Sets of Orthogonal Hypercubes of Class r

John T. Ethier, Gary L. Mullen,
Daniel Panario, Brett Stevens, and David Thomson*

October 6, 2011

Abstract

A (d, n, r, t)-hypercube is an $n \times n \times \cdots \times n$ (d-times) array on n^r symbols such that when fixing t coordinates of the hypercube (and running across the remaining $d - t$ coordinates) each symbol is repeated n^{d-r-t} times. We introduce a new parameter, r, representing the *class* of the hypercube. When $r = 1$, this provides the usual definition of a hypercube and when $d = 2$ and $r = t = 1$ these hypercubes are Latin squares. If $d \geq 2r$, then the notion of orthogonality is also inherited from the usual definition of hypercubes. This work deals with constructions of class r hypercubes and presents bounds on the number of mutually orthogonal class r hypercubes. We also give constructions of sets of mutually orthogonal hypercubes when n is a prime power.

1 Introduction

Before defining and studying sets of orthogonal hypercubes of class r, we briefly review some standard definitions and notions involving sets of orthogonal hypercubes without specified class number. Under the later terminology, the standard definition of hypercube corresponds to hypercubes of class 1.

Definition 1.1. *Let d, n, t be integers, with $d > 0$ and $n > 0$. A* (d, n, t)-hypercube of dimension d, order n and type t *is an $n \times n \times \cdots \times n$ (d times) array on n distinct symbols such that in every co-dimension-t-subarray (that is, fix t coordinates of the array and allow the remaining $d-t$ coordinates to vary) each of the n symbols appears exactly $n^{d-(t+1)}$ times.*

Moreover, two such hypercubes are said to be orthogonal *if when superimposed each of the n^2 possible distinct pairs occurs exactly n^{d-2} times.*

Finally, a set $\mathcal{H}$ of such hypercubes is mutually orthogonal *if any two distinct hypercubes in $\mathcal{H}$ are orthogonal.*

*The final three authors are supported in part by NSERC of Canada.
MSC (2010) Classification Number: 05B15.
Keywords: Hypercubes, Latin squares, mutually orthogonal.

We use the term co-dimension-t-subarray (or simply t-subarray) to emphasize that t coordinates are fixed and that the remaining $d-t$ coordinates vary. In the case of a square (which of course has dimension $d=2$), a 1-subarray is just a row or column while if $d=3$, a 1-subarray is a plane (containing n^2 cells) parallel to two of the coordinate axes while a 2-subarray is a line (containing n cells) parallel to an axis. When $d=2$ and $t=1$ the definition of a hypercube reduces to the well studied case of a Latin square.

An upper bound on the maximal number of orthogonal hypercubes with various types appears in [5, Theorem 3.2]. We note that the maximum number of orthogonal hypercubes of dimension d, order n and type 1 is upper bounded by $(n^d-1)/(n-1)-d$ and when $n=q$ is a prime power, this bound can be achieved using linear polynomials with coefficients in the finite field containing q elements.

This paper extends the usual definition of hypercubes by considering the alphabet size to be a power of the order. We call this power the *class* of a hypercube. The original definition of a hypercube corresponds to class 1 hypercubes.

The structure of the paper is as follows. In Section 2 we present the definition of hypercubes of class r and give some bounds on the existence of such cubes. We then provide constructions of such hypercubes based on other combinatorial objects and a finite field construction. In Section 3 we study sets of orthogonal hypercubes when n is a prime power and when $d=2r$. We conclude the paper with some open problems in Section 4.

2 Hypercubes of class r

We examine hypercubes and sets of orthogonal hypercubes in which we increase the number of symbols beyond the order of the hypercube. More specifically, we consider a type of hypercube introduced by Kishen [4] where the number of symbols in the hypercube is a positive integer power of the order of the hypercube. We begin by providing some bounds on these hypercubes. We also provide a definition of orthogonality for such hypercubes as well as a method for constructing individual hypercubes and orthogonal sets in certain cases.

Definition 2.1. *Let d, n, r, t be integers, with $d>0, n>0, r>0$ and $0 \le t \le d-r$. A* (d,n,r,t)-hypercube of dimension d, order n, class r and type t *is an $n \times n \times \cdots \times n$ (d times) array on n^r distinct symbols such that in every co-dimension-t-subarray (that is, fix t coordinates of the array and allow the remaining $d-t$ coordinates to vary) each of the n^r distinct symbols appears exactly n^{d-t-r} times.*

Moreover, if $d \ge 2r$, two such hypercubes are said to be orthogonal *if when superimposed each of the n^{2r} possible distinct pairs occurs exactly n^{d-2r} times.*

Finally, a set $\mathcal{H}$ of such hypercubes is mutually orthogonal *if any two distinct hypercubes in $\mathcal{H}$ are orthogonal.*

In [4], Kishen used the term "order" rather than class. In this work, we reserve the term "order" to denote the size of the array and we use the term *class* in place of Kishen's definition of "order". Figure 1 provides an example of a hypercube of dimension 3, order 3, class 2 and type 0.

0	1	2	|	4	5	3	|	8	6	7
3	4	5	|	7	8	6	|	2	0	1
6	7	8	|	1	2	0	|	5	3	4

Figure 1: A hypercube of dimension 3, order 3, class 2 and type 0.

We note that a d-dimensional hypercube of order n and class $r = 1$ is simply a hypercube of dimension d and order n, and a $d = 2$ dimensional hypercube of class $r = 1$ and type $t = 1$ is simply a Latin square of order n. Furthermore, the definition for orthogonality for class r hypercubes generalizes the standard definition of orthogonality for hypercubes.

2.1 Bounds

While there always exists a hypercube of order n for any dimension $d \geq 2$, the following lemma shows that this is not the case for hypercubes of class r.

Lemma 2.2. *Let $r \geq 2$. If $d > (n-1)^{r-1} + r$, then there does not exist a $(d, n, r, d-r)$-hypercube.*

Proof. Suppose we have a d-dimensional hypercube of order n, class r and type $d - r$. Consider the symbols which occur in the coordinate axes $x_{r+1}, x_{r+2}, \ldots, x_d$, that is, for $j = r+1, r+2, \ldots, d$, the symbols occurring when $x_i = 0$ for all $i \neq j$ and allow x_j to vary. First note that they share a common point at the origin. Now, notice that the remaining $n-1$ symbols in each of these coordinate axes must be distinct; otherwise any $(d-r)$-subarray containing two of these coordinate axes would not contain all n^r symbols.

Next, consider any of these coordinate axes, say x_{r+1}, and notice that it is contained in the r different $(d-r)$-subarrays with fixed coordinates $x_i = x_{r+2} = x_{r+3} = \cdots = x_d = 0$ for each i with $1 \leq i \leq r$. Thus, the symbols in the x_{r+1} coordinate axis cannot be the same as those in any of the $(d-r+1)$-subarrays with fixed coordinates $x_i = x_{r+1} = x_{r+2} = \cdots = x_d = 0$ for each i with $1 \leq i \leq r$. Considering the entries in the sub-hypercube with coordinates not meeting the origin, this leaves $(n-1)^r$ distinct symbols to choose from. We can use the same argument on each coordinate axis $x_{r+2}, x_{r+3}, \ldots, x_d$. Since the $n-1$ symbols in each of these $d-r$ coordinate axes must also be distinct from each other as well, we must have that $(d-r)(n-1) \leq (n-1)^r$. Hence $d \leq (n-1)^{r-1} + r$. □

We establish a general upper bound on the size of a set of mutually orthogonal hypercubes as a function of dimension, order, class and type. We begin by setting up a matrix formulation of hypercubes which is used in the proof of the bound. Let H be a hypercube of dimension d, order n, type t, and class r. Define a $n^d \times n^r$ matrix

$$N_H = (n_{x_1,x_2,\ldots,x_d,s}),$$

where

$$n_{x_1,x_2,\ldots,x_d,s} = \begin{cases} 1 & \text{if symbol } s \text{ occurs in position } H(x_1, x_2, \ldots, x_d), \\ 0 & \text{otherwise.} \end{cases}$$

If $H_1, H_2, \ldots H_N$ are mutually orthogonal, let

$$M = (N_{H_1} N_{H_2} \cdots H_{H_N}).$$

We have the following lemma.

Lemma 2.3. *Let $i, j \in \{1, 2, \ldots, N\}$. Then*

$$N_{H_i}^T N_{H_j} = \begin{cases} n^{d-r} I_{n^r} & \text{if } i = j, \\ n^{d-2r} J_{n^r} & \text{if } i \neq j, \end{cases}$$

where I_t is the $t \times t$ identity matrix and $J_t = (1)_{t \times t}$.

The proof is immediate from the definitions of the N_H. We now give a bound on the maximum number of class r hypercubes.

Theorem 2.4. *The maximum number of mutually orthogonal hypercubes of dimension d, order n, type t and class r is bounded above by*

$$\frac{1}{n^r - 1} \left(n^d - 1 - \binom{d}{1}(n-1) - \binom{d}{2}(n-1)^2 - \cdots - \binom{d}{t}(n-1)^t \right).$$

Proof. Let $H_1, H_2, \ldots H_N$ be mutually orthogonal hypercubes, $M = (N_{H_1} N_{H_2} \cdots H_{H_N})$, and H_{H_i}, $1 \leq i \leq n$, as defined above. If all elements but one are known in some co-dimension-k-subarray ($k \leq t$), then the remaining element is determined because all of the hypercubes are of type t and any co-dimension-k-subarray is a disjoint union of co-dimension-t-subarrays; thus, each symbol appears precisely n^{d-k-r} times. The position of each such remaining element corresponds to a row of M.

For any fixed set of k coordinates we consider the position of the H_i determined by setting the remaining $d-k$ coordinates to n. The element in this position in each hypercube is determined by the entries in the other positions of the co-dimension-k-subarray and thus depends on the set of k coordinates chosen and their values. To avoid multiple counting as we vary the size and selection of k coordinates, we only consider setting the fixed coordinates to values that are *not* n. Thus we determine that for any value of k, there are $\binom{d}{k}(n-1)^k$ rows of M that are dependent on the remaining rows.

Summing over k gives at least

$$\sum_{k=1}^{t} \binom{d}{k}(n-1)^k$$

dependent rows. Thus

$$\operatorname{rank}(M) \leq n^d - \sum_{k=1}^{t} \binom{d}{k}(n-1)^k.$$

We have

$$M^TM = \begin{bmatrix} n^{d-r}I_{n^r} & n^{d-2r}J_{n^r} & \cdots & n^{d-2r}J_{n^r} \\ n^{d-2r}J_{n^r} & n^{d-r}I_{n^r} & & n^{d-2r}J_{n^r} \\ \vdots & & \ddots & \vdots \\ n^{d-2r}J_{n^r} & & \cdots & n^{d-r}I_{n^r} \end{bmatrix} = n^{d-2r} \begin{bmatrix} n^rI_{n^r} & J_{n^r} & \cdots & J_{n^r} \\ J_{n^r} & n^rI_{n^r} & & J_{n^r} \\ \vdots & & \ddots & \vdots \\ J_{n^r} & & \cdots & n^rI_{n^r} \end{bmatrix},$$

and from [9] we have that its eigenvalues are $Nn^{d-r}, n^{d-r}, 0$ with multiplicities $1, N(n^r - 1), N - 1$ respectively. Thus

$$N(n^r-1)+1 = Nn^r - N + 1 = \operatorname{rank}(M^TM) = \operatorname{rank}(M) \leq n^d - \sum_{k=1}^{t} \binom{d}{k}(n-1)^k,$$

and we have

$$N \leq \frac{1}{n^r-1}\left(n^d - 1 - \binom{d}{1}(n-1) - \binom{d}{2}(n-1)^2 - \cdots - \binom{d}{t}(n-1)^t\right). \qquad \square$$

When $r = t = 1$ the bound reduces to the well-known result [1, Section IV.22.5] on the maximum number N of hypercubes: $N \leq (n^d - 1)/(n - 1) - d$. We have the following corollary when the hypercube has the largest possible type $d - r$.

Corollary 2.5. *The maximum number of mutually orthogonal hypercubes of dimension d, order n, type $d - r$ and class r is bounded above by*

$$\frac{\sum_{k=d-r+1}^{d}\binom{d}{k}(n-1)^k}{n^r-1}.$$

The bound in Theorem 2.4 is $n^{d-r} + O(n^{d-r-1})$ for any type; the type only affects the lower-order terms.

2.2 Constructions

We can relate certain classes of hypercubes to other well-known combinatorial objects, such as *orthogonal arrays*.

Definition 2.6. [1, Definition III.6.1] *An* orthogonal array *with parameter λ, strength t, degree k and s levels, denoted $OA_\lambda(t, k, s)$, is a $k \times N$ array, with $N = \lambda s^t$, with entries from a set of $s \geq 2$ symbols, having the property that in every $t \times N$ submatrix, every $t \times 1$ column vector appears λ times.*

We show later how to construct hypercubes of order n, dimension d, and class r when n is a prime power. However if n is not a prime power, the following provides a simple construction of dimension k, class $k - d$ hypercubes using orthogonality of strength d. We first give the definition of d-strength orthogonality, following [3].

Definition 2.7. *A set $\mathcal{H}$ of hypercubes of dimension $d \geq 2$ is* mutually strongly d-orthogonal *if, upon superposition of corresponding $(d-j)$-subarrays (that is, fix any $d-j$ coordinates and allow the remaining j coordinates to vary) of any j hypercubes in $\mathcal{H}$ with $1 \leq j \leq \min(d, |\mathcal{H}|)$, each j-tuple appears exactly once. This is equivalent to the existence of an $OA_1(d, d+|\mathcal{H}|, n)$.*

The following lemma generalizes two constructions, one appearing in [3] and the other appearing in [8].

Lemma 2.8. *If there exists an $OA_1(d, k, n)$ then there exists a $(k, n, k-d, d)$-hypercube.*

Proof. Let A be an $\mathrm{OA}_1(d, k, n)$ with symbols in $\mathbb{Z}_n$ (any group of size n will do). All indices of size n are also taken from $\mathbb{Z}_n$. We index the rows by the d-tuples of elements from $\mathbb{Z}_n$ taken from the first d columns of A, and construct a k-dimensional hypercube, H, of order n and class $k-d$,

$$H((j_i)_{0\leq i<d}, (c_l)_{0\leq l<k-d}) \\ = H(j_0, j_1, \ldots, j_{d-1}, c_0, \ldots, c_{k-d-1}) = (A((j_i)_{0\leq i<d}, d+l) + c_l)_{0\leq l<k-d}.$$

We now show that this hypercube has type d. Suppose that d coordinates of H are fixed; without loss of generality they are j_i, $0 \leq i < m$, and c_l, $0 \leq l < d-m$, where $0 \leq m \leq d$ and $m \geq 2d-k$. In the subarray defined by these fixed coordinates and permitting all others to vary, if

$$H((j_i)_{0\leq i<m}, (j_i)_{m\leq i<d}, (c_l)_{0\leq l<d-m}, (c_l)_{d-m\leq l<k-d}) \\ = H((j_i)_{0\leq i<m}, (j'_i)_{m\leq i<d}, (c_l)_{0\leq l<d-m}, (c'_l)_{d-m\leq l<k-d}),$$

then,

$$A((j_i)_{0\leq i<m}, (j_i)_{m\leq i<d}, d+l) = A((j_i)_{0\leq i<m}, (j'_i)_{m\leq i<d}, d+l), \quad 0 \leq l < d-m, \tag{1}$$

and

$$A((j_i)_{0\leq i<m}, (j_i)_{m\leq i<d}, d+l) + c_l \\ = A((j_i)_{0\leq i<m}, (j'_i)_{m\leq i<d}, d+l) + c'_l, \quad d-m \leq l < k-d. \tag{2}$$

When l ranges from 0 to $d-m-1$, $d+l$ varies from d to $2d-m-1$. Hence, Equation (1) specifies a d-tuple in A in columns $0, \ldots, m-1$ and $d, \ldots, 2d-m-1$. A d-tuple in any set of d columns of A can only appear in precisely one row, and thus $j_i = j'_i$ for $m \leq i < d$. These equalities permit cancellations in Equation (2) which yield that $c_l = c'_l$ for $d-m \leq l < k-d$. Thus no symbols repeat in the given subarray. □

Orthogonal hypercubes exist only if $d \geq 2r$. In this case, we present the following construction of (d, n, r, r)-hypercubes which relies heavily on linear algebra over finite fields.

Lemma 2.9. *Let n be a power of a prime, let d, r be positive integers with $d \geq 2r$ and let $q = n^r$. Consider $\mathbb{F}_q$ as a vector space over $\mathbb{F}_n$, and define $c_j \in \mathbb{F}_q$, $j = 1, 2, \ldots, d$, such that any r of them form a linearly independent set in $\mathbb{F}_q$. The hypercube constructed from the polynomial $c_1x_1 + c_2x_2 + \cdots + c_dx_d$ is a hypercube of dimension d, order n, class r and type r.*

Proof. We must show that each of the n^r elements of $\mathbb{F}_q$ occurs in each co-dimension-r-subarray exactly n^{d-2r} times. Consider now any r-subarray, and without loss of generality let $x_{d-r+1}, x_{d-r+2}, \ldots, x_d$ be fixed coordinates. Then, this subarray is generated by the polynomial $c_1x_1 + c_2x_2 + \cdots + c_{d-r}x_{d-r}$. To show that every value of $\mathbb{F}_q$ appears exactly n^{d-2r} times we solve the equation $c_1x_1+c_2x_2+\cdots+c_{d-r}x_{d-r} = \lambda$, $\lambda \in \mathbb{F}_q$. Since $\mathbb{F}_q$ is a simple extension of $\mathbb{F}_n$, we assume that $\mathbb{F}_q = \mathbb{F}_n(\alpha)$, where α is a root of an irreducible polynomial of degree r over $\mathbb{F}_n$. Denote $c_j = \sum_{i=1}^{r} a_{i,j}\alpha^{i-1}$ and $\lambda = \sum_{i=1}^{r} a_{i,\lambda}\alpha^{i-1}$ with $a_{i,j}, a_{i,\lambda} \in \mathbb{F}_n$.

We have the following matrix equation by equating coefficients of α:

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,d-r} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,d-r} \\ & & \vdots & \\ a_{r,1} & a_{r,2} & \cdots & a_{r,d-r} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{d-r} \end{bmatrix} = \begin{bmatrix} a_{1,\lambda} \\ a_{2,\lambda} \\ \vdots \\ a_{r,\lambda} \end{bmatrix}.$$

By hypothesis, any r coefficients of $x_1, x_2, \ldots, x_d$ are linearly independent and so, the above matrix has rank r. Thus, the solution set of the above equation has dimension $d-2r$, proving the claim. □

We can draw comparisons to hypercubes constructed using Lemma 2.9 directly from the matrices. In particular, any $r \times d$ matrix over a finite field $\mathbb{F}_n$ with the property that any r columns are linearly independent yields a $(d, n, r, 1)$-hypercube. If $d \geq (t+1)r$, a trivial extension of the above lemma gives that any $r \times d$ matrix with the property that any tr columns are linearly independent yields a (d, n, r, t)-hypercube.

We remark that matrices satisfying Lemma 2.9 are studied in coding theory, see [7].

Remark 2.10. *Let H be an $r \times d$ matrix over $\mathbb{F}_q$ such that any r columns are linearly independent and some $r+1$ columns are linearly dependent. Consider H as a parity-check matrix of a linear code over $\mathbb{F}_q$. Such a code has minimum distance $r+1$ and the number of codewords is q^{d-r}. When $d = 2r$ such a code reaches the Singleton bound [7], and H is the parity check matrix of a* maximum-distance separable *(MDS) code.*

Corollary 2.11. *Let q be a prime power. The number of $(2r, q, r, r)$-hypercubes is at least the number of linear MDS codes over $\mathbb{F}_q$ of length $2r$ and rank r.*

In addition, we have the following result from [2, 3].

Theorem 2.12. *Let $f_i(x_1, x_2, \ldots, x_n) = a_{i1}x_1+a_{i2}x_2+\cdots+a_{id}x_d, i = 1, \ldots, r$, be polynomials over $\mathbb{F}_q$. The corresponding hypercubes are mutually strongly d-orthogonal hypercubes of dimension d, order q and class 1 if and only if every square submatrix of (a_{ij}) is non-singular.*

Corollary 2.13. *Suppose $\mathcal{H}$ is a set of r mutually strongly $2r$-orthogonal hypercubes constructed from Theorem 2.12. Then, the resulting matrix defines a $(2r, q, r, r)$-hypercube.*

In Section 3, we use Lemma 2.9 with $d = 2r$ to construct sets of orthogonal hypercubes.

3 Sets of orthogonal hypercubes of dimension $2r$

In this section, we consider only hypercubes of dimension $2r$, order n, class r and type r. We give a bound on the number of mutually orthogonal hypercubes of this form, which significantly improves the bound in Theorem 2.4. We then construct sets of such orthogonal hypercubes when r is a prime power and $r < n$.

Theorem 3.1. *There at most $(n-1)^r$ mutually orthogonal $(2r, n, r, r)$-hypercubes.*

Proof. First, permute the symbols of each hypercube so that the r-subarray with fixed coordinates $x_{r+1} = x_{r+2} = \cdots = x_{2r} = 0$ is identical for each hypercube. Now, consider the symbol in the entry $x_{2r} = 1$, $x_1 = x_2 = \cdots = x_{2r-1} = 0$. This entry is contained in the r subarrays with fixed coordinates $x_i = x_{r+1} = x_{r+2} = \cdots = x_{2r-1} = 0$ for each i with $1 \leq i \leq r$. Thus we cannot take any entry in the subarrays with fixed coordinates $x_i = x_{r+1} = x_{r+2} = \cdots = x_{2r} = 0$ for each i with $1 \leq i \leq r$. This leaves us with $(n-1)^r$ choices for the symbol in entry $x_{2r} = 1$, $x_1 = x_2 = \cdots = x_{2r-1} = 0$. Furthermore, each hypercube must have a distinct symbol in this entry since all ordered pairs (i, i), $1 \leq i \leq n^r$, occur in the square $x_{r+1} = x_{r+2} = \cdots = x_{2r} = 0$. Therefore we have at most $(n-1)^r$ mutually orthogonal hypercubes. □

Remark 3.2. *Theorem 3.1, combined with Lemma 2.2 requires that $r = 1$ or $n \geq 3$.*

We observe that Theorem 3.1 is a generalization of the well-known bound for mutually orthogonal Latin squares.

Corollary 3.3. *There are at most $n-1$ mutually orthogonal Latin squares of order n.*

Corollary 3.4. *Let $n \geq 3$. There are at most $(n-1)^2$ mutually orthogonal $(4, n, 2, 2)$-hypercubes.*

Maximal sets of mutually orthogonal hypercubes are called *complete*. For most prime power orders n, we can construct complete sets of $(n-1)^2$ mutually orthogonal $(4, n, 2, 2)$-hypercubes using multivariate permutation polynomials over the finite field of order n. First, we show how to construct two orthogonal $(2r, n, r, r)$-hypercubes when n is a prime power.

Theorem 3.5. *Let n be a power of a prime, let r be a positive integer and let $q = n^r$. Denote as $\mathbb{F}_q$ the extension of $\mathbb{F}_n$ obtained by adjoining a root α of an irreducible polynomial*

of degree r over $\mathbb{F}_n$, that is, $\mathbb{F}_q = \mathbb{F}_n(\alpha)$. Let

$$p_1(x_1, x_2, \ldots, x_{2r}) = \sum_{j=1}^{r} \alpha^{j-1} x_j + \sum_{j=r+1}^{2r} \sum_{i=1}^{r} a_{i,j-r} \alpha^{i-1} x_j \text{ and}$$

$$p_2(x_1, x_2, \ldots, x_{2r}) = \sum_{j=1}^{r} \alpha^{j-1} x_j + \sum_{j=r+1}^{2r} \sum_{i=1}^{r} a'_{i,j-r} \alpha^{i-1} x_j,$$

with $p_1 \neq p_2$ and $a_{i,j}, a'_{s,t} \in \mathbb{F}_n^*$ for any $i, j, s, t = 1, 2, \ldots, r$.

Define the matrices A and A' by

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,r} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,r} \\ & & \vdots & \\ a_{r,1} & a_{r,2} & \cdots & a_{r,r} \end{bmatrix} \text{ and } A' = \begin{bmatrix} a'_{1,1} & a'_{1,2} & \cdots & a'_{1,r} \\ a'_{2,1} & a'_{2,2} & \cdots & a'_{2,r} \\ & & \vdots & \\ a'_{r,1} & a'_{r,2} & \cdots & a'_{r,r} \end{bmatrix},$$

and suppose that A, A' and $A - A'$ are nonsingular. Then the hypercubes generated by p_1 and p_2 are orthogonal $(2r, n, r, r)$-hypercubes.

Proof. By Lemma 2.9 the polynomials p_1 and p_2 form hypercubes of dimension $2r$, order n and class r. What remains is to show that these hypercubes are orthogonal.

Let $p_1 = \sum_{j=1}^{r} f_j \alpha^{j-1}$ and $p_2 = \sum_{j=1}^{r} f_{j+r} \alpha^{j-1}$. Then, from p_1 and p_2 we have the following system of equations:

$$\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_{2r} \end{bmatrix} = \begin{bmatrix} I_r & A \\ I_r & A' \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{2r} \end{bmatrix}.$$

By showing that $f_1, f_2, \ldots, f_{2r}$ form an orthogonal system, we show that these two polynomials construct orthogonal hypercubes.

It is known [6, Corollary 7.39] that $f_1, f_2, \ldots, f_{2r}$ form an orthogonal system if and only if $P = c_1 f_1 + c_2 f_2 + \cdots + c_{2r} f_{2r}$ is a permutation polynomial for all $(c_1, c_2, \ldots, c_{2r}) \in \mathbb{F}_n^{2r}$ with $(c_1, c_2, \ldots, c_{2r}) \neq (0, 0, \ldots, 0)$. Substituting gives

$$P = \sum_{j=1}^{r} (c_j + c_{j+r}) x_j + \sum_{j=1}^{r} \left(\sum_{i=1}^{r} c_i a_{i,j} + \sum_{i=r+1}^{2r} c_i a'_{i-r,j} \right) x_{j+r}. \tag{3}$$

Since P is a linear polynomial in $x_1, x_2, \ldots, x_{2r}$, we have that P is a permutation polynomial if and only if $P \neq 0$. Suppose, by way of contradiction, that P is not a permutation polynomial, that is, that $P = 0$. Equating coefficients of $x_1, x_2, \ldots, x_r$ gives $c_j = -c_{j+r}$, $j = 1, 2, \ldots, r$. Substituting these relations into the second term of Equation (3) gives

$$\sum_{i=1}^{r} c_i (a_{i,j} - a'_{i,j}) = 0, \ j = 1, 2, \ldots, r.$$

Since $(c_1, c_2, \ldots, c_{2r}) \neq (0, 0, \ldots, 0)$ we know that one of $c_1, c_2, \ldots, c_r$ are nonzero. Thus, we have a non-trivial zero-solution from the columns of $A - A'$, contradicting the assumption that $A - A'$ is non-singular. □

When $r = 2$ we find a complete set of mutually orthogonal hypercubes of dimension 4, order n and class 2.

Corollary 3.6. *Let n be an odd prime power. Then there exists a complete set of $(n-1)^2$ mutually orthogonal hypercubes of dimension 4, order n and class 2.*

Proof. Denote as $\mathbb{F}_n$ the finite field with n elements and let $\mathbb{F}_q = \mathbb{F}_n(\alpha)$, where α is a root of an irreducible quadratic polynomial over $\mathbb{F}_n$.

Let ω be a non-square element of $\mathbb{F}_n$ and for any $a, b \in \mathbb{F}_n^*$, define the polynomial $p_{(a,b)} = x_1 + \alpha x_2 + (a + b\alpha)x_3 + (b + a\omega\alpha)x_4$. We show that any two of these polynomials $p_{(a,b)}, p_{(x,y)}$, with $(a, b) \neq (x, y)$ form mutually orthogonal hypercubes.

Let

$$A = \begin{bmatrix} a & b \\ b & a\omega \end{bmatrix} \text{ and } A' = \begin{bmatrix} x & y \\ y & x\omega \end{bmatrix}.$$

Clearly A is non-singular since if $\det(A) = 0$, then $\omega = (b/a)^2$, contradicting the choice of ω. Similarly, A' is non-singular. Suppose now that $A - A'$ is singular, that is, $\det(A - A') = 0$. Then $(a - x)^2\omega - (b - y)^2 = 0$. If $a = x$ then $b = y$, contradicting $(a, b) \neq (x, y)$; in the same way if $b = y$ then $a - x$.

Now consider $a \neq x$ and $b \neq y$. We have

$$\omega = \left(\frac{b - y}{a - x}\right)^2,$$

contradicting that ω is not a square. Hence, the matrix $A - A'$ is non-singular and the conditions for Theorem 3.5 are satisfied. □

Corollary 3.7. *Let $n = 2^{2k}$, $k \in \mathbb{N}$. Then there exists a complete set of $(n-1)^2$ mutually orthogonal hypercubes of dimension 4, order n, and class 2.*

Proof. Since 3 divides $n - 1 = 2^{2k} - 1$, we have non-cube elements in $\mathbb{F}_n$; primitive elements, for example. Let $\omega \neq 0$ be a non-cube element of $\mathbb{F}_n$, that is $\omega \neq r^3$ for any $r \in \mathbb{F}_n$. Now, for every $a \in \mathbb{F}_n^*$ and $b \in \mathbb{F}_n^*$, let $p_{(a,b)} = x_1 + (\alpha)x_2 + (a + b\alpha)x_3 + (b^2 + a^2\omega\alpha)x_4$. We show that any two of these polynomials $p_{(a,b)}, p_{(x,y)}$ with $(a, b) \neq (x, y)$ form mutually orthogonal hypercubes. Let

$$A = \begin{bmatrix} a & b \\ b^2 & a^2\omega \end{bmatrix} \text{ and } A' = \begin{bmatrix} x & y \\ y^2 & x^2\omega \end{bmatrix}.$$

Clearly A is non-singular since if $\det(A) = 0$, then $\omega = (b/a)^3$, contradicting the choice of ω. Similarly, A' is non-singular. Suppose now that $\det(A - A') = 0$. Then $(a - x)^3\omega = (b - y)^3$. If $a = x$, then $b = y$, contradicting that $(a, b) \neq (x, y)$. If $a \neq x$, then

$$\omega = \left(\frac{b - y}{a - x}\right)^3,$$

contradicting the choice of ω. Hence, the matrix $A - A'$ is non-singular and the conditions for Theorem 3.5 are satisfied. □

Unfortunately, the approach of Corollary 3.6 and Corollary 3.7 cannot be applied to solve all of the possible $n = 2^{2k+1}$ cases at once. A new method is required in this case.

We now give sets of orthogonal hypercubes for $r > 2$. These sets are unable to meet the bound in Theorem 3.1. We obtain sets of $n - 1$ mutually orthogonal hypercubes when n is a prime power and $r < n$ using the following application of Theorem 3.5.

Theorem 3.8. *Let n be a prime power. For any integer $r < n$, there exists a set of $n - 1$ mutually orthogonal $(2r, n, r, r)$-hypercubes.*

Proof. Let α be a primitive element of $\mathbb{F}_n$ and let A be the $r \times r$ Vandermonde matrix with defining row $(\alpha, \alpha^2, \ldots, \alpha^r)$. Since $r < n$, each entry of $(\alpha, \alpha^2, \ldots, \alpha^r)$ is distinct, and so A is non-singular. Now define $A_j = \alpha^j A$, for any $j = 1, \ldots, n-2$. Each A_j is non-singular since A is non-singular, and the difference of any two distinct matrices in $\{A, A_1, \ldots, A_{n-2}\}$ is also non-singular. Therefore, the hypercubes defined using the matrices $\{A, A_1, \ldots, A_{n-2}\}$ in Theorem 3.5 are mutually orthogonal. □

When n is a prime power, using the method of Corollary 3.6 to find sets of orthogonal hypercubes of class $r = 3$ and using results about solutions of diagonal equations over finite fields [6, Theorem 6.33], one can marginally improve the bound of $n-1$ mutually orthogonal hypercubes to $n + C$, where C is a small positive constant. In general, the method of Corollary 3.6 cannot be used to construct sets of orthogonal hypercubes approaching the bound in Theorem 3.1 when $r > 2$. For higher class, a new method is needed.

4 Conclusions and problems

In this paper, we extend the usual definition of hypercubes by introducing a new parameter, the *class* r of a hypercube, which increases the alphabet size of the hypercube. We give necessary conditions on r for the existence of such hypercubes and present bounds and constructions of sets of mutually orthogonal hypercubes.

When $d = 2r$, an upper bound on the number of mutually orthogonal hypercubes is $(n-1)^r$. We give a construction of $(n-1)^2$ mutually orthogonal hypercubes when $r = 2$ when n is a prime power.

Some open problems follow.

1. Construct a complete set of mutually orthogonal $(4, n, 2, 2)$-hypercubes when $n = 2^{2k+1}$.

2. Is the $(n-1)^r$ bound in Theorem 3.1 tight when $r > 2$? If so, construct a complete set of mutually orthogonal $(2r, n, r, r)$-hypercubes of class $r > 2$. If not, determine a tight upper bound and construct such a complete set.

3. Find constructions (other than standard Kronecker product constructions) of sets of mutually orthogonal hypercubes when n is not a prime power. Such constructions will require a new method not based on finite fields.

Acknowledgement

The second and fifth authors would like to sincerely thank Gary McGuire and the Claude Shannon Institute of the University College Dublin for their support during the period January, 2011 through March, 2011 when much of the discussion for this paper took place.

References

[1] C. Colbourn and J. Dinitz, *Handbook of Combinatorial Designs* (2nd ed.), CRC Press, Boca Raton, 2007.

[2] J.T. Ethier, *Strong Forms of Orthogonality for Sets of Hypercubes*, Ph.D. thesis, The Pennsylvania State University, 2008.

[3] J.T. Ethier and G.L. Mullen, Strong forms of orthogonality for sets of hypercubes, preprint.

[4] K. Kishen, On the construction of Latin and hyper-Graeco-Latin cubes and hypercubes, *Journal of the Indian Society of Agricultural Statistics*, Vol. 2 (1950), 20-48.

[5] C.F. Laywine and G.L. Mullen, *Discrete Mathematics using Latin Squares*, John Wiley and Sons, Inc., New York, 1998.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Vol. 20, Sec. ed., Cambridge University Press, Cambridge, 1997.

[7] R. Singleton, Minimum distance q-nary codes, *IEEE Transactions on Information Theory*, Vol. 10 (1964), 116-118.

[8] B. Stevens and R. Strong, Problems and Solutions. Solutions, A Sudoku Solution from Orthogonal Latin Squares: 11192, *The American Mathematical Monthly*, Vol. 114 (2007), 839-840.

[9] A.P. Street and D.J. Street, *Combinatorics of Experimental Design*, Oxford University Press, New York, 1987.

John Ethier, Department of Mathematical and Computer Sciences, Metropolitan State College of Denver, Denver, CO 80217, U.S.A.; Email: `jethier@mscd.edu.`

Gary L. Mullen, Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, U.S.A.; Email: `mullen@math.psu.edu.`

Daniel Panario, Brett Stevens and David Thomson, School of Mathematics and Statistics, Carleton University, Ottawa, ON, K1S 5B6, Canada; Email: {daniel,brett,dthomson}@math.carleton.ca.