Difference Matrices and Orthomorphisms over Non-Abelian Groups

Kathleen A.S. Quinn
Department of Pure Mathematics, The Open University,
Walton Hall, Milton Keynes MK7 6AA

Abstract

Let G be a finite group with a normal subgroup H. We prove that if there exist a $(h, r; \lambda, H)$ difference matrix and a $(g/h, r; 1, G/H)$ difference matrix, then there exists a $(g, r; \lambda, G)$ difference matrix. This shows in particular that if there exist r mutually orthogonal orthomorphisms of H and r mutually orthogonal orthomorphisms of G/H then there exist r mutually orthogonal orthomorphisms of G. We also show that a dihedral group of order 16 admits at least 3 mutually orthogonal orthomorphisms.

1 Introduction

Let G be a group of order g. A $r \times \lambda g$ matrix $D = [d_{ij}]$ is called a $(g, r; \lambda, G)$ *difference matrix* if for each $i_1, i_2 \in \{1, \ldots, r\}$, $i_1 \neq i_2$, the multiset $\{{d_{i_1 j}}^{-1} d_{i_2 j} : j = 1, \ldots, \lambda g\}$ contains each element of G precisely λ times. For example, the following is a $(4, 4; 1, K)$ difference matrix where K is the four-group $\langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle$:

$$\begin{bmatrix} e & e & e & e \\ e & a & b & ab \\ e & b & ab & a \\ e & ab & a & b \end{bmatrix}.$$

Any $(g, r; \lambda, G)$ difference matrix can be *normalized* by pre-multiplying each row and column by the inverse of the entry which appears in the first position of that row or column, to obtain a $(g, r; \lambda, G)$ difference matrix in which the first row and column contain only the identity element.

Difference matrices are discussed in the general design theory books [2] and [5]. The following is a standard composition theorem for difference matrices, due to Jungnickel [9].

Result 1.1 *If there exists a* $(g, r; \lambda, G)$ *difference matrix and a* $(g', r; \lambda', G')$ *difference matrix, then there exists a* $(gg', r; \lambda\lambda', G \times G')$ *difference matrix.*

In this note we present a partial generalisation of this result, in which we build from difference matrices over a normal subgroup H and factor group G/H of a finite group G to a difference matrix over G. This generalisation is therefore relevant to some cases where G is non-abelian. Our theorem is not a complete generalisation of the above result because we insist that $\lambda = 1$ for the difference matrix over G/H.

Difference matrices generalise the notion of *orthomorphisms* of a group. Two permutations θ_1 and θ_2 of a finite group G are said to be *orthogonal* if the mapping $x \mapsto \theta_1(x)^{-1}\theta_2(x)$ is also a permutation of G. A permutation of a group G which is orthogonal to the identity permutation is called an *orthomorphism* of G. The final $r-1$ rows of a normalized $(g, r; 1, G)$ difference matrix with $r \geq 3$ specify $r-2$ mutually orthogonal orthomorphisms of G: the first of these rows lists the elements of G and each of the other $r-2$ rows gives the respective images of these elements under an orthomorphism. Thus it is clear that a $(g, r; 1, G)$ difference matrix with $r \geq 3$ is equivalent to a set of $r-2$ mutually orthogonal orthomorphisms of G.

A set of r mutually orthogonal orthomorphisms of a group G can be used to construct a set of $r+1$ mutually orthogonal latin squares based on G. This was first observed by Mann [10], and the construction is used in [3] and [8], for example. Mann's construction is not the only way in which mutually orthogonal latin squares can be constructed from mutually orthogonal orthomorphisms of a group: [1] surveys some other ways.

Orthomorphisms have been extensively studied. The most comprehensive text on them is [6].

In [11], Paige proves the following result.

Result 1.2 *Let* G *be a finite group with a normal subgroup* H*. If both* H *and* G/H *admit an orthomorphism, then* G *admits an orthomorphism.*

(Paige states and proves the result in terms of *complete mappings* rather than orthomorphisms. A complete mapping of a group G is a permutation ϕ of G such that the mapping $x \mapsto x\phi(x)$ is a also a permutation of G. It is straightforward to verify that θ is an orthomorphism of G if and only if the mapping $x \mapsto x^{-1}\theta(x)$ is a complete mapping of G.)

The case $\lambda = 1$ of our theorem on difference matrices is a generalisation of Paige's result. We state this case as Corollary 2.2. It is a worthwhile addition to the known standard composition theorems for mutually orthogonal orthomorphisms of groups, relevant to non-abelian groups. A recent paper by Bowler [4] is essentially a particular case of Corollary 2.2.

Bowler [4] shows that a dihedral group of order $4n$, $n \equiv 1, 5 \pmod 6$, admits at least two mutually orthogonal orthomorphisms. It is also known that the maximum number of mutually orthogonal orthomorphisms of a dihedral group of order 12 is two (see [6]). In the final section of this note we show that a dihedral group of order 16 admits at least three mutually orthogonal orthomorphisms. A group whose order is twice an odd number admits no orthomorphisms, by a well-known theorem of Hall and Paige [7].

2 A composition theorem for difference matrices

Theorem 2.1 *Let G be a finite group with a normal subgroup H. If there exists both a $(h, r; \lambda, H)$ difference matrix and a $(g/h, r; 1, G/H)$ difference matrix, then there exists a $(g, r; \lambda, G)$ difference matrix.*

Proof. Let C and D be a $(h, r; \lambda, H)$ difference matrix and a $(g/h, r; 1, G/H)$ difference matrix respectively. Let $C = [c_{ij}]$. Choose any set of coset representatives for H in G, and let $U = [u_{ik}]$ be the matrix formed from D by replacing each entry by its coset representative in this set. Let $B =$

$$\left[\begin{array}{cccc|cccc|c} c_{11}u_{11} & c_{12}u_{11} & \cdots & c_{1,\lambda h}u_{11} & c_{11}u_{12} & c_{12}u_{12} & \cdots & c_{1,\lambda h}u_{12} & \cdots \\ c_{21}u_{21} & c_{22}u_{21} & \cdots & c_{2,\lambda h}u_{21} & c_{21}u_{22} & c_{22}u_{22} & \cdots & c_{2,\lambda h}u_{22} & \cdots \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \\ c_{r1}u_{r1} & c_{r2}u_{r1} & \cdots & c_{r,\lambda h}u_{r1} & c_{r1}u_{r2} & c_{r2}u_{r2} & \cdots & c_{r,\lambda h}u_{r2} & \cdots \end{array}\right.$$

$$\left.\begin{array}{c|cccc} \cdots & c_{11}u_{1,g/h} & c_{12}u_{1,g/h} & \cdots & c_{1,\lambda h}u_{1,g/h} \\ \cdots & c_{21}u_{2,g/h} & c_{22}u_{2,g/h} & \cdots & c_{2,\lambda h}u_{2,g/h} \\ & \vdots & \vdots & & \vdots \\ \cdots & c_{r1}u_{r,g/h} & c_{r2}u_{r,g/h} & \cdots & c_{r,\lambda h}u_{r,g/h} \end{array}\right].$$

We show that B is a $(g, r; \lambda, G)$ difference matrix. We shall refer to the submatrices into which we have partitioned B as *blocks*.

Consider any two rows of B, indexed by i_1 and i_2 respectively. We consider the λg differences between the entries in row i_1 and the corresponding entries in row i_2. Here and in the rest of this proof, the word *difference* will always mean a difference $x^{-1}y$ between an entry x in row i_1 and the corresponding entry y in row i_2.

We begin by showing that the multisets of differences arising from any two different blocks of B are disjoint. Let the two blocks be indexed by k_1 and k_2 respectively. All differences arising from the first block are of the form $(c_{i_1j_1}u_{i_1k_1})^{-1}(c_{i_2j_1}u_{i_2k_1})$ for some j_1, and all those arising from the second block are of the form $(c_{i_1j_2}u_{i_1k_2})^{-1}(c_{i_2j_2}u_{i_2k_2})$ for some j_2. We have

$$\begin{aligned}
& (c_{i_1j_1}u_{i_1k_1})^{-1}(c_{i_2j_1}u_{i_2k_1}) &=& (c_{i_1j_2}u_{i_1k_2})^{-1}(c_{i_2j_2}u_{i_2k_2}) \\
\Rightarrow\ & u_{i_1k_1}{}^{-1}c_{i_1j_1}{}^{-1}c_{i_2j_1}u_{i_2k_1} &=& u_{i_1k_2}{}^{-1}c_{i_1j_2}{}^{-1}c_{i_2j_2}u_{i_2k_2} \\
\Rightarrow\ & u_{i_1k_1}{}^{-1}c_{i_1j_1}{}^{-1}c_{i_2j_1}u_{i_2k_1}H &=& u_{i_1k_2}{}^{-1}c_{i_1j_2}{}^{-1}c_{i_2j_2}u_{i_2k_2}H \\
\Rightarrow\ & u_{i_1k_1}{}^{-1}u_{i_2k_1}u_{i_2k_1}{}^{-1}c_{i_1j_1}{}^{-1}c_{i_2j_1}u_{i_2k_1}H && \\
& &=& u_{i_1k_2}{}^{-1}u_{i_2k_2}u_{i_2k_2}{}^{-1}c_{i_1j_2}{}^{-1}c_{i_2j_2}u_{i_2k_2}H \\
\Rightarrow\ & u_{i_1k_1}{}^{-1}u_{i_2k_1}H &=& u_{i_1k_2}{}^{-1}u_{i_2k_2}H
\end{aligned}$$

(because $u_{i_2k_1}{}^{-1}c_{i_1j_1}{}^{-1}c_{i_2j_1}u_{i_2k_1}$ and $u_{i_2k_2}{}^{-1}c_{i_1j_2}{}^{-1}c_{i_2j_2}u_{i_2k_2}$ are conjugates of elements of H and are therefore themselves elements of H)

$$\begin{aligned}
\Rightarrow\ & (u_{i_1k_1}H)^{-1}(u_{i_2k_1}H) &=& (u_{i_1k_2}H)^{-1}(u_{i_2k_2}H) \\
\Rightarrow\ & k_1 &=& k_2
\end{aligned}$$

(since each element of G/H appears just once in D as a difference between an entry in row i_1 and the corresponding entry in row i_2).

Hence the multisets of differences arising from the two different blocks of B are indeed disjoint.

We now show that the multiset of differences arising from any particular block of B contains h elements of G, each repeated λ times. This follows immediately from the fact that C is a $(h, r; \lambda, H)$ difference matrix, since for any k indexing a block,

$$\begin{aligned}
& (c_{i_1j_1}u_{i_1k})^{-1}(c_{i_2j_1}u_{i_2k}) &=& (c_{i_1j_2}u_{i_1k})^{-1}(c_{i_2j_2}u_{i_2k}) \\
\Leftrightarrow\ & c_{i_1j_1}{}^{-1}c_{i_2j_1} &=& c_{i_1j_2}{}^{-1}c_{i_2j_2}\,.
\end{aligned}$$

We can deduce that the multiset of λg differences arising from all g/h blocks of B contains each element of G precisely λ times.

Thus B is a $(g, r; \lambda, G)$ difference matrix, as claimed. □

Corollary 2.2 *Let G be a finite group with a normal subgroup H. If there exist r mutually orthogonal orthomorphisms of H and r mutually orthogonal orthomorphisms of G/H then there exist r mutually orthogonal orthomorphisms of G.*

Proof. This is immediate from Theorem 2.1 on taking $\lambda = 1$. □

The pivotal theorem in Bowler's paper [4] states that if Z_n admits at least two mutually orthogonal orthomorphisms then so does $D_{2n} =$

$\langle a, b \mid a^{2n} = b^2 = (ab)^2 = e \rangle$. This is an immediate consequence of Corollary 2.2, since D_{2n} has $\langle a^2 \rangle \cong Z_n$ as a normal subgroup, and $D_{2n}/\langle a^2 \rangle$ is the four-group, which admits two mutually orthogonal orthomorphisms, as can be seen from the difference matrix given in Section 1. Z_n admits two mutually orthogonal orthomorphisms whenever $n \equiv 1, 5 \pmod 6$: for example (using additive notation) $x \mapsto 2x$ and $x \mapsto 3x$.

3 Mutually orthogonal orthomorphisms of dihedral groups

We denote the maximum number of mutually orthogonal orthomorphisms of a group G by $\omega(G)$. Very little seems to be known about orthomorphisms of non-abelian groups. Computer searches have provided some data for small groups. It is known that the dihedral and quaternion groups of order 8 each have 48 orthomorphisms, and in each case no two are orthogonal. The alternating group of order 12 has 3 776 orthomorphisms, no two of which are orthogonal. The dihedral group of order 12 has 6 336 orthomorphisms, and $\omega(D_6) = 2$. All of these results can be found in [6]. In [4], Bowler shows that a dihedral group of order $4n$, $n \equiv 1, 5 \pmod 6$, admits two mutually orthogonal orthomorphisms. We have the following result, obtained by a non-exhaustive computer search, for a dihedral group of order 16.

Proposition 3.1 $\omega(D_8) \geq 3$.

Proof. The following mappings are mutually orthogonal orthomorphisms of $D_8 = \langle a, b \mid a^8 = b^2 = (ab)^2 = e \rangle$. We write $a^i b^j$ as ij.

x	00	10	20	30	40	50	60	70
$\theta_1(x)$	00	01	61	60	41	40	20	21
$\theta_2(x)$	00	30	41	40	31	21	10	71
$\theta_3(x)$	00	31	30	71	51	01	40	20

x	01	11	21	31	41	51	61	71
$\theta_1(x)$	30	71	10	51	31	70	11	50
$\theta_2(x)$	70	60	51	50	61	11	20	01
$\theta_3(x)$	11	41	61	60	21	50	70	10

We include the check:

x	00	10	20	30	40	50	60	70
$x^{-1}\theta_1(x)$	00	71	41	30	01	70	40	31
$x^{-1}\theta_2(x)$	00	20	21	10	71	51	30	01
$\theta_1(x)^{-1}\theta_2(x)$	00	51	20	60	10	61	70	30
$x^{-1}\theta_3(x)$	00	21	10	41	11	31	60	30
$\theta_1(x)^{-1}\theta_3(x)$	00	50	31	11	70	41	20	01
$\theta_2(x)^{-1}\theta_3(x)$	00	01	11	31	60	20	30	51

x	01	11	21	31	41	51	61	71
$x^{-1}\theta_1(x)$	51	20	11	60	10	61	50	21
$x^{-1}\theta_2(x)$	11	31	50	61	60	40	41	70
$\theta_1(x)^{-1}\theta_2(x)$	40	11	41	01	50	21	71	31
$x^{-1}\theta_3(x)$	70	50	40	51	20	01	71	61
$\theta_1(x)^{-1}\theta_3(x)$	61	30	51	71	10	60	21	40
$\theta_2(x)^{-1}\theta_3(x)$	21	61	70	10	40	41	50	71

□

References

[1] D. Bedford, Orthomorphisms and near orthomorphisms of groups and orthogonal latin squares: a survey, *Bull. Inst. Comb. Appl.* **15** (1995), 13–33.

[2] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, 1985.

[3] R.C. Bose, I.M. Chakravati and D.E. Knuth, On methods of constructing sets of mutually orthogonal latin squares using a computer I, *Technometrics* **2** (1960), 507-516.

[4] A. Bowler, Orthomorphisms of dihedral groups, *Discrete Math.*, to appear.

[5] C.J. Colbourn and J.H. Dinitz (ed.), *The CRC Handbook of Combinatorial Designs*, CRC Press, 1996.

[6] A.B. Evans, *Orthomorphism Graphs of Groups*, *Lecture Notes in Mathematics* **1535**, Springer-Verlag, 1992.

[7] M. Hall and L.J. Paige, Complete mappings of finite groups, *Pacific J. Math.* **5** (1955), 541-549.

[8] D.M. Johnson, A.L. Dulmage and N.S. Mendelsohn, Orthomorphisms of groups and orthogonal latin squares I, *Canad. J. Math.* **13** (1961), 356-372.

[9] D. Jungnickel, On difference matrices, resolvable transversal designs and generalized Hadamard matrices, *Math. Z.* **167** (1979), 49–60.

[10] H.B. Mann, The construction of orthogonal latin squares, *Ann. Math. Statist.* **13** (1942), 418-423.

[11] L.J. Paige, Complete mappings of finite groups, *Pacific J. Math.* **1** (1951), 111-116.