THE CARDINALITY OF SETS OF k-INDEPENDENT VECTORS OVER FINITE FIELDS

By

S.B. Damelin

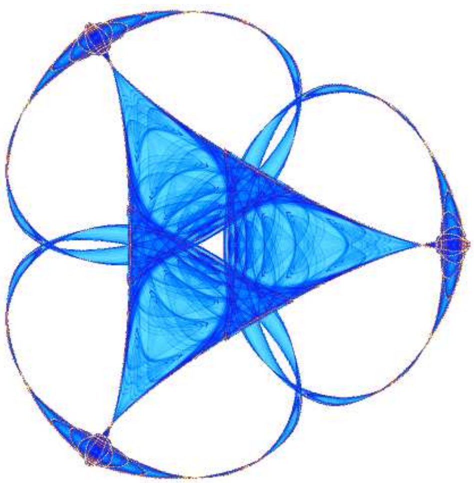
G. Michalski

and

G.L. Mullen

IMA Preprint Series # 2066

(October 2005)



INSTITUTE FOR MATHEMATICS AND ITS APPLICATIONS

UNIVERSITY OF MINNESOTA

400 Lind Hall

207 Church Street S.E.

Minneapolis, Minnesota 55455–0436

Phone: 612/624-6066 Fax: 612/626-7370

URL: http://www.ima.umn.edu

The Cardinality of Sets of k-Independent Vectors over Finite Fields

S. B. Damelin[*], G. Michalski and Gary L. Mullen

Abstract

A set of vectors is k-independent if all its subsets with no more than k elements are linearly independent. We obtain a result concerning the maximal possible cardinality $Ind_q(n, k)$ of a k-independent set of vectors in the n-dimensional vector space F_q^n over the finite field F_q of order q. Namely, we give a necessary and sufficient condition for $Ind_q(n, k) = n + 1$.

1 Introduction

For q a prime power, let F_q denote the finite field of order q, and let F_q^n denote the n-dimensional vector space of all n-tuples over F_q. For $k \geq 1$ an integer, we say that a set of vectors $A \subseteq F_q^n$ is **k-independent** if all its subsets with at most k elements are linearly independent. We are interested in the maximal possible cardinality, $Ind_q(n, k)$, of a k-independent subset of F_q^n. Clearly $(k + 1)$-independence implies k-independence, and since any set of $n + 1$ vectors in a vector space of dimension n must be linearly dependent, we can assume that $1 \leq k \leq n$. We clearly have

$$q^n - 1 = Ind_q(n, 1) \geq Ind_q(n, 2) \geq \cdots \geq Ind_q(n, n) \geq n + 1.$$

It is not hard to see that the last inequality in the sequence above holds because we can use the n unit vectors and the all ones vector of length n

[*]Supported, in part by grants EP/C000285 and NSF-DMS-0439734. S.B. Damelin thanks the Institute for Mathematics and Applications for their hospitality.

over F_q to form an n-independent set containing $n+1$ vectors. On the other hand, the first inequality above becomes an equality when $q = 2$, for over F_2, 2-independence is equivalent to 1-independence. Actually, a general formula for $Ind_q(n, 2)$ is not hard to find. Recalling that any two vectors are linearly independent over a field if and only if they are not scalar multiples of each other, we have

Observation 1. *Let q be a prime power, and $n \geq 1$ an integer. Then*

$$Ind_q(n, 2) = \frac{q^n - 1}{q - 1}. \tag{1.1}$$

Using the n unit vectors and the all ones vector of length n over F_q, it is easy to see that $Ind_q(n, k) \geq n + 1$ for any k with $1 \leq k \leq n$.

In [1], the authors investigated formulae for $Ind_2(n, k)$ in two extreme cases: they first noted the well known formula for the case when $k = 3$. More importantly, they considered the case when $k \geq 2n/3$. The results from [1] are stated in the theorem below, where m and n are positive integers.

Theorem 1. *The following formulae hold:*

(a)
$$Ind_2(n, 3) = 2^{n-1}, \text{ for } n \geq 3. \tag{1.2}$$

(b)
$$Ind_2(n, n-m) = n + 1, \text{ for } n \geq 3m + 2, \; m \geq 0. \tag{1.3}$$

(c)
$$Ind_2(n, n-m) = n + 2, \text{ for } n = 3m + i, \; i = 0, 1, \; m \geq 2. \tag{1.4}$$

In this paper we generalize the result stated in part (b) of Theorem 1. We present a simple condition on q, n and k which is both necessary and sufficient for $Ind_q(n, k) = n + 1$ to hold.

Our main result is the following:

Theorem 2. *Let q be a prime power, and let k and n be integers with $2 \leq k \leq n$. Then $Ind_q(n, k) = n + 1$ if and only if*

$$k \geq \frac{q}{q+1}(n+1)$$

In particular, in the case $q = 2$, Theorem 2 says that the inequality in Theorem 1 (b) is not only sufficient, but also necessary.

We note that our current result (Theorem 2) is most effective when the prime power q is small. For example when $q = 2$ and n is large, we are able to determine the value of $Ind_2(n, k)$ for many values of k, in particular for all k in the range $(2n + 2)/3 \leq k \leq n$.

2 k-Extensions and k-Closures

Clearly, when calculating $Ind_q(n, k)$, we can restrict our attention to **maximal** k-independent sets; i.e. those k-independent sets that don't have proper supersets that are still k-independent.

Observation 2. *Every maximal k-independent set contains a basis of F_q^n over F_q.*

Proof. For $X \subseteq F_q^n$, we use $span\,(X)$ to denote the linear subspace generated by X. If $A \subseteq F_q^n$ is maximal k-independent then every element of F_q^n is a linear combination of (less than k) elements of A; i.e. $span\,(A) = F_q^n$. Consider a maximal linearly independent $B \subseteq A$. If follows (by maximality of B) that $A \subseteq span\,(B)$, and therefore $F_q^n = span\,(A) \subseteq span\,(B)$; i.e. B is a basis of F_q^n. □

Since k-independence is preserved by automorphisms of F_q^n, in the light of Observation 2, while studying $Ind_q(n, k)$ we can restrict our attention even further, namely to the supersets of the standard basis, which we denote by B. We shall say that a set $W \subseteq F_q^n$ is a k**-extension** (of B) if W is disjoint from B, and $W \cup \mathsf{B}$ is k-independent; if $W \cup \mathsf{B}$ is *maximal* k-independent then W will be called a k**-closure** (of B). Let $Cls_q(n, k)$ denote the maximal possible cardinality of a k-closure in F_q^n. The above remarks imply that

$$Ind_q(n, k) = n + Cls_q(n, k). \tag{2.1}$$

Theorem 2 determines exactly for which q, n and k, singletons are the only possible nonempty k-extensions of the standard basis B, and therefore, the only possible k-closures in F_q^n; i.e. for which q, n and k we have $Cls_q(n, k) = 1$.

3 The Proof of Theorem 2

Throughout this section q is a prime power, and n and k are integers with $2 \le k \le n$. We will need the following notation.

For $\mathbf{a} = (a_1, \ldots, a_n) \in F_q^n$, $\mathrm{supp}(\mathbf{a})$ will denote the *support* of the vector $\mathbf{a}$, i.e. the set $\{i : a_i \neq 0, i = 1, \ldots, n\}$; the cardinality of this set will be denoted by $\|\mathbf{a}\|$. ($\|\ \| : F_q^n \to R^+$ satisfies the usual norm conditions, where the absolute value is replaced by the trivial valuation on F_q. In particular, $\|\alpha\mathbf{a}\| = \|\mathbf{a}\|$, for every $\alpha \in F_q^*$.)

We use $|X|$ to denote the cardinality of the set X; and if x is a real number, $\lfloor x \rfloor$ and $\lceil x \rceil$ denote the largest integer not larger than x, and the smallest integer not smaller than x, respectively. We begin with a characterization of k-extensions in terms of $\|\ \|$.

Lemma 1. *Suppose that $W \neq \emptyset$ is disjoint from the standard basis B. Then W is a k-extension if and only if for every nonempty $U \subseteq W$ and $\{\alpha_\mathbf{u} : \mathbf{u} \in U\} \subseteq F_q^*$, we have*

$$\left\| \sum_{\mathbf{u} \in U} \alpha_\mathbf{u} \mathbf{u} \right\| > k - |U|.$$

Proof. Suppose first that W is a k-extension, and let

$$\mathbf{w} = \sum_{\mathbf{u} \in U} \alpha_\mathbf{u} \mathbf{u}$$

be as above. By expanding $\mathbf{w}$ in the standard basis we get

$$\mathbf{w} = \sum_{\mathbf{u} \in U} \alpha_\mathbf{u} \mathbf{u} = \sum_{\mathbf{v} \in C} \beta_\mathbf{v} \mathbf{v}$$

for some $C \subseteq \mathsf{B}$, with $|C| = \|\mathbf{w}\|$, and $\beta_\mathbf{v} \in F_q^*$, for $\mathbf{v} \in C$. It follows that $U \cup C$ is a linearly dependent subset of the k-independent set $W \cup \mathsf{B}$, and therefore its cardinality $|U \cup C| = |U| + \|\mathbf{w}\|$ must be greater than k; i.e. $||\mathbf{w}|| > k - |U|$, as required.

Next, suppose that W is not a k-extension, (i.e. $W \cup \mathsf{B}$ is not k-independent). Then for some $U \subseteq W, C \subseteq \mathsf{B}$ with $|U| + |C| \le k$, and some $\alpha_\mathbf{u}, \beta_\mathbf{v} \in F_q^*$, for $\mathbf{u} \in U$ and $\mathbf{v} \in C$, we have

$$\sum_{\mathbf{u} \in U} \alpha_\mathbf{u} \mathbf{u} + \sum_{\mathbf{v} \in C} \beta_\mathbf{v} \mathbf{v} = \mathbf{0}.$$

In particular,

$$\left\|\sum_{\mathbf{u}\in U}\alpha_{\mathbf{u}}\mathbf{u}\right\| = \left\|-\sum_{\mathbf{v}\in C}\beta_{\mathbf{v}}\mathbf{v}\right\| = |C| \leq k-|U|. \qquad \square$$

Lemma 1 will be used in the proof of Theorem 2 through the following corollary.

Corollary 1.

(a) *If W is a k-extension then $\|\mathbf{a}\| \geq k$, for every $\mathbf{a} \in W$.*

(b) *A singleton $\{\mathbf{a}\} \subseteq F_q^n - B$ is a k-extension if and only if $\|\mathbf{a}\| \geq k$.*

(c) *Suppose $\mathbf{a}, \mathbf{b} \in F_q^n - B$ are distinct. Then $\{\mathbf{a}, \mathbf{b}\}$ is a k-extension if and only if $\|\mathbf{a}\|, \|\mathbf{b}\| \geq k$ and $\|\alpha\mathbf{a}+\beta\mathbf{b}\| \geq k-1$, for all $\alpha, \beta \in F_q^*$.*

(d) *Suppose $W \subseteq F_q^n - B$ consists of vectors with pairwise disjoint supports. Then W is a k-extension if and only if $\|\mathbf{a}\| \geq k$, for every $\mathbf{a} \in W$.*

Proof. The proofs of parts (a), (b), and (c) are straightforward from Lemma 1. In proving part (d) we use the fact that if U consists of vectors with pairwise disjoint supports then for every $\{\alpha_{\mathbf{u}} : \mathbf{u} \in U\} \subseteq F_q^*$

$$\left\|\sum_{\mathbf{u}\in U}\alpha_{\mathbf{u}}\mathbf{u}\right\| = \sum_{\mathbf{u}\in U}\|\alpha_{\mathbf{u}}\mathbf{u}\| = \sum_{\mathbf{u}\in U}\|\mathbf{u}\|. \qquad \square$$

One consequence of Corollary 1 is a slight improvement on the lower bound on $Ind_q(n,k)$ given in the introduction ($Ind_q(n,k) \geq n+1$, for $2 \leq k \leq n$).

Observation 3. $Ind_q(n,k) \geq n + \lfloor n/k \rfloor$.

Proof. Let $m = \lfloor n/k \rfloor$. Partition the set $\{1,\ldots,km\}$ into k-element subsets $A_1,\ldots,A_m$. For each $i=1,\ldots,m$, let $\mathbf{a}_i$ be any vector with $\mathrm{supp}(\mathbf{a}_i) = A_i$. The set $\{\mathbf{a}_1,\ldots,\mathbf{a}_m\}$ is a k-extension by Corollary 1(d). $\square$

Next, in connection with Corollary 1(d), we are going to take a closer look at $\|\alpha\mathbf{a}+\beta\mathbf{b}\|$, for $\mathbf{a},\mathbf{b}\in F_q^n$ and $\alpha,\beta\in F_q^*$. Let A and B denote the support of $\mathbf{a}$ and $\mathbf{b}$, respectively, and let $\mathbf{a}=(a_1,\ldots,a_n)$ and $\mathbf{b}=(b_1,\ldots,b_n)$. For any $\xi\in F_q^*$ we define $X_\xi := \{i\in A\cap B : a_i/b_i=\xi\}$. It is not hard to see that the support of $\alpha\mathbf{a}+\beta\mathbf{b}$ equals $A\cup B - X_{-\beta/\alpha}$. In particular,

$$\|\alpha\mathbf{a}+\beta\mathbf{b}\| = |A\cup B| - \left|X_{-\beta/\alpha}\right|.$$

So if $\ell(\mathbf{a},\mathbf{b})=\max_{\xi\in F_q^*}|X_\xi|$ then we have

$$\min_{\alpha,\beta\in F_q^*}\|\alpha\mathbf{a}+\beta\mathbf{b}\| = |A\cup B| - \ell(\mathbf{a},\mathbf{b}). \tag{3.1}$$

Note also that

$$|A\cap B| \leq (q-1)\ell(\mathbf{a},\mathbf{b}). \tag{3.2}$$

Indeed, $|A\cap B| = \left|\bigcup_{\xi\in F_q^*} X_\xi\right| = \sum_{\xi\in F_q^*}|X_\xi| \leq (q-1)\max_{\xi\in F_q^*}|X_\xi|$.

Lemma 2. *Suppose $\mathbf{a},\mathbf{b}\in F_q^n$ are distinct, and let A and B denote the support of $\mathbf{a}$ and $\mathbf{b}$, respectively.*

(a) *If $\|\mathbf{a}\|,\|\mathbf{b}\|\geq k$ then $\{\mathbf{a},\mathbf{b}\}$ is a k-extension iff*

$$\ell(\mathbf{a},\mathbf{b}) \leq |A\cup B| - k + 1. \tag{3.3}$$

(b) *If $\{\mathbf{a},\mathbf{b}\}$ is a k-extension then*

$$2k-n \leq |A\cap B| \leq (q-1)(n-k+1).$$

Proof. (a) Follows from Corollary 1(c), since by (3.1) the inequality (3.3) is equivalent to $\min_{\alpha,\beta\in F_q^*}\|\alpha\mathbf{a}+\beta\mathbf{b}\|\geq k-1$.

(b) By Corollary 1(a), we have $|A|,|B|\geq k$, and so the first inequality follows because

$$|A|+|B|-|A\cap B| = |A\cup B| \leq n.$$

The second inequality follows from (3.2) and part (a) of this lemma:

$$|A\cap B| \leq (q-1)\ell(\mathbf{a},\mathbf{b}) \leq (q-1)(|A\cup B|-k+1). \qquad \square$$

Corollary 2. *If $Ind_q(n,k) \geq n+2$, then $q-1 \geq \frac{2k-n}{n-k+1}$.*

Proof. Indeed, if $Ind_q(n,k) \geq n+2$, then there are $\mathbf{a}$ and $\mathbf{b}$ such that $\{\mathbf{a},\mathbf{b}\}$ is a two-element k-extension (cf. 2.1). But then by Lemma 2(b),

$$q-1 \geq \frac{|\mathrm{supp}(\mathbf{a}) \cap \mathrm{supp}(\mathbf{b})|}{n-k+1} \geq \frac{2k-n}{n-k+1}. \qquad \square$$

In the proof of our last lemma we shall need a basic combinatorics observation. Suppose X and Y are finite sets with $Y \neq \emptyset$. By a **partition** of X by Y we understand any family $\{X_y : y \in Y\}$ of subsets of X such that the union of the family equals X, and its members are pairwise disjoint, with some of them possibly empty. We define the **index** of the partition $\{X_y : y \in Y\}$ to be the maximal of the cardinalities $|X_y|$, for $y \in Y$.

Observation 4. *For any finite sets X, Y, with $Y \neq \emptyset$, there is a partition of X by Y with the index not greater than $\lceil |X|/|Y| \rceil$.*

Lemma 3. *Suppose that r and s are positive integers with $r, s \leq n \leq r+s$. Then there exist distinct $\mathbf{a}, \mathbf{b} \in F_q^n$ such that*

(a) $\|a\| = r,\ \|b\| = s$,

(b) $\ell(\mathbf{a},\mathbf{b}) \leq \left\lceil \frac{r+s-n}{q-1} \right\rceil$,

(c) $|\mathrm{supp}(\mathbf{a}) \cup \mathrm{supp}(\mathbf{b})| = n$.

Proof. Let $\mathbf{a} = (1,\dots,1,0,\dots,0)$, with $\|\mathbf{a}\| = r$. Let X be the $(r+s-n)$-element set $\{n-s+1,\dots,r\}$. Let $\left\{X_\beta : \beta \in F_q^*\right\}$ be a partition of X by F_q^* with the index not greater than $\lceil (r+s-n)/(q-1) \rceil$ (cf. Observation 4). We define $\mathbf{b} = (b_1,\dots,b_n)$ where

$$b_i = \begin{cases} 0 & \text{if } \ i \leq n-s \\ \beta & \text{if } \ i \in X_\beta \\ 1 & \text{if } \ i > r. \end{cases}$$

It is clear that $\|\mathbf{b}\| = s$. Also,

$$\ell(\mathbf{a},\mathbf{b}) = max_{\beta \in F_q^*} |X_\beta| \leq \lceil (r+s-n)/(q-1) \rceil .$$

To see that condition (c) holds note that $\mathrm{supp}(\mathbf{a}) \cap \mathrm{supp}(\mathbf{b}) = X$, and so $|\mathrm{supp}(\mathbf{a}) \cup \mathrm{supp}(\mathbf{b})| = \|\mathbf{a}\| + \|\mathbf{b}\| - |X| = r+s-(r+s-n) = n$. $\square$

Proof of Theorem 2: Note that the condition $k \geq \frac{q}{q+1}(n+1)$ is equivalent to

$$q < \frac{2k-n}{n-k+1} + 1. \tag{3.4}$$

If (3.4) holds then Corollary 2 implies that $Ind_q(n,k) \leq n+1$; i.e. $Ind_q(n,k) = n+1$ (see the remark preceding Observation 3).

Now suppose that (3.4) does not hold. Note that this implies

$$\left\lceil \frac{r+s-n}{q-1} \right\rceil \leq n-k+1. \tag{3.5}$$

We will show that $Ind_q(n,k) \geq n+2$. By Observation 3 this is true if $2k \leq n$. Suppose then that $2k > n$. By Lemma 3 applied to $r = s = k$, there exist distinct $\mathbf{a}, \mathbf{b} \in F_q^n$ such that $\|\mathbf{a}\| = \|\mathbf{b}\| = k$, $\ell(\mathbf{a}, \mathbf{b}) \leq \lceil (r+s-n)/(q-1) \rceil$, and $|\mathrm{supp}(\mathbf{a}) \cup \mathrm{supp}(\mathbf{b})| = n$. To complete the proof it is enough to show that $\{\mathbf{a}, \mathbf{b}\}$ is a k-extension. The latter follows from Lemma 2(a) since by (3.5) and the properties of $\mathbf{a}$ and $\mathbf{b}$ above

$$\ell(\mathbf{a}, \mathbf{b}) \leq n-k+1 = |\mathrm{supp}(\mathbf{a}) \cup \mathrm{supp}(\mathbf{b})| - k + 1. \qquad \square$$

4 An application to sets of k-orthogonal hypercubes

In [1, Section 3], numerous applications of Theorem 1 were given related to the construction of hypercubes and orthogonal arrays, pseudo (t, m, s)-nets and linear codes. We refer the reader to the paper [1] and the references cited therein for a comprehensive account of these applications.

We now present an application of our results to the construction of sets of orthogonal hypercubes. By a *hypercube of dimension n and order b* is meant a $b \times \cdots \times b$ array consisting of 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 $n = k = 2$ these ideas reduce to the usual notion of mutually orthogonal latin squares of order b.

Given a set of k-independent vectors of length n over F_q, we can build sets of k-orthogonal hypercubes of order q and dimension n. Let $a_1x_1 + \cdots + a_nx_n$ denote a vector of length n in a k-orthogonal set. One can then construct a hypercube of order q and dimension n by placing the field element $a_1b_1 + \cdots + a_nb_n$ in the cell of the hypercube labelled by $(b_1, \ldots, b_n)$, where each $b_i \in F_q$. Since each coefficient vector $(a_1, \ldots, a_n)$ has at least one nonzero entry, it is clear that the array represented by the vector is indeed a hypercube of dimension n and order q.

Moreover, given k such vectors from a k-independent set, the corresponding set of k hypercubes will be k-orthogonal. This follows from the fact that the k vectors are k-independent over F_q, and hence the $k \times n$ matrix obtained from the coefficients of the k vectors will have rank k. Hence each element of F_q^k will be picked up exactly q^{n-k} times, so the k hypercubes are indeed k-orthogonal. This construction thus yields $Ind_q(n, k)$, k-orthogonal hypercubes of dimension n and order q.

We now raise a question regarding hypercubes of prime power orders. Let q, n, and k be such that they satisfy Theorem 2 so that $Ind_q(n, k) = n + 1$. Then as above, we can construct $n + 1$ hypercubes, each of dimension n and order q, which are k-orthogonal.

Question: If q is a prime power and the values of q, n and k satisfy Theorem 2 so that $Ind_q(n, k) = n + 1$, is it possible to have more than $n + 1$ hypercubes of order q and dimension n which are k-orthogonal?

We close by referring the reader to [2] and [3] for discussions of latin squares and hypercubes.

References

[1] S.B. Damelin, G. Michalski, G.L. Mullen, and D. Stone, *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*, Monatsh. Math. **141** (2004), pp. 277-288.

[2] J. Dénes and A.D. Keedwell, Latin Squares and their Applications, Academic Press, New York, 1974.

[3] C.F. Laywine and G.L. Mullen, Discrete Mathematics Using Latin Squares, Wiley, New York, 1998.

Institute for Mathematics and its Applications, University of Minnesota, 400 Lind Hall, 207 Church Hill, S.E, Minneapolis, MN 55455;
Email: damelin@georgiasouthern.edu

Department of Mathematical Sciences, Georgia Southern University, P. O. Box 8093, Statesboro, GA 30460; Email: gmichals@georgiasouthern.edu

Department of Mathematics, The Pennsylvania State University, University Park, PA 16802; Email: mullen@math.psu.edu