ON THE NON-EXISTENCE OF

$(g, g\lambda - 1; \lambda)$-DIFFERENCE MATRICES

Arne Winterhof

Abstract. A $(g, k; \lambda)$-difference matrix over the group $(G, \circ)$ of order g is a k by $g\lambda$ matrix $D = (d_{ij})$ with entries from G such that for each $1 \leq i < j \leq k$ the multiset $\{d_{il} \circ d_{jl}^{-1} | 1 \leq l \leq g\lambda\}$ contains every element of G exactly λ times.
Some known results on the non-existence of generalized Hadamard matrices, i.e. $(g, g\lambda; \lambda)$-difference matrices, are extended to $(g, g\lambda - 1; \lambda)$-difference matrices.

1 Introduction

Let $(G, \circ)$ be a group of order g. A $(g, k; \lambda)$-*difference matrix* is a k by $g\lambda$ matrix $D = (d_{ij})$ with entries from G such that for each $1 \leq i < j \leq k$ the multiset

$$\{d_{il} \circ d_{jl}^{-1} | 1 \leq l \leq g\lambda\}$$

contains every element of G exactly λ times.
See de Launey [8] and Colbourn/de Launey [2] for surveys on difference matrices and [10] for a new construction method.
Since a (g, l, λ)-difference matrix with $l < k$ can be constructed from a (g, k, λ)-difference matrix by erasing rows, most previous research on difference matrices has concentrated on constructions with large k. So it is natural to ask how large k can be.
Jungnickel [6] proved that a $(g, k; \lambda)$-difference matrix satisfies $k \leq g\lambda$.
For $k = g\lambda$ several non-existence results are known. (A $(g, g\lambda; \lambda)$-difference matrix is called a generalized Hadamard matrix.) De Launey [7] established the following non-existence result for $(g, g\lambda; \lambda)$-difference matrices over abelian groups.

RESULT 1 *Suppose there exists a $(g, \lambda g; \lambda)$-difference matrix with λg odd. Let $p > 2$ be a prime dividing g and suppose m is an integer dividing the p-free, and squarefree part of λ. Then the order of m modulo p is odd.*

Brock [1] proved a kindred result.

RESULT 2 *If a $(g, \lambda g; \lambda)$-difference matrix over G with λg odd exists, then*

$$c^2 = (\lambda g)a^2 + (-1)^{(s-1)/2} s b^2$$

has a non-trivial solution $a, b, c \in \mathbf{Q}$ for every s the order of a non-trivial homomorphic image of G.

ARS COMBINATORIA 64(2002), pp. 265-269

For $k < g\lambda$ the only non-existence result for $(g, k; \lambda)$-difference matrices known by the author was proved by Drake [3].

RESULT 3 *A $(g, 3; \lambda)$-difference matrix does not exist if $g \equiv 2 \bmod 4$ and λ is odd.*

In this note we extend de Launey's result on $(g, g\lambda; \lambda)$-difference matrices to $(g, g\lambda - 1; \lambda)$-difference matrices. Moreover, using the authors method introduced in [9] we prove a result with the flavour of Brock's result for groups of prime order $p \equiv 3 \bmod 4$. Both extensions are based on Lemma 1 below. It seems that this lemma can not be extended to $(g, k; \lambda)$-difference matrices with $k \leq g\lambda - 2$.
Finally we compare de Launey's result with Brock's result for groups of prime order.

2 Extension of de Launey's Result

THEOREM 1 *Suppose there exists a $(g, \lambda g - 1; \lambda)$-difference matrix over the abelian group G with λg odd. Let $p > 2$ be a prime dividing g and suppose m is an integer dividing the p-free and squarefree part of λ. Then the order of m modulo p is odd.*

We prove the theorem after some preliminary lemmas.
Let denote by C_p the cyclic group of order p.

LEMMA 1 *If there exists a $(p, \mu p - 1; \mu)$-difference matrix D over C_p then there exists a μp by μp matrix $D' = (d'_{ij})$ over $\mathbf{Z}(C_p)/(\sum_{\omega \in C_p} \omega)$ satisfying*

$$DetD' DetD'^* = (\mu p)^{\mu p},$$

where $D'^* = (\overline{d'_{ij}})^T$ and $\overline{d'_{ij}} = \sum_{\omega \in C_p} a_\omega \omega^{-1}$ if $d'_{ij} = \sum_{\omega \in C_p} a_\omega \omega$, $a_\omega \in \mathbf{Z}$.

PROOF. Put $n = \mu p$ and suppose there exists a $(p, n - 1; \mu)$-difference matrix D.
We permute the columns of D such that the row $A_n = (n\ 0 \ldots 0)$ and the rows of the permuted matrix are linearly independent over

$$R := \mathbf{Z}(C_p)/(\sum_{\omega \in C_p} \omega)$$

and multiply the rows with elements of C_p such that the first column is $(1 \ldots 1)^T$.
Let denote by $B_1, \ldots, B_{n-1} \in R^n$ the rows of the resulting matrix which are mutually orthogonal, i.e. $B_i B_j^* = \sum_{l=1}^{n} b_{il} \bar{b}_{jl} = 0$ if $i \neq j$.
Obviously,

$$B_n := A_n - \sum_{i=1}^{n-1} B_i$$

is orthogonal to B_i for $i = 1, \ldots, n-1$, and

$$B_n B_n^* = n.$$

For $D' = \begin{pmatrix} B_1 \\ \vdots \\ B_n \end{pmatrix}$ we have

$$D' D'^* = n I_n,$$

where I_n denotes the n by n identity matrix over R, and thus the assertion. □

LEMMA 2 *Let $p > 2$ and q be primes such that for some s $q^s \equiv -1 \bmod p$. If $d \in \mathbf{Z}(C_p)/(\sum_{\omega \in C_p} \omega)$ satisfies $d\overline{d} \equiv 0 \bmod q$ then $d \equiv 0 \bmod q$.*

PROOF. Let ω be a generator of C_p and $d = d_1\omega + d_2\omega^2 + \ldots + d_{p-1}\omega^{p-1}$ with $d_1, \ldots, d_{p-1} \in \mathbf{Z}$, then

$$d^{q^s} \equiv d_1^{q^s} \omega^{q^s} + d_2^{q^s} \omega^{2q^s} + \ldots + d_{p-1}^{q^s} \omega^{(p-1)q^s}$$

$$\equiv d_1\omega^{-1} + d_2\omega^{-2} + \ldots + d_{p-1}\omega^{1-p} \equiv \overline{d} \bmod q.$$

Hence, $d^{q^s+1} \equiv 0 \bmod q$ and thus $d \equiv d^{q^{2s}} \equiv 0 \bmod q$. □

PROOF OF THEOREM 1. Suppose there exists a $(g, \lambda g - 1; \lambda)$-difference matrix over G. Since G is abelian there exists an epimorphism $\phi : G \to C_p$ and thus a $(p, \lambda g - 1; \lambda g/p)$-difference matrix over C_p. By Lemma 1 there exists a $d \in \mathbf{Z}(C_p)/(\sum_{\omega \in C_p} \omega)$ satisfying $d\overline{d} = (\lambda g)^{\lambda g}$. Let $m = p_1 \cdots p_t$ be the prime decomposition of m and e_i the order of p_i modulo p. Then $m^{e_1 \cdots e_t} \equiv 1 \bmod p$.
If e_i is even, for some i, then $p_i^{e_i/2} \equiv -1 \bmod p$. By Lemma 2 there exists d_1 with $d = p_i d_1$ and $d_1\overline{d_1} = \frac{(\lambda g)^{\lambda g}}{p_i^2}$. Repeated application of Lemma 2 yields $d_r\overline{d}_r = \frac{(\lambda g)^{\lambda g}}{p_i^{2r}}$, where $p_i \not| \frac{(\lambda g)^{\lambda g}}{p_i^{2r}}$ for some positive integer r. Since λg is odd it follows $p_i \not| m$ which is a contradiction. □

3 Extension of Brock's Result

THEOREM 2 *Let $p \equiv 3 \bmod 4$ be a prime, λ be odd and M be the p-free and squarefree part of λ. If there exists a $(p, \lambda p - 1, \lambda)$-difference matrix then $c^2 = Ma^2 - pb^2$ has a non-trivial solution $a, b, c \in \mathbf{Z}$.*

PROOF. If there exists a $(p, p\lambda - 1, \lambda)$-difference matrix, then there exists a $d \in \mathbf{Q}(C_p)/(\sum_{\omega \in C_p} \omega)$ satisfying $d\bar{d} = (\lambda p)^{\lambda p}$ by Lemma 1.
For primes p the fields $\mathbf{Q}(C_p)/(\sum_{\omega \in C_p} \omega)$ and the pth cyclotomic field $\mathbf{Q}(\zeta_p)$ are isomorphic and we may consider d as an element of $\mathbf{Q}(\zeta_p)$, where $\zeta_p = e^{2\pi\sqrt{-1}/p}$. Since $N_{\mathbf{Q}(\zeta_p)}(d) = N_{\mathbf{Q}(\zeta_p)}(\bar{d})$ we have

$$N_{\mathbf{Q}(\zeta_p)}(d)^2 = N_{\mathbf{Q}(\zeta_p)}((\lambda p)^{\lambda p}) = (\lambda p)^{\lambda p(p-1)},$$

where $N_{\mathbf{Q}(\zeta_p)}(.)$ denotes the absolute norm of $\mathbf{Q}(\zeta_p)$ into $\mathbf{Q}$. Hence, there exists an $y \in \mathbf{Q}(\zeta_p)$ such that $N_{\mathbf{Q}(\zeta_p)}(y) = (\lambda p)^{\lambda p(p-1)/2}$.
Since $p \equiv 3 \bmod 4$ we have

$$\mathbf{Q} \leq \mathbf{Q}(\sqrt{-p}) \leq \mathbf{Q}(\zeta_p)$$

(see e.g. [4,Chapter 27d]). By the transitivity of the norm there exists an $z \in \mathbf{Q}(\sqrt{-p})$ such that

$$N_{\mathbf{Q}(\sqrt{-p})}(z) = (\lambda p)^{\lambda p(p-1)/2} = p^{l\lambda p(p-1)/2} b^2 M = N_{\mathbf{Q}(\sqrt{-p})}(w) M,\ w \in \mathbf{Q}(\sqrt{-p})$$

since $\lambda p(p-1)/2$ is odd, $N_{\mathbf{Q}(\sqrt{-p})}(b) = b^2$ for $b \in \mathbf{Q}$ and $N_{\mathbf{Q}(\sqrt{-p})}(\sqrt{-p}) = p$. For $x = zw^{-1}$ we have $N_{\mathbf{Q}(\sqrt{-p})}(x) = M$.
If $x = u + v\sqrt{-p}, u, v \in \mathbf{Q}$, then (u, v) is a solution of $u^2 = M - pv^2$. Let n be the least common nominator of u and v, then $a = n$, $b = vn$ and $c = un$ is an integer solution of $c^2 = Ma^2 - pb^2$. □

4 Comparison of the Results

1. By Legendre's theorem (see e.g. [5, Proposition 17.3.1]) $c^2 = Ma^2 + (-1)^{(p-1)/2} pb^2$, M a p-free and squarefree integer, has a non-trivial solution if and only if there exist $x_1, x_2 \in \mathbf{Z}$ satisfying

$$x_1^2 \equiv (-1)^{(p-1)/2} p \bmod M$$

and

$$x_2^2 \equiv M \bmod p.$$

It can be seen easily that the second congruence can be omitted.
Let $x_1^2 \equiv (-1)^{(p-1)/2} p \bmod M$ and $M = q_1 \cdots q_r$ be the prime decomposition of M. Then $x_1^2 \equiv (-1)^{(p-1)/2} p \bmod q_i$ and thus $\left(\frac{(-1)^{(p-1)/2} p}{q_i}\right) = 1$ for $i = 1, \ldots, r$, where $\left(\frac{\cdot}{\cdot}\right)$ denotes Legendre's symbol. We have $\left(\frac{M}{p}\right) = \left(\frac{q_1}{p}\right) \cdots \left(\frac{q_r}{p}\right) = \left(\frac{(-1)^{(p-1)/2} p}{q_1}\right) \cdots \left(\frac{(-1)^{(p-1)/2} p}{q_r}\right) = 1$ and M is a quadratic residue modulo p.

2. If the order of any prime divisor q_i of M is odd, then

$$\left(\frac{(-1)^{(p-1)/2}p}{q_i}\right) = \left(\frac{q_i}{p}\right) = \left(\frac{q_i}{p}\right)^{\mathrm{ord}_p q_i} = \left(\frac{1}{p}\right) = 1.$$

Hence, $(-1)^{(p-1)/2}p$ is a quadratic residue modulo any prime divisor of M and thus a quadratic residue modulo M. Thus, for groups of prime order de Launey's result covers Brock's result. Moreover, Theorem 1 covers Theorem 2.

3. If $p \equiv 3 \bmod 4$ and $-p$ is a quadratic residue modulo M then M is a quadratic residue modulo p by 1. Hence, $M^{(p-1)/2} \equiv 1 \bmod p$ and the order of M (and thus the order of any divisor m of M) modulo p is odd. So we have seen that for groups of prime order $p \equiv 3$ mod 4 de Launey's and Brock's result are equivalent. (For groups of prime order $p \equiv 3$ mod 4 Theorem 1 and Theorem 2 are also equivalent.)

References

[1] B. W. Brock, Hermitian congruence and the existence and completion of generalized Hadamard matrices, *J. Combin. Theory A* 49 (1988), 233-261.

[2] C. J. Colbourn and W. de Launey, Difference matrices, in C. J. Colbourn (ed.) et al., *The CRC handbook of combinatorial designs.* CRC Press, Boca Raton, 1996, 287-297.

[3] D. A. Drake, Partial λ-geometries and generalized Hadamard matrices over groups, *Canad. J. Math.* 31 (1979), 617-627.

[4] H. Hasse, "Zahlentheorie", Akademie-Verlag, Berlin, 1949.

[5] K. Ireland and M. Rosen, "A classical introduction to modern number theory", Springer, New York, 1982.

[6] D. Jungnickel, On difference matrices, transversal designs, resolvable transversal designs, and large sets of mutually orthogonal F-squares, *Math. Z.* 167 (1979), 49-60.

[7] W. de Launey, On the non-existence of generalised weighing matrices, *Ars Combin.* 17A (1984), 117-132.

[8] W. de Launey, A survey of generalised Hadamard matrices and difference matrices $D(k, \lambda, G)$ with large k, *Utilitas Mathematica* 30 (1986), 5-29.

[9] A. Winterhof, On the non-existence of generalized Hadamard matrices, *J. Statistical Planning Inference* 84 (2000), 337-342.

[10] A. Winterhof, Some estimates for character sums and applications, *Designs, Codes and Crypt.*, to appear.

Institute of Discrete Mathematics
Austrian Academy of Sciences
Sonnenfelsgasse 19/2
A-1010 Vienna, Austria
E-Mail: arne.winterhof@oeaw.ac.at