leq s$

contains exactly b^t points of the point set. In addition, a set of b^m points in $[0,1)^s$ is a *weak pseudo (t,m,s)-net in base* b if every elementary interval of volume b^{t-m} satisfying (i) contains exactly b^t points of the point set.

We have shown that given a set of $s = Ind(n,k)$, k-independent vectors of length $n = t+k$, we can construct a set of s, k-orthogonal hypercubes of dimension $t+k$ and order 2. By [8, Theorem 13] such a collection of hypercubes is equivalent to an orthogonal array $OA(2^{t+k}, s, 2, k)$ of index 2^t. From [4, Corollary 3.3.2], the existence of an $OA(2^{t+k}, s, 2, k)$ is equivalent to the existence of a pseudo $(t, t+k, s)$-net in base 2. Hence from [4, Corollary 3.3.9] we have:

Theorem 13 If $s = Ind(n,k)$, then each of the following equivalent objects can be constructed.

(1) A set of s, k-orthogonal hypercubes of dimension $t+k$ and order 2.

(2) An orthogonal array $OA(2^{t+k}, s, 2, k)$ of index 2^t.

(3) A pseudo $(t, t+k, s)$-net in base 2.

(4) A weak pseudo $(t, t+k, s)$-net in base 2.

Remark 14: Since our construction of sets of k-independent vectors deals only with the case $b = 2$, we have stated Theorem 13 only for the $b = 2$ case. We note however that given a set of $s\prime$, k-independent vectors of length $t+k$ over the finite field of b elements where b is any prime power, one will have proved the existence of each of the above equivalent combinatorial objects in which s is replaced by $s\prime$ and 2 is replaced by b.

3.3 Linear Codes

It is known that a *linear code* C with a parity check matrix H has minimum distance $d_C \geq s+1$ if and only if any s columns of H are linearly independent; see Lemma 9.14 of [7]. We can thus construct a binary linear code C with length $Ind(n,k)$, dimension $Ind(n,k) - n$, and minimum distance $d_C \geq k+1$. Hence from Theorem 1, part (c), if $n = 3m+i, i = 0,1, m \geq 2$, we can construct a binary linear code C_n of length $n+2$, dimension 2, and minimum distance $d_{C_n} \geq n - m + 1$. We note in passing that while the resulting code C_n has a very small dimension, it has a large minimum distance.

3.4 An Example

As an illustration, if $n = 6 = 3(2)$ so that $m = 2$, from Theorem 2, we know that $Ind(6, 4) = 8$. Moreover the following set of 8 vectors of length 6 is 4-independent.

$$\begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array}.$$

From the discussion above we can thus construct a set of 8 binary hypercubes each of dimension 6, which are 4-orthogonal as well as an orthogonal array $OA(2^6, 8, 2, 4)$ of index 2^2. Moreover, we can also construct a binary linear code C with parameters $[8, 2, d_C \geq 5]$.

Acknowledgments The first author acknowledges time spent at The Pennsylvania State University during the 1999-2000 academic year, where part of this research was carried out. The first author's research is supported, in part, by a 2002 Summer Research award from Georgia Southern University. The authors thank B. McLean, J. Solomon and G. Watson for helpful discussions.

References

[1] R. C. Bose, *On the application of the properties of Galois fields to the problem of construction of hyper-Graeco latin squares*, Sankhya **3**(1938), pp. 323-338.

[2] A. T. Clayman, K. M. Lawrence, G. L. Mullen, H. Niederreiter and N. J. A. Sloane, *Updated tables of paramaters of* (t, m, s)*-nets*, J. Combin. Designs **7**(1999), pp. 381-393.

[3] J. W. P. Hirschfeld, *Maximum sets in finite projective spaces*, Surveys In Combinatorics, London Math. Soc. Lecture Note Series **82**, Cambridge University Press, Cambridge, 1983, pp. 55–76.

[4] K. M. Lawrence, *Combinatorial Bounds and Constructions in the Theory of Uniform Point Distributions in Unit Cubes, Connections with Orthogonal Arrays and a Poset Generalization of a Related Problem in Coding Theory*, Ph.D. Thesis, University of Wisconsin, 1995.

[5] K. M. Lawrence, A. Mahalanabis, G. L. Mullen and W. Schmid, *Construction of digital* (t, m, s)*-nets from linear codes*, Finite Fields and Applications, (S.D.Cohen and H. Niederreiter Eds.), Lecture Note Series of the London Math Soc.,**233**(1996), Cambridge University Press, pp. 189-208.

[6] C. F. Laywine and G. L. Mullen, *A hierarchy of complete orthogonal structures*, Ars Combinatoria, **63**(2002), pp. 75-88.

[7] R. Lidl and H. Niederreiter, *Finite Fields*, Sec. Ed., Encyclo. Math. and Appl., Vol. 20, Cambridge Univ. Press, 1997.

[8] G. L. Mullen, *Orthogonal hypercubes and related designs*, J. Statist. Planning and Inference, 73(1998), pp. 177-188.

[9] G. L. Mullen and W. C. Schmid, *An equivalence between* (t, m, s)*-nets and strongly orthogonal hypercubes*, J. Combinatorial Theory, Ser. A**76**(1996), pp. 164-174.

[10] G. L. Mullen and G. Whittle, *Point sets with uniformity properties and orthogonal hypercubes*, Monatsh. Math. 113(1992), pp. 265-273.

[11] H. Niederreiter, *Point sets and sequences with small discrepancy*, Monatsh. Math. **104**(1987), pp. 273-337.

[12] W. R. Scott, *Group Theory*, Dover publications, New York, 1987.

[13] G. Tallini, *Le geometrie di Galois e le loro applicazioni alla statistica e alla teoria dell'informazione*, Rendiconti di Matematica (3-4), **19**(1960), pp. 379-400.

* Department of Mathematics and Computer Science, Georgia Southern University, Post Office Box 8093, Statesboro, GA 30460, U. S. A
(1) Email address: damelin@gsu.cs.gasou.edu
(2) Email address: gmichals@gsaix2.cc.gasou.edu
(3) Email address: drstone@gsvms2.cc.gasou.edu
** Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, U. S. A
Email address: mullen@math.psu.edu.