Sets of Orthogonal Hypercubes

Gary L. Mullen

Penn State University

mullen@math.psu.edu

Dec. 2013

Latin Squares

A latin square (LS) of order n is an $n \times n$ array based on n distinct symbols, each occuring once in each row and each col.

Two LSs are orthogonal if when superimposed, each of the n^2 pairs occurs once.

$$\begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix} \qquad \begin{matrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{matrix}$$

A set $\{L_1, \ldots, L_t\}$ is mutually orthogonal (MOLS) if L_i orth. L_j for all $i \neq j$

A set $\{L_1, \ldots, L_t\}$ is mutually orthogonal (MOLS) if L_i orth. L_j for all $i \neq j$

Let $N(n)$ be the max number of MOLS order n

Theorem (HMWK prob.)

$N(n) \leq n - 1$

Theorem (Moore, Bose)

If q is a prime power, $N(q) = q - 1$

Theorem (Moore, Bose)

If q is a prime power, $N(q) = q - 1$

Next Fermat Prob. (Prime Power Conj.) There are $n - 1$ MOLS order n iff n is prime power.

Conjecture (Euler 1782)

If $n = 2(2k+1)$ *(*n *is odd multiple of 2) then no pair MOLS of order* n*;*
i.e. $N(n) = 1$

Conjecture (Euler 1782)

If $n = 2(2k+1)$ *(*n *is odd multiple of 2) then no pair MOLS of order* n*; i.e.* $N(n) = 1$

Theorem (Tarry 1900)

$N(6) = 1$

Conjecture (Euler 1782)

If $n = 2(2k+1)$ *(*n *is odd multiple of 2) then no pair MOLS of order* n*; i.e.* $N(n) = 1$

Theorem (Tarry 1900)

$N(6) = 1$

Euler Conj. false at $n = 10$ (and all other $n = 2(2k+1), k \geq 2$

Theorem (Bose, Parker, Shrikhande 1960)

If $n \neq 2, 6$, $N(n) \geq 2$

Conjecture (Euler 1782)

If $n = 2(2k+1)$ *(*n *is odd multiple of 2) then no pair MOLS of order* n*; i.e.* $N(n) = 1$

Theorem (Tarry 1900)

$N(6) = 1$

Euler Conj. false at $n = 10$ (and all other $n = 2(2k+1), k \geq 2$

Theorem (Bose, Parker, Shrikhande 1960)

If $n \neq 2, 6$*,* $N(n) \geq 2$

Prob. $2 \leq N(10) \leq 6$

Prob. Find formula for $N(n)$ if n not prime power.

Hypercubes

For $d \geq 2$, a d-dimensional hypercube of order n is an $n \times \cdots \times n$ array with n^d points based on n distinct symbols so that if any coordinate is fixed, each of the n sym. occurs n^{d-2} times in that subarray.

H_1 orth. H_2 if upon superposition, each of the n^2 pairs occurs n^{d-2} times.

$\{H_1, \ldots, H_t\}$ mutually orth. if H_i orth. H_j for all $i \neq j$

Let $N_d(n)$ be max number of orth. hcubes order n and dim. d

Theorem

Let $n = q_1 \times \cdots \times q_r, q_1 < \cdots < q_r$ *prime powers*

$$\frac{q_1^d - 1}{q_1 - 1} - d \leq N_d(n) \leq \frac{n^d - 1}{n - 1} - d$$

Other Notions of Orthogonality for Hcubes

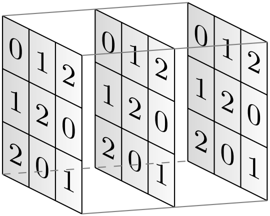
Many of the following results are due to John Ethier

Ph. D. thesis, Penn State, 2008

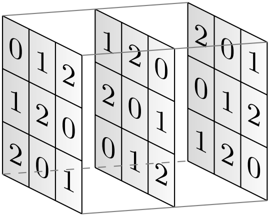
For $1 \leq t \leq d$, a t- subarray, is a subset of hcube obtained by fixing $d - t$ coordinates, running the other coordinates.

Ex: If $d = 2$, a 1-subarray is a row or a col.

An hcube has type j, $0 \leq j \leq d-1$, if in each $(d-j)$-dim. subarray, each sym. occurs exactly n^{d-j-1} times.



has type 1.



has type 2.

A set of d hcubes, dim. d, order n, is d-orth. if each of the n^d, d-tuples occurs once.

A set of $j \geq d$ hcubes is mutually d-orth (MdOH) if any d hcubes are d-orth.

Theorem

If $d \geq 2$, max # MdOH, type 0, order n and dim. d is $\leq n + d - 1$.

Codes

An (l, n^d, D) code has length l, n^d codewords, and min. dist. D

Theorem (Singleton)

$D \leq l - d + 1$

Code is MDS if $D = l - d + 1$

Theorem

A set of $l \geq d$, d-orth hcubes order n, dim. d, type 0 is equivalent to an n-ary MDS $(l, n^d, l - d + 1)$ code.

Theorem

A set of $l \geq d$, d-orth hcubes order n, dim. d, type 0 is equivalent to an n-ary MDS $(l, n^d, l-d+1)$ code.

Corollary (Golomb)

A set of $l-2$ MOLS order n is equivalent to an n-ary MDS $(l, n^2, l-1)$ code.

r hcubes order n, dim. d are mutually strong d-orth (MSdOH) if upon superposition of corresponding j-subarrays of any j hcubes with $1 \leq j \leq min(d, r)$, each j-tuple occurs exactly once.

Note:

1. If $d = 2$ and $r \geq 2$ implies MOLS
2. If $r \geq d$ strong d-orth. implies d-orth

r hcubes order n, dim. d are mutually strong d-orth (MSdOH) if upon superposition of corresponding j-subarrays of any j hcubes with $1 \leq j \leq min(d, r)$, each j-tuple occurs exactly once.

Note:

1. If $d = 2$ and $r \geq 2$ implies MOLS
2. If $r \geq d$ strong d-orth. implies d-orth

Theorem

If $l > d$, a set of $l - d$ MSdOH order n, dim. d, is equiv. to an n-ary MDS $(l, n^d, l - d + 1)$ code.

r hcubes order n, dim. d are mutually strong d-orth (MSdOH) if upon superposition of corresponding j-subarrays of any j hcubes with $1 \leq j \leq min(d, r)$, each j-tuple occurs exactly once.

Note:

1. If $d = 2$ and $r \geq 2$ implies MOLS
2. If $r \geq d$ strong d-orth. implies d-orth

Theorem

If $l > d$, a set of $l - d$ MSdOH order n, dim. d, is equiv. to an n-ary MDS $(l, n^d, l - d + 1)$ code.

Theorem

There are at most $n - 1$ MSdOH order n, dim. $d \geq 2$.

Theorem

An n-ary MDS $(d, n^{d-1}, 2)$ code is equiv. to an hcube of order n, dim. $d-1$, and type $d-2$.

Theorem

An n-ary MDS $(d, n^{d-1}, 2)$ code is equiv. to an hcube of order n, dim. $d-1$, and type $d-2$.

Theorem

The # of $(d-1)$-dim. hcubes order n, type $d-2$ equals the # of n-ary $(d, n^{d-1}, 2)$ MDS codes

Theorem

An n-ary MDS $(d, n^{d-1}, 2)$ code is equiv. to an hcube of order n, dim. $d-1$, and type $d-2$.

Theorem

The # of $(d-1)$-dim. hcubes order n, type $d-2$ equals the # of n-ary $(d, n^{d-1}, 2)$ MDS codes

Theorem

(i) Let $S(n,l,d)$ be # sets of $l-d$, MSdOH order n, dim d, type $d-1$
(ii) Let $L(n,l,d)$ be # n-ary MDS $(l, n^d, l-d+1)$ codes. Then

$$L(n,l,d) = (l-d)!S(n,l,d).$$

Constructions of Hypercubes

Lemma

A poly. $a_1x_1 + \cdots + a_dx_d$, *not all* $a_i = 0 \in F_q$ *gives an hcube order* q, *dim.* d.

(type $j-1$ if j, $a_i \neq 0$).

Constructions of Hypercubes

Lemma

A poly. $a_1x_1 + \cdots + a_dx_d$, *not all* $a_i = 0 \in F_q$ *gives an hcube order* q, *dim.* d.

(type $j-1$ if j, $a_i \neq 0$).

Theorem

Let $f_i(x_1, \ldots, x_d) = a_{i1}x_1 + \cdots + a_{id}x_d$, $i = 1, \ldots, r$ *be polys. over* F_q. *The corres. hcubes are MSdOH order* q, *dim.* d *iff every square submatrix of* $M = (a_{ij})$ *is nonsing.*

Constructions of Hypercubes

Lemma

A poly. $a_1x_1 + \cdots + a_dx_d$*, not all* $a_i = 0 \in F_q$ *gives an hcube order* q*, dim.* d*.*

(type $j-1$ if j, $a_i \neq 0$).

Theorem

Let $f_i(x_1, \ldots, x_d) = a_{i1}x_1 + \cdots + a_{id}x_d$*,* $i = 1, \ldots, r$ *be polys. over* F_q*. The corres. hcubes are MSdOH order* q*, dim.* d *iff every square submatrix of* $M = (a_{ij})$ *is nonsing.*

Theorem

Let f_i *be a set of* $t \geq d$ *lin. polys. over* F_q*. The corres. hcubes of order* q*, dim.* d *are* d*-orth iff every* d *rows of* M *are lin. indep.*

Non-prime powers - Kronecker product

Glue smaller hcubes together to get larger ones of same dim.

Conjecture

The max # of mutually d-orth hcubes order n, dim. d, $n > d$ satisfies

$$\begin{cases} n+2 & \textit{for } d = 3 \textit{ and } d = n-1 \textit{ both with } n \textit{ even} \\ n+1 & \textit{in all other cases} \end{cases}$$

Conjecture

The max # of mutually d-orth hcubes order n, dim. d, $n > d$ satisfies

$$\begin{cases} n+2 & \text{for } d=3 \text{ and } d=n-1 \text{ both with } n \text{ even} \\ n+1 & \text{in all other cases} \end{cases}$$

Conjecture

The max # of mutually strong d-orth hcubes order n, dim. d, $n > d$ satisfies

$$\begin{cases} n+2-d & \text{for } d=3 \text{ and } d=n-1 \text{ both with } n \text{ even} \\ n+1-d & \text{in all other cases} \end{cases}$$

For $2 \le k \le d$, k hcubes order n, dim. d are k-**orth** if each of the n^k, k-tuples occurs exactly n^{d-k} times.

For $2 \leq k \leq d$, k hcubes order n, dim. d are k-**orth** if each of the n^k, k-tuples occurs exactly n^{d-k} times.

Theorem

For a set of t lin. polys. over F_q with the property that any k poly. represent k-orth hcubes

$$t \leq q^{d-k+1} + q^{d-k} + \cdots + q + k - 1$$

For $2 \leq k \leq d$, k hcubes order n, dim. d are k-**orth** if each of the n^k, k-tuples occurs exactly n^{d-k} times.

Theorem

For a set of t lin. polys. over F_q with the property that any k poly. represent k-orth hcubes

$$t \leq q^{d-k+1} + q^{d-k} + \cdots + q + k - 1$$

Conjecture

Let $d \geq 2$. The max # of mutually k-orth hcubes order n, dim. d, type 0 is

$$n^{d-k+1} + n^{d-k} + \cdots + n + k - 1$$

Hypercubes of class r

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: A hypercube of dimension 3, order 3, and class 2.

Definition

Let d, n, r, t *be integers, with* $d > 0, n > 0, r > 0$ *and* $0 \leq t \leq d - r$. *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.*

Definition

Let d, n, r, t be integers, with $d > 0, n > 0, r > 0$ and $0 \leq t \leq d - r$. 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 $d \geq 2r$, 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.

Definition

Let d, n, r, t be integers, with $d > 0, n > 0, r > 0$ and $0 \leq t \leq d - r$. 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 $d \geq 2r$, 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.

Theorem

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

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

Lemma

Let n be a power of a prime, let d, r be positive integers with $d \geq 2r$ and let $q = n^r$. Consider F_q as a vector space over F_n, and define $c_j \in F_q$, $j = 1, 2, \ldots, d$, such that any r of them form a linearly independent set in F_q. The hypercube constructed from the polynomial $c_1 x_1 + \cdots + c_d x_d$ is a hypercube of dimension d, order n, class r and type r.

Lemma

Let n be a power of a prime, let d, r be positive integers with $d \geq 2r$ and let $q = n^r$. Consider F_q as a vector space over F_n, and define $c_j \in F_q$, $j = 1, 2, \ldots, d$, such that any r of them form a linearly independent set in F_q. The hypercube constructed from the polynomial $c_1 x_1 + \cdots + c_d x_d$ is a hypercube of dimension d, order n, class r and type r.

Theorem

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

Corollary

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.

Corollary

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.

Corollary

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.

Problems

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

Problems

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 the previous Theorem 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.

Problems

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 the previous Theorem 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 for mutually orthogonal hypercubes when n is not a prime power. Such constructions will require a new method not based on finite fields.

Other Kinds of Orthogonality

Höhler (1970) studies hcubes involving an extra condition for orth.

For $d \geq 2$ max number Höhler orth hcubes is $(n-1)^{d-1}$.

Other Kinds of Orthogonality

Höhler (1970) studies hcubes involving an extra condition for orth.

For $d \geq 2$ max number Höhler orth hcubes is $(n-1)^{d-1}$.

Theorem (Höhler 1970)

For $d > 2$ max reached iff n is a prime power!!

Other Kinds of Orthogonality

Höhler (1970) studies hcubes involving an extra condition for orth.

For $d \geq 2$ max number Höhler orth hcubes is $(n-1)^{d-1}$.

Theorem (Höhler 1970)

For $d > 2$ max reached iff n is a prime power!!

Morgan studies equi-orthogonal hcubes (special case of strong orthogonality)

References

Dénes/Keedwell, "Latin Squares," Academic Press, 1974

Dénes/Keedwell, "Latin Squares," North Holland, 1991

Mullen, "A candidate for the next Fermat problem," Math. Intell., 1995

Laywine/Mullen/Whittle, D-dim. hcubes ..., Monatsh. Math., 1995

Morgan, "Construction of sets of orth. freq. hcubes," Disc. Math., 1998

Laywine/Mullen, "Discrete Math. Using LSs," Wiley, 1998

Colbourn/Dinitz, “Handbook of Comb. Designs,” CRC Press, 2007

Ethier/Mullen, “Strong Forms of Orthogonality for Sets of Hypercubes,” Disc. Math. 2012

Ethier/Mullen “Strong forms of orthogonality for sets of frequency hypercubes,”Quasigroups and Related Systems, 2013.

Ethier/Mullen/Panario/Stevens/Thomson, “Sets of orthogonal hypercubes of class r,” J. Combin. Thy., A 2011.