Difference Matrices, Generalized Hadamard Matrices and Orthomorphism Graphs of Groups

Anthony B. Evans
Department of Mathematics & Statistics
Wright State University
Dayton, Ohio 45435

ABSTRACT Orthomorphism graphs of groups are defined and a correspondence, between cliques of orthomorphism graphs and difference matrices and generalized Hadamard matrices, is established. Some examples of orthomorphism graphs are given. Also, for $\lambda = 1$, known values and bounds for clique numbers of orthomorphism graphs of groups of small order are surveyed.

1. INTRODUCTION.

Let G be a finite group and let $I = \{1, \cdots, \lambda\}$. We shall use g_i to denote the element $(g,i) \in G \times I$. There is a natural "binary operation" $(G \times I) \times (G \times I) \to G$ defined on $G \times I$, given by $g_i h_j = gh$. Similarly $g_i^{-1} = g^{-1}$ and $gh_i = gh$.

θ: $G \times I \to G$ is a λ-orthomorphism of G (or $\theta \in \mathrm{Orth}_\lambda(G)$) if in each of the lists $\theta(g_i)$, $g_i \in G \times I$, and $g_i^{-1}\,\theta(g_i)$, $g_i \in G \times I$, each element of G occurs exactly λ times.

Let $\theta, \phi \in \mathrm{Orth}_\lambda(G)$. We say that θ is adjacent to ϕ (written $\theta \sim \phi$) if each element of G occurs exactly λ times in the list $\theta(g_i)^{-1}\,\phi(g_i)$, $g_i \in G \times I$. Note that $\theta \sim \phi$ if and only if $\phi \sim \theta$.

The λ-orthomorphism graph of G has as its vertex set the λ-orthomorphisms of G, adjacency being defined as above. We shall use $\mathrm{Orth}_\lambda(G)$ to denote both the set of λ-orthomorphisms of G and the λ-orthomorphism graph of G. A λ-orthomorphism graph of G is any induced subgraph of $\mathrm{Orth}_\lambda(G)$.

An r-clique of an orthomorphism graph $\mathcal{H}$ is a set of r mutually adjacent orthomorphisms of $\mathcal{H}$ and $\omega(\mathcal{H})$, the clique number of $\mathcal{H}$, is the largest value of r for which an r-clique of $\mathcal{H}$ exists.

Given an orthomorphism graph $\mathcal{H}$, there are two questions that

JCMCC 1(1987), pp. 97–105

most concern us; what is the value of $\omega(\mathcal{H})$, in particular is $\omega(\mathcal{H}) = \lambda|G|-2$, and can we find cliques in $\mathcal{H}$ with certain preassigned properties.

An $(n, r; \lambda, G)$-difference matrix is an $r \times n\lambda$ matrix (a_{ij}) with entries in the group G, $|G|=n$, such that, for all i,k, $i \neq k$, each element of G occurs exactly λ-times in the list $a_{ij}^{-1} a_{kj}$, $j = 1, \cdots, n\lambda$. An (n,λ)-generalized Hadamard matrix is an $(n,n\lambda; \lambda,G)$-difference matrix.

In the next section we give some results on orthomorphism graphs, including the correspondence between difference matrices and cliques of orthomorphism graphs. In the third section we list the known values and bounds for $\omega(\mathrm{orth}_1(G))$, $|G| \leq 15$, and in the fourth section we give several examples of orthomorphism graphs.

2. Orthomorphisms and difference matrices.

In this section we give some basic results on orthomorphisms and difference matrices. We show a correspondence between cliques of orthomorphism graphs and difference matrices, and we give some constructions of orthomorphisms and cliques from other orthomorphisms and cliques. In the first result we establish a correspondence between cliques of orthomorphism graphs and difference matrices.

Theorem 2.1. Any $(n,r;\lambda,G)$-difference matrix corresponds to an $r-2$ clique of $\mathrm{Orth}_\lambda(G)$ and any $r-2$ clique of $\mathrm{Orth}_\lambda(G)$ corresponds to an $(n,r; \lambda,G)$-difference matrix.

Proof. If A is an $(n,r; \lambda,G)$-difference matrix then so is any matrix obtained from A using the following operations.

a. permuting rows

b. permuting columns

c. multiplying all the elements of a row on the right by an element of G.

d. multiplying all the elements of a column on the left by an element of G.

Thus, without loss of generality, we may assume that $a_{1j}=1$ for all j. Thus each element of G occurs exactly λ times in $a_{21},\cdots, a_{2\ n\lambda}$. If $a_{2\ j(i)}=g$ for $i = 1, \cdots, \lambda$ then identifying $a_{2\ j(i)}$ with g_i and setting $\theta_k(g_i) = a_{k+2\ j(i)}$, $k=1,\cdots,r-2$ gives rise to an r-2 clique, $\theta_1,\cdots,\theta_{r-2}$ of $\mathrm{Orth}_\lambda(G)$.

Conversely, let $\theta_1,\cdots,\theta_{r-2}$ be an r-2 clique of $\mathrm{Orth}_\lambda(G)$. We can construct an $(n,r;\lambda,G)$-difference matrix as follows. Set $a_{1j}=1$ for all j. Let $\epsilon: G\times I\to\{1,\cdots,n\lambda\}$ be a bijection and set $a_{2j} = \epsilon^{-1}(j)$, for all j, and $a_{ij} = \theta_{i-2}(a_{2j})$ for $i = 3, \cdots, r$ and all j. (a_{ij}) is an $(n,r;\ \lambda,G)$-difference matrix. □

Corollary 2.1. A (G,λ)-generalized Hadamard matrix corresponds to a $\lambda|G|-2$ clique of $\mathrm{Orth}_\lambda(G)$ and a $\lambda|G|-2$ clique of $\mathrm{Orth}_\lambda(G)$ corresponds to a (G,λ)-generalized Hadamard matrix.

Corollary 2.2.

$$\omega(\mathrm{Orth}_\lambda(G)) \le \lambda|G|-2.$$

Proof. Jungnickel [12] showed that if an $(n,r;\ \lambda,G)$-difference matrix exists then

$$r \le \lambda\ n = \lambda|G|.$$ □

In the next three theorems and their corollaries we give some methods for constructing new orthomorphisms, cliques and difference matrices from old ones. The proofs of these results are straightforward and are left to the reader.

Theorem 2.2. Let $\theta\in \mathrm{Orth}_\lambda(G)$ and let $H \trianglelefteq G$, $|H| = m$. Let $\phi: G\to G/H$ be the canonical homomorphism. Let $I'=\{1,\cdots, m\ \lambda\}$ and let

ϕ':G/H x I' → GxI be a bijection satisfying $\phi'(h_i) = g_j$ only if $\phi(g) = h$. Then $\phi\theta\phi' \in \text{Orth}_{\lambda m}(G/H)$. Further, if θ, $\Psi \in \text{Orth}_{\lambda}(G)$, $\theta \sim \Psi$, then $\phi\theta\phi' \sim \phi\Psi\phi'$.

Corollary 2.3. (See Jungnickel [12]).

If there exists an (n,r; λ,G)-difference matrix and if H $\triangleleft$ G, |H| = m, then there exists an (n/m,r;λ,G/H)-difference matrix.

Theorem 2.3. Let $\theta \in \text{Orth}_{\lambda}(G)$ and $\Psi \in \text{Orth}_{\mu}(H)$. Let I' = $\{1,\cdots,\lambda\mu\}$ and Let ϵ:I'→$\{1,\cdots,\lambda\}$ x $\{1,\cdots,\mu\}$ be a bijection, $\epsilon(i) = (\alpha(i),\beta(i))$, and define $\theta \times \Psi$:(GxH) x I' → G x H by $\theta \times \Psi\ ((g,h)_i) = (\theta(g_{\alpha(i)}), \Psi(h_{\beta(i)}))$. Then $\theta \times \Psi \in \text{Orth}_{\lambda\mu}(GxH)$. Further, if $\theta,\theta' \in \text{Orth}_{\lambda}(G)$ and $\Psi,\Psi' \in$ Orth $\mu(H)$, $\theta \sim \theta'$, $\Psi \sim \Psi'$, then $\theta \times \Psi \sim \theta' \times \Psi'$.

Corollary 2.4. (See Jungnickel [12]).

If there exists an (n, r; λ,G)-difference matrix and an (m,r;μ,H)-difference matrix then there exists an (nm, r;$\lambda\mu$,GxH)-difference matrix.

Theorem 2.4. Let $\theta \in \text{Orth}_{\lambda}(G)$ and $\Psi \in \text{Orth}_{\mu}(G)$ and let I = $\{1,\cdots,\lambda+\mu\}$. Define (θ,Ψ): G x I → G by

$$(\theta,\Psi)\ (g_i) = \begin{cases} \theta(g_i) & \text{if } i = 1,\cdots,\lambda, \\ \Psi(g_{i-\lambda}) & \text{if } i = \lambda+1,\cdots,\lambda+\mu. \end{cases}$$

Then $(\theta,\Psi) \in \text{Orth}_{\lambda+\mu}(G)$. Further, if $\theta,\theta' \in \text{Orth}_{\lambda}(G)$ and $\Psi,\Psi' \in \text{Orth}_{\mu}(G)$, $\theta \sim \theta'$, $\Psi \sim \Psi'$, then $(\theta,\Psi) \sim (\theta',\Psi')$.

Corollary 2.5. (See Jungnickel [12]).

If there exists an (n,r; λ,G)-difference matrix and an (n,r; μ,G)-difference matrix then there exists an (n,r; $\lambda + \mu$,G)-difference matrix.

3. $\omega(\mathrm{Orth}_1(G))$ for $|G| \leq 15$.

By corollary 2.2, $\omega(\mathrm{Orth}_1(G)) \leq |G|-2$. Equality is known to hold if G is an elementary abelian group, and the Bruck-Ryser theorem rules out equality for many values of $|G|$. Hall and Paige [10] proved that $\mathrm{Orth}_1(G) = \emptyset$ if the Sylow 2-subgroup of G is cyclic.

We list below the known values or bounds for $\omega(\mathrm{Orth}_1(G))$, $|G| \leq 15$, G not an elementary abelian group, and the Sylow 2-subgroup of G trivial or non-cyclic.

1. $\omega(\mathrm{Orth}_1(Z_2 \times Z_4)) = 2$. This was proved by Johnson, Dulmage and Mendelsohn [11] in 1961, using machine computation. This was later reproved by Chang, Hsiang and Tai [3] in 1964, using "massive computation" and "proof by exhaustion".

2. $\omega(\mathrm{Orth}_1(D_4)) = 1$. This was proved by Chang and Tai [4] in 1964 using the same methods as Chang, Hsiang and Tai [3].

3. $\omega(\mathrm{Orth}_1(Q_8)) = 1$. See Chang and Tai [4].

4. $\omega(\mathrm{Orth}_1(Z_9)) = 1$. See Chang, Hsiang and Tai [3].

5. $\omega(\mathrm{Orth}_1(D_6)) = 2$. See Chang, Hsiang and Tai [3]. This was later reproved by Baumert and Hall [1] in 1973, using machine computation.

6. $\omega(\mathrm{Orth}_1(A_4)) = 1$ or 2? Chang, Hsiang and Tai [3] found the answer to be 1. Later, Baumert and Hall [1] reported that no 3-clique could be found, using machine computation.

7. $\omega(\mathrm{Orth}_1(Z_6 \times Z_2)) = 4$. 4-cliques of $\mathrm{Orth}_1(Z_6 \times Z_2)$ were constructed by Bose, Chakravarti and Knuth [2] in 1960, using machine computation, and by Johnson, Dulmage and Mendelsohn [11], using hand calculations. That no larger cliques existed was established, using machine computation, by Parker and VanDuren (cited in Johnson, Dulmage and Mendelsohn [11]) in 1961 and later by Baumert and Hall [1].

8. $3 \leq \omega(\mathrm{Orth}_1(Z_{15})) \leq 12$. A lower bound of 2 was established by Keedwell [14] in 1966, using his "column method". This was improved to 3 by Schellenberg, Van Rees and Vanstone [18] in 1978. The upper bound was established by DeLauney [5] in 1984.

4. Some Examples of Orthomorphism Graphs.

We now list some known examples of orthomorphism graphs.

1. Let $a_0,\cdots,a_q$ be a planar difference set modulo $v = q^2 + q + 1$ and let $M = (m(i,j))$ be a $(q+1) \times (q+1)$ matrix with entries from $\{0,\cdots,q\}$. Define $\theta_M: a_i - a_j \to a_{m(i,j)} - a_j$. Then $\theta_M \in \mathrm{Orth}_1(Z_v)$ if and only if M is a latin square satisfying $m(i,i) = i$ for all i(See Evans [7]). $\theta_M \sim \theta_k$ if and only if M is orthogonal to K. Note, in particular, that if H denotes the orthomorphism graph induced by $\{\theta_M;$ M a latin square satisfying $m(i,i) = i$ for all $i\}$ and if N(n) denotes the maximum possible number of mutually orthogonal latin squares of order n then $N(q+1)-1 \leq \omega(H) \leq N(q+1)$.

2. Let $a_1,\cdots,a_q$ be an affine difference set modulo $v = q^2-1$ and let $M = (m(i,j))$ be a $q \times q$ matrix with entries in $\{1,\cdots,q\}$. Define

$$\theta_{M,\phi}: \begin{cases} a_i - a_j \to a_{m(i,j)} - a_j \\ i(q+1) \to (q+1)\phi(i), \quad i=0,\cdots,q-2. \end{cases}$$

Then $\theta_{M,\phi} \in \mathrm{Orth}_1(Z_v)$ if and only if M is a latin square, satisfying $m(i,i) = i$ for all i, and $\phi \in \mathrm{Orth}_1(Z_{q-1})$. $\theta_{M,\phi} \sim \theta_{K,\psi}$ if and only if M and K are orthogonal and $\phi \sim \psi$. See Jungnickel [13] for a difference matrix version of this.

3. Let $G \cong GF(q)^+$, q odd.

Set $\theta_{A,B}: x \to \begin{cases} Ax & x \text{ a square.} \\ Bx & x \text{ a nonsquare.} \\ 0 & x = 0. \end{cases}$

$\theta_{A,B} \in \mathrm{Orth}_1(G)$ if and only if both AB and (A-1)(B-1) are squares. $\theta_{A,B} \sim \theta_{C,D}$ if and only if (A-B)(C-D) is a square. (See Evans [6] and Mendesohn and Wolk [16]).

$\{\theta_{A,A^r};\ A \neq 0,1\}$ is a q-2 clique of $\mathrm{Orth}_1(G)$ and if $q = p^r$, p prime, $r > 1$, then $\{\theta_{A,A^p};\ A \neq 0,1\}$ is also a q-2 clique of $\mathrm{Orth}_1(G)$.

It is natural to ask, if q is prime, what the largest possible number n could be for which $\theta_{A(1),B(1)}, \cdots, \theta_{A(n),B(n)}$ is a clique of $\mathrm{Orth}_1(G)$ and $A(i) \neq B(i)$ for some i.

Mendelsohn and Wolk [16] showed, using machine computation, that for q = 13, n = 5 and for q = 17, n = 7. They speculated that for some prime q, n = q-2. This would imply the existence of a non-Desarguesian projective plane of prime order q. Evans [7] showed, by simple calculations, that $n \neq q-2$ for $q \leq 47$.

4. As a generalization of the above example, let $G \cong GF(q)^+$, q = ef+1, and let g be a primitive element of GF(q). The sets $C_i = \{g^{ej+i};\ j = 0, \cdots, f-1\}$, $i=0,\cdots,e-1$ are called cyclotomy classes. For $A(0),\cdots,A(e-1) \in GF(q)$ define $\theta_{A(0),\cdots,A(e-1)}$ as follows.

$$\theta_{A(0),\cdots,A(e-1)}(x) = \begin{cases} A(i)x & \text{if } x \in C_i \\ 0 & \text{if } x = 0. \end{cases}$$

$\theta_{A(0),\cdots,A(e-1)} \in \mathrm{Orth}_1(G)$ if and only if the mappings $C_i \to A(i)C_i$ and $C_i \to (A(i) - 1)\, C_i$ are both permutations of the cyclotomy classes (See Evans [8]).

$\theta_{A(0),\cdots,A(e-1)} \sim \theta_{B(0),\cdots,B(e-1)}$ if and only if the mapping $C_i \to (A(i) - B(i))C_i$ is a permutation of the cyclotomy classes.

Niederreiter and Robinson [17] have given implicit constructions of some orthomorphisms of this type.

5. If $\alpha \in \mathrm{Aut}(G)$, the automorphism group of G, then $\alpha \in \mathrm{Orth}_1(G)$ if and only if α is fixed point free, i.e. $\alpha(x) = x$ implies x is the identity element of G. Further, if we define $\bar{\alpha}$ by $\bar{\alpha}(x) = \alpha(x)^{-1}$, $\alpha \in \mathrm{Aut}(G)$, then $\bar{\alpha} \in \mathrm{Orth}_1(G)$ if and only if $\alpha(x) = y^{-1}x^{-1}y$ implies that x is the identity element of G. For $\alpha, \beta \in \mathrm{Aut}(G)$ the following hold.

i) $\alpha \sim \beta$ if and only if $\alpha\beta^{-1}$ is fixed point free.

(ii) $\bar{\alpha} \sim \bar{\beta}$ if and only if $\alpha\beta^{-1}$ is fixed point free.

(iii) $\bar{\alpha} \sim \beta$ if and only if $\beta^{-1}\alpha(x) = y^{-1}x^{-1}y$ implies that x is the identity element of G.

$\mathrm{Aut}(G) \cap \mathrm{Orth}_1(G)$ was studied by Mann [15] and $(\mathrm{Aut}(G) \cap \mathrm{Orth}_1(G)) \cup (\{\bar{\alpha};\ \alpha \in \mathrm{Aut}(G)\} \cap \mathrm{Orth}_1(G))$ by Evans [9].

REFERENCES

1. Baumert, L.; Hall, M. Jr. "Nonexistence of certain Planes of order 10 and 12" J. Combin. Theory Ser A 14(1973), 273-280.

2. Bose, R. C.; Chakravarti, I. M.; Knuth, D.E. "On Methods of Constructing Sets of Mutually Orthogonal Latin Squares using a Computer. I." Technometrics 2(1960), 507-516.

3. Chang, L.Q., Hsiang, K.; Tai, S. "Congruent Mappings and Congruence Classes of Orthomorphisms of Groups" Acta Math Sinica 14(1964), 747-756 (Chinese). Translated as: Chinese Math Acta 6(1965), 141-152.

4. Chang, L.Q.; Tai, S.S. "On the Orthogonal Relations among Orthomorphisms of Non-commutative Groups of Small Orders". Acta Math. Sinica 14(1964), 471-480 (Chinese). Translated as: Chinese Math. Acta 5(1964), 506-515.

5. De Launey, W. "On the Nonexistence of Generalized Hadamard Matrices". J. Statist. Plann. Inference 10(1984), No. 3, 385-396.

6. Evans, A.B. "Orthomorphisms of Z_p". Discrete Math., to appear

7. _____ "Orthomorphisms of Groups", submitted

8. _____ "Orthomorphisms of GF $(q)^+$", submitted.

9. _____ "Orthomorphism Graphs of Groups", submitted.

10. Hall, M.; Paige, L.J. "Complete Mappings of Finite Groups", Pacific J. Math. 5(1955), 541-549.

11. Johnson, D. M.; Dulmage, A.L.; Mendelsohn, N.S. "Orthomorphisms of Groups and Orthogonal Latin Squares I." Canad. J. Math. 13(1961), 356-372.

12. Jungnickel, D. "On Difference Matrices, Resolvable Transversal Designs and Generalized Hadamard Matrices". Math. Z. 167(1979), no. 1, 49-60.

13. _____ "On Difference Matrices and Regular Latin Squares". Abh. Math. Sem. Univ. Hamburg 50(1980), 219-231.

14. Keedwell, A.D. "On Orthogonal Latin Squares and a Class of Neofields". Rend. Mat. e Appl. (5) 25(1966), 519-561.

15. Mann, H.B. "The Construction of Orthogonal Latin Squares". Ann. Math. Statist. 13(1942), 418-423.

16. Mendelsohn, N.S.; Wolk, B. "A Search for a Nondesarguesian Plane of Prime Order." Proceedings of an international conference on Finite Geometry (Winnipeg, 1984). Lecture Notes in Pure and Applied Mathematics Vol. 103. Marcel Dekker, New York, 1985 pp.199-208.

17. Niederreiter, H.; Robinson, K.H. "Complete Mappings of Finite Fields." J. Austral. Math. Soc. Ser. A. 33(1982), 197-212.

18. Schellenberg, P.J.; Van Rees, G.H.J.; Vanstone, S.A. "Four Pairwise Orthogonal Latin Squares of Order 15." Ars Combinatoria, vol. 6(1978), 141-150.