The geometry of sets of orthogonal frequency hypercubes

Mavron, V. C.; McDonough, Thomas; Mullen, Gary L.

Published in:
Journal of Combinatorial Designs

DOI:
10.1002/jcd.20135

Publication date:
2006

Citation for published version (APA):
Mavron, V. C., McDonough, T., & Mullen, G. L. (2006). The geometry of sets of orthogonal frequency hypercubes. *Journal of Combinatorial Designs*, *15*(6), 449-459. https://doi.org/10.1002/jcd.20135

The Geometry of Sets of Orthogonal Frequency Hypercubes

V. C. Mavron* T. P. McDonough* Gary L. Mullen†

10/01/2006; revised 04/09/2006

Abstract

We extend the notion of a framed net, introduced by D. Jungnickel, V.C. Mavron, and T.P. McDonough in The geometry of frequency squares, *J. Combinatorial Theory A*, **96** (2001), 376–387, to that of a d-framed net of type ℓ, where $d \geq 2$ and $1 \leq \ell \leq d-1$, and we establish a correspondence between d-framed nets of type ℓ and sets of mutually orthogonal frequency hypercubes of dimension d. We provide a new proof of the maximal size of a set of mutually orthogonal frequency hypercubes of type ℓ and dimension d, originally established by C.F. Laywine, G.L. Mullen, and G. Whittle in D-dimensional hypercubes and the Euler and MacNeish conjectures, *Monatsh. Math.* **119** (1995), 223–238, and we obtain a geometric characterization of the framed net when this bound was satisfied as a PBIBD based on a d-class association Hamming scheme $H(d, n)$.

1 Introduction

In [7] the authors established a correspondence between sets of mutually orthogonal frequency squares (MOFS) and nets satisfying an extra property, which they called

*Institute of Mathematical and Physical Sciences, The University of Wales, Aberystwyth SY23 3BZ, United Kingdom, Email: vcm@aber.ac.uk, tpd@aber.ac.uk

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

framed nets. They provided a new proof for the maximal size of a set of MOFS and obtained a geometric characterization of the framed net when this bound was satisfied. In this paper we extend these ideas to sets of mutually orthogonal frequency hypercubes of dimension $d \geq 2$ and d-framed nets. Corresponding to sets of mutually orthogonal frequency hypercubes of a given type ℓ we introduce the concept of a d-framed net of type ℓ. We provide a new proof of the maximal size of a set of a set of mutually orthogonal frequency hypercubes of type ℓ and dimension d, originally established in [9]. We obtain a geometric characterization of the framed net when this bound was satisfied, and show that it is a PBIBD based on a d-class association Hamming scheme $H(d, n)$.

In Section 2 we recall the basic concepts relating to hypercubes and association schemes. In Section 3 we introduce the concepts of a *frame* and a *framed net*, we set up the correspondence between sets of mutually orthogonal frequency hypercubes and framed nets, and we identify the framed nets in the extremal case, postponing some of the detailed calculations to Section 5 where various polynomial identities are established. In Section 4 we give an explicit construction of the framed nets arising in the case of a particular family of parameters.

2 Basic definitions

Let $d \geq 2$ be a fixed positive integer and let $n = m\mu$. By an $F_d(n; \mu)$ *frequency hypercube* H is meant an $n \times \cdots \times n$ array $[H_{(j_1,\ldots,j_d)}]$ of dimension d, size n, and order m (i.e. each index j_i belongs to an n-set N_i and the entries belong to an m-set S) with the property that when any one of the d indices is fixed, each of the m distinct symbols appears exactly n^{d-1}/m times in that subarray. Two such hypercubes are said to be *orthogonal* if when superimposed, each of the m^2 possible ordered pairs occurs exactly n^d/m^2 times. Moreover a set of r (≥ 2) $F_d(n; \mu)$ frequency hypercubes is said to be *orthogonal* if its elements are pairwise orthogonal. More generally, we say that a frequency hypercube $F_d(n; \mu)$ has *type* ℓ, with $1 \leq \ell \leq d-1$, if, when any ℓ of the d coordinates are fixed, each of the m distinct symbols appears exactly $n^{d-\ell}/m$ times in that subarray. If $\ell \geq 2$, a hypercube of type ℓ is clearly of type $\ell - 1$ also. Hypercubes of the maximal type $d-1$ are sometimes referred to as *permutation cubes*; see, for example, [5, pp. 181-186].

Several examples illustrating this terminology and notation may be in order. An $F_2(n; 1)$ hypercube is simply a latin square of order n, and an $F_2(n; \mu)$ hypercube is an $F(n; \mu)$ frequency square of size n based upon m distinct symbols; see for example [6]. In both of these cases, the squares are of type $\ell = 1$ since in both the study of latin and frequency squares, one fixes a row or a column, and then counts the number of times (once in the case of latin squares and $\mu \geq 1$ in the case of frequency

squares) that each of the m symbols occurs in each row and in each column. For $d \geq 2$, an $F_d(n;1)$ frequency hypercube is a d-dimensional latin hypercube of order n as discussed in [9]. We refer to [11] for constructions of sets of orthogonal frequency hyperrectangles based upon a prime power number of symbols, and to [4] for some related results by type. See also [9] for some results related to latin hypercubes.

In Section 3 we prove that the maximum number r of mutually orthogonal frequency hypercubes of type ℓ and of the form $F_d(n;\mu)$ with $n = m\mu$, is bounded above by

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

See [9] or [8] for alternative proofs of this inequality. Moreover, in the case when $n = q^e$ where q is a prime power and $e \geq 1$, we construct a complete set of orthogonal $F_d(q^e; q^{e-1})$ hypercubes of type ℓ.

An *association scheme* with d classes on a finite set X is a set of symmetric $\{0,1\}$-matrices $A_0, \ldots, A_d$ with rows and columns indexed by X, such that

(i) $A_0 = I$, where I denotes the identity matrix,
(ii) $\sum_{i=0}^{d} A_i = J$, where J denotes the all-one matrix,
(iii) $A_i A_j$ lies in the real span of $A_0, \ldots, A_d$.

Two elements $x_1, x_2 \in X$ are *i-th associates* if the (x_1, x_2)-entry of A_i is 1. We refer the reader to [2] for general properties of association schemes.

A *Hamming scheme* $H(d,n)$ is an association scheme defined on a set X of size n^d, together with a bijection δ from X to the set of d-tuples S^d of an n-set S, where two elements $x_1, x_2 \in X$ are i-th associates if the n-tuples $\delta(x_1)$ and $\delta(x_2)$ differ in exactly i places.

Let X be a v-set. A *d-class partially balanced incomplete block design (d-class PBIBD)* is a design, on whose point set X is defined a d-class association scheme, such that, for $i = 0, \ldots, d$, the number of blocks on a pair of points which are i-th associates depends only on i. We will denote this number by λ_i.

A d-class PBIBD with $\lambda_1 = \cdots = \lambda_d = \lambda$ is a *balanced incomplete block design (BIBD)*, i.e. a $2-(v,k,\lambda)$-design. A design D is said to be *resolvable* if its blocks can be partitioned into subsets called *parallel classes*, each of which partitions the point set of the design. If the resolution of D is such that any two blocks from different parallel classes meet in a constant number μ of points, then D is said to be an *affine* design.

As defined in [3], an (m, r, μ)-net N is an affine $1-(\mu m^2, \mu m, r)$ design and conversely. As a result, the number of blocks in a parallel class of N is m, and any two non-parallel blocks meet in μ points and there are r parallel classes. It is known from Bose's theorem (see [3]) that $r \leq (\mu m^2 - 1)/(m-1)$ for any $(m, r; \mu)$-net N,

with equality if and only if N is a 2-design. In this case, N is a 2-$(\mu m^2, \mu m, \lambda)$ design with $\lambda = (\mu m - 1)/(m - 1)$ and is called a *complete net*.

3 Nets and mutually orthogonal hypercubes

In [7] the authors studied a particular kind of net, called a *framed net*, which turned out to be equivalent to a set of orthogonal frequency squares. We generalize this notion to higher dimensions.

A *d-frame* on an n^d-set X is a d-tuple $[X_1 : X_2 : \ldots : X_d]$, where each X_i, $1 \le i \le d$, is a partition $\{X_{i,1}, \ldots, X_{i,n}\}$ of X into n subsets each of cardinality n^{d-1} such that for any $t \in \{1, \ldots, d\}$, any t-subset $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, d\}$, and any t-tuple $(j_1, \ldots, j_t) \in \{1, \ldots, n\}^d$,

$$|X_{i_1,j_1} \cap \cdots \cap X_{i_t,j_t}| = n^{d-t}. \tag{1}$$

Note that a d-frame on X introduces a natural bijection $\{1, \ldots, n\}^d \to X$ in which $(j_1, \ldots, j_d)$ maps to the unique element of $X_{1,j_1} \cap \cdots \cap X_{d,j_d}$. Using this bijection, we may transfer the Hamming scheme to X and speak of two points of X being i-th associates when the corresponding points of $\{1, \ldots, n\}^d$ are i-th associates.

A *d-framed* $(m, r; n^d/m^2)$*-net* of *type* ℓ, with $1 \le \ell \le d-1$, is an $(m, r; n^d/m^2)$-net D whose point set X admits a d-frame $[X_1 : X_2 : \ldots : X_d]$, with $X_i = \{X_{i,1}, \ldots, X_{i,n}\}$ for $1 \le i \le d$, such that, for any $t \in \{1, \ldots, \ell\}$, any t-set $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, d\}$, any t-tuple $(j_1, \ldots, j_t) \in \{1, \ldots, n\}^t$, and for any block B of D,

$$|B \cap X_{i_1,j_1} \cap \cdots \cap X_{i_t,j_t}| = n^{d-t}/m. \tag{2}$$

The framed $(m, r; \mu^2)$-net considered in [7] is a 2-framed $(m, r; \mu^2)$-net of type 1.

The next result generalizes Theorem 3.2 of [7].

Theorem 3.1 *Let $\ell \ge 1$. There exists a set of r mutually orthogonal frequency hypercubes of the form $F_d(n; \mu)$ and type ℓ if and only if there exists a d-framed $(m, r; n^d/m^2)$-net of type ℓ.*

Proof: Let $H^{(1)}, \ldots, H^{(r)}$ be mutually orthogonal frequency hypercubes of the form $F_d(n; \mu)$ and type ℓ defined on the set $S = \{1, \ldots, m\}$. Construct a design D whose point set X is the set of ordered d-tuples $(j_1, \ldots, j_d)$ with $1 \le j_1, \ldots, j_d \le n$, and whose blocks are the point sets

$$B_x^{(u)} = \{(j_1, \ldots, j_d) \,:\, H^{(u)}_{(j_1,\ldots,j_d)} = x\} \tag{3}$$

for $1 \le u \le r, x \in S$.

Since $H^{(u)}$ is an $F_d(n;\mu)$ frequency hypercube, each element $s \in S$ appears n^d/m times in $H^{(u)}$ so that $B_x^{(u)}$ contains exactly n^d/m points. The set $\{B_x^{(u)} : s \in S\}$ partitions the point set of D for any u with $1 \le u \le r$. Now let $1 \le u, v \le r$ and $x, y \in S$. If $u = v$ and $x \ne y$, $B_x^{(u)}$ and $B_y^{(v)}$ do not meet. If $u \ne v$, $B_x^{(u)}$ and $B_y^{(v)}$ meet in n^d/m^2 points by orthogonality of the hypercubes $H^{(u)}$ and $H^{(v)}$. Hence, D is an $(m, r; n^d/m^2)$-net.

For $i \in \{1, \ldots, d\}$ and $k \in \{1, \ldots, n\}$, define $X_{i,k} = \{(j_1, \ldots, j_d) \in X : j_i = k\}$. Then $|X_{i,k}| = n^{d-1}$. Also, for $i = 1, \ldots, d$, $X_i = \{X_{i,1}, \ldots, X_{i,n}\}$ is a partition of X. It is trivial to verify that $[X_1 : \ldots : X_d]$ is a d-frame on X.

Let $1 \le t \le \ell$. Let $\{i_1, \ldots, i_t\}$ be a t-set from $\{1, \ldots, \ell\}$ and let $\{j_1, \ldots, j_t\} \in \{1, \ldots, n\}^t$. Since the hypercube $H^{(u)}$ is of type ℓ, there are exactly n^{d-t}/m d-tuples in X with the entries in positions $i_1, \ldots, i_t$ prescribed as $j_1, \ldots, j_t$, respectively, and for which the corresponding entry in $H^{(u)}$ is a given $x \in S$. In other words,

$$\left|B_x^{(u)} \cap X_{i_1,j_1} \cap \cdots \cap X_{i_t,j_t}\right| = n^{d-t}/m. \tag{4}$$

Hence D is a d-framed net of type ℓ.

Conversely, assume D is a d-framed $(m, r; n^d/m^2)$-net of type ℓ, with d-frame $[X_1 : \cdots : X_d]$, where $X_i = \{X_{i,1}, \ldots, X_{i,n}\}$. Then each point of D is uniquely expressible as the single element of an intersection $X_{1,i_1} \cap \cdots \cap X_{d,i_d}$. Let $K = \{K_1, \ldots, K_m\}$ be a parallel class of D and define a hypercube H by $H_{(i_1,\ldots,i_d)} = x$ if and only if $X_{1,i_1} \cap \cdots \cap X_{d,i_d} \subseteq K_x$.

Since D has type ℓ, for any $t \in \{1, \ldots, \ell\}$, any t-set $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, d\}$, any t-tuple $(j_1, \ldots, j_t) \in \{1, \ldots, n\}^t$, and for any block K_x of K,

$$|K_x \cap X_{i_1,j_1} \cap \cdots \cap X_{i_t,j_t}| = n^{d-t}/m. \tag{5}$$

That is, the number of entries in H which are equal to x with the t positions $i_1, \ldots, i_t$ prescribed as $j_1, \ldots, j_t$, respectively, is exactly n^{d-t}/m. So, H is an $F_d(n;\mu)$ frequency hypercube of type ℓ.

Now let H and H' be hypercubes corresponding to different parallel classes K and K'. Let (x, y) be a pair with $1 \le x, y \le m$. The number of d-tuples $(i_1, \ldots, i_d)$ with $H_{(i_1,\ldots,i_d)} = x$ and $H'_{(i_1,\ldots,i_d)} = y$ is $|K_x \cap K'_y| = n^d/m^2$, so the hypercubes H and H' are indeed orthogonal. □

The next Theorem generalizes Theorem 3.5 of [7]. First, we introduce the polynomials

$$p^{(d,\ell)}(x) = \sum_{k=\ell+1}^{d} \binom{d}{k} x^k \text{ and } q_i^{(d,\ell)}(x) = \sum_{k=0}^{\ell} (-1)^{\ell-1+k} \binom{i}{k} \binom{d-1-i}{\ell-k} x^k \tag{6}$$

for $i, \ell = 0, \ldots, d-1$.

Theorem 3.2 *Let $1 \le \ell \le d-1$ and suppose that there is a d-framed $(m, r; n^d/m^2)$-net of type ℓ. Then $r \le p^{(d,\ell)}(n-1)/(m-1)$, with equality if, and only if, the net is a PBIBD based on a d-class association Hamming scheme $H(d,n)$. In this case, for $i = 1, \ldots, d$, the number of blocks on a pair of points which are i-th associates is $r\left((m-1)q_{d-i}^{(d,\ell)}(n-1)/p^{(d,\ell)}(n-1)+1\right)/m$.*

Proof: Consider the d-framed $(m, r; n^d/m^2)$-net Δ of type ℓ with d-frame $[X_1 : \cdots : X_d]$, where $X_i = \{X_{i1}, \ldots, X_{in}\}$. Any point of Δ is uniquely expressible in the form $X_{1,j_1} \cap \cdots \cap X_{d,j_d}$. Let P be the point $X_{1,1} \cap \cdots \cap X_{d,1}$.

For any point $Q \ne P$, let λ_Q be the number of blocks on P and Q. Counting pairs (Q, B), where Q is a point different from P and B is a block on both P and Q, we obtain $\sum_{Q \ne P} \lambda_Q = r(n^d/m - 1)$. Counting ordered triples (Q, B, B'), where B, B' are distinct blocks on P and Q and $Q \ne P$, we obtain $\sum_{Q \ne P} \lambda_Q(\lambda_Q - 1) = r(r-1)(n^d/m^2 - 1)$. Hence, $\sum_{Q \ne P} \lambda_Q^2 = r(r-1)(n^d/m^2 - 1) + r(n^d/m - 1)$.

For any t with $0 \le t \le d$, let N_t be the set of points $X_{1,j_1} \cap \cdots \cap X_{d,j_d}$ for which exactly t of the $j_1, \ldots, j_d$ are equal to 1. Clearly, $|N_t| = \binom{d}{t}(n-1)^{d-t}$. Note also that $N_d = \{P\}$. For $i = 1, \ldots, d$, define $\delta_i = (1/|N_i|)\sum_{Q \in N_i} \lambda_Q$.

Now suppose that $0 \le t \le \ell$. For any t-subset $U = \{i_1, \ldots, i_t\}$ of the set $E = \{1, \ldots, d\}$, let $X_U = X_{i_1,1} \cap \cdots \cap X_{i_t,1}$. Then $\sum_{Q \in X_U,\ Q \ne P} \lambda_Q$ is the number of pairs (Q, B) with $Q \in X_U$, $Q \ne P$ and B a block on P and Q. Hence, $\sum_{Q \in X_U,\ Q \ne P} \lambda_Q = r\left(n^{d-t}/m - 1\right)$. So, $\sum_{U \subseteq E, |U|=t} \sum_{Q \in X_U,\ Q \ne P} \lambda_Q = r\binom{d}{t}\left(n^{d-t}/m - 1\right)$. However, $\sum_{U \subseteq D, |U|=t} \sum_{Q \in X_U,\ Q \ne P} \lambda_Q = \sum_{i=t}^{d-1} \sum_{Q \in N_i} \binom{i}{t}\lambda_Q = \sum_{i=t}^{d-1} \binom{i}{t}\binom{d}{i}(n-1)^{d-i}\delta_i = \sum_{i=t}^{d-1} \binom{d}{t}\binom{d-t}{i-t}(n-1)^{d-i}\delta_i$. Hence, $\sum_{i=t}^{d-1} \binom{d-t}{i-t}(n-1)^{d-i}\delta_i = r\left(n^{d-t}/m - 1\right)$.

Moreover, $0 \le \sum_{i=0}^{d-1} \sum_{Q \in N_i} (\lambda_Q - \delta_i)^2 = \sum_{Q \ne P} \lambda_Q^2 - \sum_{i=0}^{d-1} |N_i|\delta_i^2$. We will show in Section 5 that the function

$$f(y_0, \ldots, y_{d-1}) = r(r-1)\left(\frac{n^d}{m^2} - 1\right) + r\left(\frac{n^d}{m} - 1\right) - \sum_{i=0}^{d-1} \binom{d}{i}(n-1)^{d-i} y_i^2 \quad (7)$$

achieves a maximum subject to the relations

$$\sum_{i=t}^{d-1} \binom{d-t}{i-t}(n-1)^{d-i} y_i = r\left(n^{d-t}/m - 1\right), \quad 0 \le t \le \ell, \quad (8)$$

at the point given by

$$\bar{y}_i = r\left((m-1)q_i^{(d,\ell)}(n-1)/p^{(d,\ell)}(n-1)+1\right)/m, \quad i = 0, \ldots, d-1. \quad (9)$$

A straightforward calculation will show that this maximum value is

$$\left(p^{(d,\ell)}(n-1) - r(m-1)\right) r(m-1)n^d/m^2 p^{(d,\ell)}(n-1). \quad (10)$$

Thus, $r \leq p^{(d,\ell)}(n-1)/(m-1)$.

Moreover, $r = p^{(d,\ell)}(n-1)/(m-1)$ if, and only if, $\lambda_Q = \delta_i = \bar{y}_i$ whenever $Q \in N_i$; that is, whenever P and Q are $(d-i)$-th associates in the Hamming scheme. In this case, $\lambda_i = \bar{y}_{d-i}$ for $i = 1, \ldots, d$. □

4 The classical case

In this section, for any prime power q and any positive integer $e \geq 1$, we provide a construction for a complete set of $F_d(q^e; q^{e-1})$ frequency hypercubes of type ℓ, where $1 \leq \ell \leq d-1$. We also illustrate how to construct directly the corresponding d-framed net arising in Theorem 3.2. Let F_q denote the finite field of order q.

Our hypercube construction is an extension of the polynomial representation construction provided in [10] for sets of orthogonal frequency squares. The construction of the d-framed net uses affine geometries and extends that of [7]. In reality, the two constructions are quite similar since linear polynomials over finite fields define hyperplanes in affine geometries. We first consider the hypercube construction.

Consider the collection of all linear polynomials $a_1x_1 + \cdots + a_{de}x_{de}$ over the field F_q where none of the sets of coefficients $(a_{ke+1}, \ldots, a_{(k+1)e}) = (0, \ldots, 0)$ for $k = 0, 1, \ldots, d-1$, and where no two vectors of coefficients are constant F_q multiples of each other. In this notation, when a coordinate is fixed, we are actually fixing e of the coefficients, namely $(a_{ke+1}, \ldots, a_{k+1)e})$ for some $k = 0, 1, \ldots, d-1$. Each such linear polynomial represents an $F_d(q^e; q^{e-1})$ frequency hypercube. Moreover, each hypercube is of type $d-1$ since if we fix any $d-1$ of the d coordinates, we are fixing $(d-1)e$ of the coefficients, and so the resulting linear equation $a_1x_1 + \cdots + a_{de}x_{de} = \alpha$ has exactly $q^{de-(d-1)e-1}$ solutions in F_q^{de} for any $\alpha \in F_q$. (We also note that if $\ell + 1$ of the sets of coefficients are nonzero, then the resulting hypercube will be of type ℓ.)

Moreover, since no two of the vectors of coefficients are F_q multiples of each other, any two such linear polynomials over F_q will form a linear system of rank 2, and hence they will have q^{de-2} solutions in F_q^{de} for any pair $(\alpha, \beta) \in F_q^2$. Thus the resulting hypercubes are indeed orthogonal.

We now proceed to construct the d-framed net which is equivalent to the set of orthogonal hypercubes, and which arises in Theorem 3.2. To this end, let $V = V(de, q)$ denote the de-dimensional vector space over the finite field F_q. Further let $AG(de, q)$ denote the affine geometry of dimension de over F_q.

Let $P_1, \ldots, P_d$ be any d, e-dimensional subspaces of V which satisfy $P_1 \cap \cdots \cap P_d = \{0\}$, and $V = P_1 + \cdots + P_d$. For example, one could choose a basis of V so that for $i = 0, 1, \ldots, d-1$, $P_i = \{(0, \ldots, 0, x_{ie+1}, \ldots, x_{ie+e}, 0, \ldots, 0) | x_j \in F_q, ie+1 \leq j \leq$

$ie + e\}$.

Let Δ be the net whose points are those of $AG(de, q)$ and whose blocks are the affine hyperplanes U for which $|P_i \cap U| = q^{e-1}$. Then Δ is a net since, if U is a block of Δ, then so is every block in the parallel class of U.

The number of de-dimensional subspaces containing an e-dimensional subspace S is the number of $(e-1)$-dimensional subspaces in the quotient space V/S which is of course isomorphic to the space $V(e, q)$; namely $(q^e - 1)^d/(q - 1)$. Since $V = P_1 + \cdots + P_d$, no hyperplane contains all of the $P_i, i = 1, \ldots, d$. Hence the number of parallel classes not containing any of the P_i is $(q^e - 1)^d/(q - 1)$. Hence Δ is a $(q, (q^e - 1)^d/(q - 1); q^{e-1})$-net. Moreover, since for each $i = 1, \ldots, d$, P_i has q^e cosets, the e-dimensional affine subspaces in $AG(de, q)$ parallel to any of the P_i form a d-frame for Δ. Further, two cosets say $P_i + \mathbf{x}$ and $P_j + \mathbf{y}$ meet in exactly one point in $AG(de, q)$ for any $\mathbf{x}, \mathbf{y} \in V$.

5 Polynomial identities

We complete the proof of Theorem 3.2 in this section by establishing Proposition 5.6, before which we prove some elementary results from combinatorial theory and linear algebra. Throughout this section, n, d and ℓ are integers, with $n > 1$, $d > 0$ and $0 \leq \ell < d$. The polynomials $p^{(d,\ell)}(x)$ and $q_i^{(d,\ell)}(x)$, $i = 0, \ldots, d-1$ are as defined in (6).

Proposition 5.1 *Let $0 \leq t \leq \ell$. Then* $\displaystyle\sum_{i=t}^{d-1} \binom{d-t}{i-t} x^{d-i} q_i^{(d,\ell)}(x) = -p^{(d,\ell)}(x).$

Proof: The left hand side is $\sum_{i=t}^{d-1} \binom{d-t}{i-t} x^{d-i} \sum_{k=0}^{\ell} (-1)^{\ell-1+k} \binom{i}{k} \binom{d-1-i}{\ell-k} x^k$, which upon setting $j = k + d - i$, is equal to $\sum_{i=t}^{d-1} \sum_{j=d-i}^{d-i+\ell} (-x)^j (-1)^{i+\ell-d-1} \binom{d-t}{i-t} \binom{i}{j+i-d} \binom{d-1-i}{\ell-j+d-i}$. Any term with $j < \max\{d-i, \ell+1\}$ or $j > \min\{d, d-i+\ell\}$ is clearly 0, since one of the binomial coefficients is 0. Hence, the sum may be rewritten as

$$\sum_{j=\ell+1}^{d} (-x)^j \sum_{i=t}^{d-1} (-1)^{i+\ell-d-1} \binom{d-t}{i-t} \binom{i}{j+i-d} \binom{d-1-i}{\ell-j+d-i}. \tag{11}$$

Replacing i by $d - i$, the coefficient of $(-x)^j$ is $\sum_{i=1}^{d-t} (-1)^{i+\ell-1} \binom{d-t}{i} \binom{d-i}{d-j} \binom{i-1}{j-\ell-1}$. Since $\binom{i-1}{j-\ell-1} = \sum_{s=0}^{j-\ell-1} (-1)^{j-\ell-1-s} \binom{i}{s}$, we may rewrite this coefficient as

$$\sum_{s=0}^{j-\ell-1} (-1)^{j-s} \sum_{i=1}^{d-t} (-1)^i \binom{d-t}{i} \binom{d-i}{d-j} \binom{i}{s}. \tag{12}$$

Now $\sum_{i=0}^{d-t}(-1)^i\binom{d-t}{i}\binom{d-i}{d-j}\binom{i}{s} = {}_2F_1(s-\ell, s+t-d; s-d; 1)$, where ${}_2F_1$ is the hypergeometric function; see, for example, [1]. In particular, we can apply the Chu-Vandermonde theorem [1, corollary 2.2.3] to get ${}_2F_1(s-\ell, s+t-d; s-d; 1) = (-t)_{\ell-s}/(s-d)_{\ell-s}$, where $(a)_n = a(a+1)\dots(a+n-1)$ is the rising factorial. The constraints on the parameters s, t, d and ℓ ensure that the numerator of this fraction is zero and the denominator is non-zero. Thus, $\sum_{i=0}^{d-t}(-1)^i\binom{d-t}{i}\binom{d-i}{d-j}\binom{i}{s} = 0$. So, $\sum_{i=1}^{d-t}(-1)^i\binom{d-t}{i}\binom{d-i}{d-j}\binom{i}{s} = 0$ or $-\binom{d}{j}$ according as $s > 0$ or $s = 0$. Hence, the coefficient of $(-x)^j$ in (11) is $(-1)^{j-1}\binom{d}{j}$. So, the expression in (11) is $-p^{(d,\ell)}(x)$, as required. □

We wish to acknowledge the help given by G. E. Andrews in simplifying the proof of the preceding proposition by pointing to the connection with the hypergeometric function. He also noted that the polynomial $q_i^{(d,\ell)}(x)$ is also connected with the hypergeometric function; in fact, $q_i^{(d,\ell)}(x) = (-1)^{\ell-1}\binom{d-1-\ell}{\ell}{}_2F_1(-i, -\ell; d-i-\ell; -x)$.

Corollary 5.2 *Let* $0 \le k < j \le \ell$. *Then* $\displaystyle\sum_{i=k}^{d-1}\binom{d-j}{i-k}x^{d-i}q_i^{(d,\ell)}(x) = 0$.

Proof: We form the sum $\sum_{t=k}^{j}(-1)^{j-k}\binom{j-k}{t-k}\sum_{i=t}^{d-1}\binom{d-t}{i-t}x^{d-i}q_i^{(d,\ell)}(x)$. Changing the order of summation, we get $\sum_{i=k}^{d-1}\left(\sum_{t=k}^{j}(-1)^{j-k}\binom{j-k}{t-k}\binom{d-t}{d-i}\right)x^{d-i}q_i^{(d,\ell)}(x)$, which is $\sum_{i=k}^{d-1}\binom{d-j}{i-k}x^{d-i}q_i^{(d,\ell)}(x)$. However, $\sum_{t=k}^{j}(-1)^{j-k}\binom{j-k}{t-k}(-p^{(d,\ell)}(x)) = 0$, clearly. □

Corollary 5.3 *Let* $0 \le k \le \ell$. *Then*

$$\sum_{i=k}^{d-1}\binom{d-k}{i-k}\binom{d-i-1}{\ell-k}x^{d-i}q_i^{(d,\ell)}(x) = (-1)^{\ell-k+1}p^{(d,\ell)}(x).$$

Proof: We establish the result by induction on $\ell - k$. If $k = \ell$, the left-hand side is $\sum_{i=\ell}^{d-1}\binom{d-\ell}{i-\ell}x^{d-i}q_i^{(d,\ell)}(x)$, which is $-p^{(d,\ell)}(x)$ by Proposition 5.1. Now suppose that $k < \ell$ and that we have established $\sum_{i=k+1}^{d-1}\binom{d-k-1}{i-k-1}\binom{d-i-1}{\ell-k-1}x^{d-i}q_i^{(d,\ell)}(x) = (-1)^{\ell-k}p^{(d,\ell)}(x)$. By Corollary 5.2, $\binom{d-k-1}{\ell-k}\sum_{i=k}^{d-1}\binom{d-\ell}{i-k}x^{d-i}q_i^{(d,\ell)}(x) = 0$. Subtracting the first equation from the second, we notice that the coefficient of $x^{d-i}q_i^{(d,\ell)}(x)$ on the left-hand side, when $i \ge k$, is $\binom{d-k-1}{\ell-k}\binom{d-\ell}{i-k} - \binom{d-k-1}{i-k-1}\binom{d-i-1}{\ell-k-1} = \binom{d-k}{i-k}\binom{d-i-1}{\ell-k}$. The right-hand side is $(-1)^{\ell-k+1}p^{(d,\ell)}(x)$. □

Corollary 5.4 *Let* $0 \le k \le \ell$. *Then*

$$\sum_{i=0}^{d-1}\binom{d}{i}x^{d-i}q_i^{(d,\ell)}(x)^2 = (-1)^{\ell-k+1}((x+1)^d - p^{(d,\ell)}(x))p^{(d,\ell)}(x).$$

Proof: The left-hand side is

$$\sum_{i=0}^{d-1}\binom{d}{i}x^{d-i}(-1)^{\ell-1}\sum_{k=0}^{\ell}(-1)^k\binom{i}{k}\binom{d-i-1}{\ell-k}x^k q_i^{(d,\ell)}(x)$$

$$=\sum_{k=0}^{\ell}(-1)^k(-1)^{\ell-1}x^k\sum_{i=0}^{d-1}\binom{d}{i}\binom{i}{k}\binom{d-i-1}{\ell-k}x^{d-i}q_i^{(d,\ell)}(x)$$

$$=\sum_{k=0}^{\ell}(-1)^k(-1)^{\ell-1}x^k\binom{d}{k}\sum_{i=0}^{d-1}\binom{d-i}{d-k}\binom{d-i-1}{\ell-k}x^{d-i}q_i^{(d,\ell)}(x)$$

$$=\sum_{k=0}^{\ell}(-1)^k x^k\binom{d}{k}p^{(d,\ell)}(x)$$

by Corollary 5.3. Since $\sum_{k=0}^{\ell}x^k\binom{d}{k}=(x+1)^d-p^{(d,\ell)}(x)$, the result follows. □

Proposition 5.5 *Let r, s be positive integers with $r \le s$. Let $A=[a_{i,\ell}]$ be a real positive definite symmetric $s\times s$ matrix. Let $B=[b_{i,\ell}]$ be a real $r\times s$ matrix of rank r. Let $\mathbf{c}=(c_1,\ldots,c_r)\in\mathbb{R}^r$. Then, in the $(s-r)$-flat $U=\{\mathbf{x}:\mathbf{x}B^t=\mathbf{c}\}$, where $\mathbf{x}=(x_1,\ldots,x_s)$, the quadratic form $f(x_1,\ldots,x_r)=\sum_{i,\ell=1}^{r}a_{i,\ell}x_ix_\ell$ has a unique minimum point.*

Proof: We find the critical points of f on U by the method of Lagrange multipliers. Thus, we find the critical points $(\mathbf{z},\mathbf{x})$ of the function $\mathbf{x}A\mathbf{x}^t-\mathbf{x}B^t\mathbf{z}^t+\mathbf{c}\mathbf{z}^t$, where $\mathbf{z}=(z_1,\ldots,z_r)$. These are the points $(\mathbf{z},\mathbf{x})$ satisfying

$$B\mathbf{x}^t=\mathbf{c}^t \quad\text{and}\quad B^t\mathbf{z}^t-A\mathbf{x}^t=\mathbf{0}. \tag{13}$$

The matrix of coefficients $\begin{bmatrix}0 & B\\ B^t & -A\end{bmatrix}$ is a real symmetric matrix. Suppose that 0 is one of its eigenvalues and $(\mathbf{u}^t,\mathbf{v}^t)$ is a corresponding eigenvalue. Then $B\mathbf{v}^t=\mathbf{0}$ and $B^t\mathbf{u}^t=A\mathbf{v}^t$, so that $\mathbf{v}A\mathbf{v}^t=\mathbf{0}$. As A is positive definite, $\mathbf{v}=\mathbf{0}$. Hence, $\mathbf{u}B=\mathbf{0}$. Since B has maximal rank, $\mathbf{u}=\mathbf{0}$. Hence, 0 cannot be an eigenvalue. So, equations (13) have a unique solution, giving a unique critical point for f on U. Since A is positive definite, it is clear that this critical point is a minimum point. □

Proposition 5.6 *The function $f(y_0,\ldots,y_{d-1})$, defined in (7), achieves a maximum value, subject to the relations (8), at a unique point $(\bar{y}_0,\ldots,\bar{y}_{d-1})$ given by (9). This maximum value is the expression given in (10).*

Proof: The function f is clearly negative definite and the matrix of coefficients of the relations is clearly of rank $\ell+1$. From Proposition 5.5, f has a unique maximum point on the flat defined by these relations. We will exhibit the unique solution to these relations and the auxiliary relations by the Lagrange multiplier method and determine the value of the function at this point in a series of lemmas.

We first list explicitly the relations (13) in this case. They are

$$\sum_{i=t}^{d-1} \binom{d-t}{i-t} (n-1)^{d-i} y_i = r\left(\frac{n^{d-t}}{m} - 1\right) \tag{14}$$

for $0 \le t \le \ell$, and

$$\sum_{t=0}^{\ell} \binom{d-t}{i-t} z_i = 2\binom{d}{i} y_i \tag{15}$$

for $0 \le i \le d-1$.

Next, we define

$$\bar{y}_i = \frac{r}{m}\left(\frac{(m-1)q_i^{(d,\ell)}(n-1)}{p^{(d,\ell)}(n-1)} + 1\right) \tag{16}$$

for $0 \le i \le d-1$, and

$$\bar{z}_t = \frac{2r}{m}\left(\frac{(-1)^{\ell-1}(m-1)(-n)^t}{p^{(d,\ell)}(n-1)}\binom{d}{t}\binom{d-t-1}{\ell-t} + \delta_{t,0}\right)/m \tag{17}$$

for $0 \le t \le \ell$, where $\delta_{t,0} = 1$ or 0 according as $t = 0$ or $t \ne 0$.

Lemma 5.7 *Let $0 \le t \le \ell$. Then, equation (14) is satisfied by setting $y_i = \bar{y}_i$ for $0 \le i \le d-1$.*

Proof: The left-hand side of equation (14), with $y_i = \bar{y}_i$ for $0 \le i \le d-1$, is
$\frac{r(m-1)}{mp^{(d,\ell)}(n-1)} \sum_{i=t}^{d-1} \binom{d-t}{i-t}(n-1)^{d-i} q_i^{(d,\ell)}(n-1) + \frac{r}{m}\sum_{i=t}^{d-1}\binom{d-t}{i-t}(n-1)^{d-i}$
$= -r(m-1)/m + r(n^{d-t}-1)/m = r(n^{d-t}/m - 1)$, using Proposition 5.1. □

Lemma 5.8 *Let $0 \le i \le d-1$. Then, equation (15) is satisfied by setting $y_i = \bar{y}_i$ and $z_t = \bar{z}_t$ for $0 \le t \le \ell$.*

Proof: The left-hand side of equation (15), with $z_t = \bar{z}_t$ for $0 \le t \le \ell$, is

$$\frac{2r(m-1)(-1)^{\ell-1}}{mp^{(d,\ell)}(n-1)} \sum_{t=0}^{\ell} \binom{d-t}{i-t}(-n)^t \binom{d}{t}\binom{d-t-1}{\ell-t} + \frac{2r}{m}\binom{d}{i}$$

$$= \frac{2r(m-1)(-1)^{\ell-1}}{mp^{(d,\ell)}(n-1)}\binom{d}{i}\sum_{t=0}^{\ell}(-n)^t\binom{i}{t}\binom{d-t-1}{\ell-t} + \frac{2r}{m}\binom{d}{i} \tag{18}$$

Now,

$$\sum_{t=0}^{\ell}(-n)^t\binom{i}{t}\binom{d-t-1}{\ell-t} = \sum_{t=0}^{\ell}\sum_{s=0}^{t}(1-n)^s(-1)^{t-s}\binom{t}{s}\binom{i}{t}\binom{d-t-1}{\ell-t}$$

$$= \sum_{t=0}^{\ell}\sum_{s=0}^{t}(1-n)^s(-1)^{t-s}\binom{i}{s}\binom{i-s}{t-s}\binom{d-t-1}{\ell-t}$$

$$= \sum_{s=0}^{\ell}\binom{i}{s}(1-n)^s\sum_{t=0}^{\ell}(-1)^t\binom{i-s}{t}\binom{d-s-t-1}{d-\ell-1} \tag{19}$$

Let α_s be the inner sum in (19). Then α_s is the coefficient of x^0 in the product $\sum_{t=0}^{\ell}(-1)^t\binom{i-s}{t}x^t\sum_{t=0}^{\ell}\binom{d-s-t-1}{d-\ell-1}x^{-t}$. The limits of summation of the first sum can be changed to 0 and $i-s$ and those of the second sum can be changed to $-\infty$ and $\ell-s$, without affecting the coefficient of x^0. The resulting product is $(1-x)^{i-s}(1-x)^{-(d-\ell)}x^{-(\ell-s)} = (1-x)^{-(d-i-\ell+s)}x^{-(\ell-s)}$. Note that $\ell \geq s$ and $d > i$. Hence, the coefficient of $x^{\ell-s}$ in $(1-x)^{-(d-i-\ell+s)}$ is $\binom{d-i-1}{\ell-s}$ whether $d-i > \ell-s$ or not, since in the latter case it is clearly 0. That is, $\alpha_s = \binom{d-i-1}{\ell-s}$. So, (19) is $(-1)^{\ell-1}q_i^{(d,\ell)}(n-1)$. Substituting this expression into (18), we get

$$\binom{d}{i}\frac{2r}{m}\left(\frac{(m-1)q_i^{(d,\ell)}(n-1)}{p^{(d,\ell)}(n-1)} + 1\right),$$

which is the right-hand side of (15). □

Lemma 5.9

$$f(y_0,\ldots,y_{d-1}) = \frac{\left(p^{(d,\ell)}(n-1) - r(m-1)\right)r(m-1)n^d}{m^2p^{(d,\ell)}(n-1)}$$

Proof: $\dfrac{m^2}{r^2}f(\bar{y}_0,\ldots,\bar{y}_{d-1}) - \left(\dfrac{1}{r} - \dfrac{m-1}{p^{(d,\ell)}(n-1)}\right)(m-1)n^d$

$$= -m^2 + n^d + \frac{(m-1)^2n^d}{p^{(d,\ell)}(n-1)} - \frac{(m-1)^2}{p^{(d,\ell)}(n-1)^2}\sum_{i=0}^{d-1}\binom{d}{i}(n-1)^{d-1}q_i^{(d,\ell)}(n-1)^2$$

$$-\frac{2(m-1)}{p^{(d,\ell)}(n-1)}\sum_{i=0}^{d-1}\binom{d}{i}(n-1)^{d-1}q_i^{(d,\ell)}(n-1) - \sum_{i=0}^{d-1}\binom{d}{i}(n-1)^{d-1}$$

By Proposition 5.1, $\sum_{i=0}^{d-1} \binom{d}{i}(n-1)^{d-1} q_i^{(d,\ell)}(n-1) = -p^{(d,\ell)}(n-1)$. By Corollary 5.4, $\sum_{i=0}^{d-1} \binom{d}{i}(n-1)^{d-1} q_i^{(d,\ell)}(n-1)^2 = (n^d - p^{(d,\ell)}(n-1))p^{(d,\ell)}(n-1)$. Clearly, $\sum_{i=0}^{d-1} \binom{d}{i}(n-1)^{d-1} = n^d - 1$. The result follows immediately. □

Acknowledgment The third author would like to sincerely thank the Institute of Mathematical and Physical Sciences of the University of Wales for the very warm hospitality extended to him during his visit in April 2004.

References

[1] G. E. Andrews, R. Askey, and R. Roy, *Special Functions*, Cambridge University Press, Cambridge, 1999.

[2] R. A. Bailey, *Association Schemes: Designed Experiments, Algebra and Combinatorics*, Cambridge University Press, Cambridge, 2004.

[3] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, second edition, Cambridge University Press, Cambridge, 1999.

[4] B. Cheng and G. L. Mullen, Constructions for mutually orthogonal frequency hyperrectangles of prescribed type, *Discrete Math.*, **242** (2002), 55–64.

[5] J. Dénes and A. D. Keedwell, *Latin Squares*, Academic Press, New York, 1974.

[6] A. Hedayat, D. Raghavarao, and E. Seiden, Further contributions to the theory of F-squares design, *Ann. Statist.*, **3** (1975), 712–716.

[7] D. Jungnickel, V. C. Mavron, and T. P. McDonough, The geometry of frequency squares, *J. Combin. Theory A*, **96** (2001), 376–387.

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

[9] C. F. Laywine, G. L. Mullen, and G. Whittle, D-dimensional hypercubes and the Euler and MacNeish conjectures, *Monatsh. Math.*, **119** (1995), 223–238.

[10] G. L. Mullen, Polynomial representation of complete sets of mutually orthogonal frequency squares of prime power order, *Discrete Math.*, **69** (1988), 79–84.

[11] S. J. Suchower, Polynomial representations of complete sets of frequency hyperrectangles with prime power dimensions, *J. Combin. Theory A*, **62** (1993), 46–65.