Weighing Matrices from Generalized Hadamard Matrices by 2-Adjugation

R. Craigen
Dept. of Mathematics and Computer Science
University of Lethbridge
Lethbridge, Alberta
Canada T1K 3M4
craigen@alpha.uleth.ca

October 31, 1991

Abstract

In 1988 Sarvate and Seberry introduced a new method of construction for the family of weighing matrices $W(n^2(n-1), n^2)$, where n is a prime power. We generalize this result, replacing the condition on n with the weaker assumption that a generalized Hadamard matrix $GH(n; G)$ exists with $|G| = n$, and give conditions under which an analogous construction works for $|G| < n$. We generalize a related construction for a $W(13, 9)$, also given by Sarvate and Seberry, producing a whole new class. We build further on these ideas to construct several other classes of weighing matrices.

1 Introduction and preliminaries

Recall that the *2-adjugate*, $D_2(M)$, of an $n \times n$ matrix M with entries in a commutative ring $\mathbf{R}$ (that is, $M \in M_n(\mathbf{R})$) is defined to be the $\frac{n(n-1)}{2} \times \frac{n(n-1)}{2}$ matrix whose rows and columns are indexed by unordered pairs from the list $1, \ldots, n$ (with some fixed ordering among these pairs) and whose $(i, i'), (j, j')$ entry is the 2×2 minor corresponding to rows i and i' and columns j and j'.

The Cauchy-Binet theorem [4, p. 25] applies to the analogous *k-adjugate* D_k and states that for $1 \leq k \leq n$, D_k is multiplicative—that is, for any $M, M' \epsilon M_n(\mathbf{R})$, $D_k(M) D_k(M') = D_k(M M')$. We shall only need the case $k = 2$.

Henceforth, let G be a fixed abelian group with $|G| = g$ and let us take $\mathbf{R}$ to be the group ring $Z[G]$. We define a map $* : \mathbf{R} \to \mathbf{R}$ by linearly extending the inverse map $* : x \to x^* := x^{-1}$, $x \epsilon G$. Then $*$ is an involution on the ring $\mathbf{R}$, and since G is abelian, $*$ must therefore be an automorphism of the ring. We can also "extend" $*$ to an involution on the matrix ring $M_n(G)$ by $(m_{ij})^* := (m_{ji}{}^*)$. Since $*$ is an automorphism of $\mathbf{R}$, we have

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix}^* = \begin{vmatrix} a^* & c^* \\ b^* & d^* \end{vmatrix}.$$

Combining this with the Cauchy-Binet theorem, we arrive at the following lemma.

Lemma 1 *For all* $M \epsilon M_n(\mathbf{R})$, $D_2(M) D_2(M)^* = D_2(MM^*)$.

More generally, $*$ "commutes" with determinants of any degree, and so the k-degree analogue of this lemma holds.

Now $G = \{x_1, \ldots, x_g\}$ has a *regular representation*, $\pi : G \to M_g(Z)$, which is given by

$$\pi(x_k)_{ij} = \begin{cases} 0 & \text{if } x_i x_j{}^{-1} \neq x_k \\ 1 & \text{if } x_i x_j{}^{-1} = x_k \end{cases}.$$

Thus π is a group homomorphism which maps elements of G to permutation matrices which are pairwise *disjoint*—that is, their entry-wise product equals 0. There is a unique homomorphism, which we also denote by π, extending π linearly to the group ring $\mathbf{R}$. This satisfies $\pi(x^*) = \pi(x)^t$, since this holds on the basis of group elements. Moreover, if we write G for the element of the ring obtained by summing the elements of the group G in $\mathbf{R}$, then we have $\pi(G) = J_g$, the $g \times g$ matrix with all entries equal to 1. As well, π induces a ring homomorphism $M_n(\mathbf{R}) \to M_{gn}(Z)$ also denoted π, by operating on matrices entry-wise. This also satisfies $\pi(M^*) = \pi(M)^t$.

A *generalized Hadamard matrix* $M = GH(n, G)$ is a matrix in $M_n(\mathbf{R})$, all of whose entries are elements of G, satisfying the condition

$$MM^* = nI + \frac{n}{g} G(J - I). \qquad (1)$$

We shall have some uses for the following well-known result.

Lemma 2 (Drake, [2]) *For any prime p and integers $0 \leq s \leq t$, there exists a $GH(p^t, EA(p^s))$.*

Here $EA(p^r)$ denotes the *elementary abelian group* of order p^r, $Z_p \times \cdots \times Z_p$, which is defined for all primes p.

A *weighing matrix* $W = W(n, w)$ of *weight* w is an $n \times n$ $(0, \pm 1)$-matrix satisfying

$$WW^t = wI. \tag{2}$$

Sarvate and Seberry [5] demonstrated that there is a $W(g^2(g-1), g^2)$ for prime powers g by a construction utilizing the 2-adjugate of the generalized Hadamard matrix $GH(g, EA(g))$ given by lemma 2. They accidentally gave a proof which was valid only for prime g, but in fact they had indeed verified the more general result, and this was merely an oversight. We repeat their construction, giving a shorter proof which avoids such problems, not relying at all on the structure of Galois fields—and is in fact more general, provided that one can produce a $GH(g, G)$, with g not a prime power. Whether or not this is possible is presently unresolved.

2 Construction of the special matrix D

Let $M = GH(n; G)$. We calculate that

$$D_2(M)D_2(M)^* = D_2(MM^*) = (n^2 - \frac{n^2}{g}G)I_{\frac{n(n-1)}{2}}, \tag{3}$$

since the principal minor of MM^* have the form $\begin{vmatrix} n & \frac{n}{g}G \\ \frac{n}{g}G & n \end{vmatrix}$, and each non-principal minors has one of the forms $\begin{vmatrix} \frac{n}{g}G & \frac{n}{g}G \\ \frac{n}{g}G & \frac{n}{g}G \end{vmatrix}$, $\begin{vmatrix} \frac{n}{g}G & \frac{n}{g}G \\ n & \frac{n}{g}G \end{vmatrix}$ or some permutation of the latter. Now $G^2 = \sum_{x \epsilon G} \sum_{y \epsilon G} xy = gG$, so all the non-principal minors are 0.

Moreover, since each entry, u, of $D_2(M)$ is a 2×2 minor, it is of the form $x - y$, $x, y \epsilon G$. Thus $uG = 0$, and it follows that $D_2(M)(GN)^* = 0$ for any matrix $N \epsilon M_{\frac{n(n-1)}{2}}(\mathbf{R})$. We write $D := \pi(D_2(M))$. Sarvate and Seberry constructed this D in the case $G = EA(n)$, where $n = g$ is a prime power. Then they constructed the companion matrix $E := \pi(GI_{\frac{g(g-1)}{2}}) =$

$I \otimes J_g$ and pointed out that matrix

$$\begin{pmatrix} E & D \\ D & E \end{pmatrix} \tag{4}$$

is a $W(g^2(g-1), g^2)$. For, by the foregoing observations, $ED^t = DE^t = 0$, and using (3), we see that $DD^t + EE^t = I_{\frac{g(g-1)}{2}} \otimes (g^2 I_g - gJ_g) + I_{\frac{g(g-1)}{2}} \otimes gJ_g = g^2 I_{\frac{g^2(g-1)}{2}}$. Moreover, this holds whenever a $GH(g,G)$ exists.

Theorem 3 *Given a $GH(g,G)$, there is a $W(g^2(g-1), g^2)$.*

Notice that, while the statement of this result is apparently more general than that of Sarvate and Seberry, it remains to be determined whether or not this is indeed a strict generalization. They also noted another use for the matrix D in the case $n = g = 3$, as follows. The matrix

$$\left(\begin{array}{cccc|ccccccccc}
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & - & - & - & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & - & - & - \\
0 & 1 & 1 & 1 & - & - & - & 1 & 1 & 1 & 0 & 0 & 0 \\
\hline
1 & 0 & 1 & - & & & & & & & & & \\
1 & 0 & 1 & - & & & & & & & & & \\
1 & 0 & 1 & - & & & & & & & & & \\
1 & - & 0 & 1 & & & & & & & & & \\
1 & - & 0 & 1 & & & & & D & & & & \\
1 & - & 0 & 1 & & & & & & & & & \\
1 & 1 & - & 0 & & & & & & & & & \\
1 & 1 & - & 0 & & & & & & & & & \\
1 & 1 & - & 0 & & & & & & & & &
\end{array}\right)$$

is a $W(13, 9)$. Here we produce a simple generalization of this construction.

Theorem 4 *Given a $GH(g,G)$ and a weighing matrix $W = W(\frac{g(g-1)}{2} + 1, g)$, there is a $W(\frac{g(g^2-1)}{2} + 1, g^2)$.*

<u>Proof:</u> Let W_i represent the ith row vector of W, indexing from 0 to

$\frac{g(g-1)}{2}$, and let e represent the $1 \times g$ vector $(1, \ldots, 1)$. Then

$$\left(\begin{array}{c|ccc} W_0{}^t W_0 & W_1{}^t e & \cdots & W_{\frac{g(g-1)}{2}}{}^t e \\ \hline e^t W_1 & & & \\ \vdots & & D & \\ e^t W_{\frac{g(g-1)}{2}} & & & \end{array}\right) \qquad (5)$$

is the required matrix. □

Example 1 By lemma 2 there is a $GH(3, Z_3)$. Using this and the weighing matrix

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & - \\ 1 & - & 0 & 1 \\ 1 & 1 & - & 0 \end{pmatrix},$$

we obtain the example given by Sarvate and Seberry.

Example 2 By lemma 2, there is a $GH(4, Z_2 \times Z_2)$. The circulant with first row (-110100) is a $W(7,4)$. Thus we obtain a $W(31,16)$.

3 The next step: $g \neq n$

We see that $\{D, E\}$, as given in the last section, is an example of an *orthogonal set* (see [1] for a complete introduction to orthogonal sets, their construction and application). Now let us drop the assumption that $g = n$, and postulate the existence of a weighing matrix $W = W(\frac{n(n-1)}{2}, (\frac{n}{g})^2)$. If we write $E := \pi(GW)$, and $D = \pi(D_2(M))$ as before, we have another orthogonal set, and (4) is a $W(gn(n-1), n^2)$.

Theorem 5 *Given a $GH(n, G)$ and a $W(\frac{n(n-1)}{2}, (\frac{n}{g})^2)$, there is a $W(gn(n-1), n^2)$.*

Example 3 With $Z_3 = <\gamma : \gamma^3 = 1>$, we construct the circulant matrix A with first row $(1\gamma\gamma^2\gamma^2\gamma)$. Then

$$\begin{array}{c|ccc} 1 & 1 & \cdots & 1 \\ \hline 1 & & & \\ \vdots & & A & \\ 1 & & & \end{array}$$

is a $GH(6, Z_3)$. We take $n = 6$ and $g = 3$. It is well-known [3] that a $W(15, 4)$ exists. Therefore we obtain a $W(90, 36)$.

Example 4 As before, we have a $GH(9, Z_3)$. Since $W(36, 9)$ is known [3], we obtain a $W(216, 81)$.

Here is a variation on theorem 4 which works in this more general setting.

Theorem 6 *Given a* $GH(n, G)$ *and a* $W(\frac{n(n-1)}{2}, \frac{n^2}{g})$, *there is a* $W(\frac{n(n-1)(g+1)}{2}, n^2)$.

Proof: As in theorem 4, except that we take $W_0 = (0, \ldots, 0)$. □

Example 5 We may take $n = 8$, $g = 4$. Since a $W(28, 16)$ is known [3], we obtain a $W(140, 64)$.

4 Further use of orthogonal sets

The construction of D and E as described in section 3 produces orthogonal sets with *coweights* (see [1]) equal to 1. We consider here how to obtain other coweights.

Let $W = W(m, w)$ and $V = W(\frac{mn(n-1)}{2}, w')$. Then let $D := W \otimes \pi(D_2(M))$ and $E := V \otimes J_g$. Now D and E are $(0, \pm 1)$-matrices satisfying $DE^t = ED^t = 0$ and $w'g^2 DD^t + wn^2 EE^t = ww'(ng)^2 I_{\frac{mng(n-1)}{2}}$. Using the theory of orthogonal sets, we have the following theorem.

Theorem 7 *Given a* $GH(n, G)$, *weighing matrices* $W(m, w)$, $W(\frac{mn(n-1)}{2}, w')$ *and disjoint weighing matrices* $W(k, twn^2)$, $W(k, tw'g^2)$, *there is a* $W(\frac{mngk(n-1)}{2}, tww'(ng)^2)$.

Here m, k, w, w' are any suitable positive integers and t may be any suitable rational number (here "suitable" only means that the postulated weighing matrices exist). Theorem 5 is the special case of this result corresponding to $k = 2$, $m = w = 1$, $w' = (\frac{n}{g})^2$ and $t = n^{-2}$.

Now suppose there is an $SBIBD(g, r, \lambda)$. Then the (± 1) incidence matrix, H, of this design satisfies

$$HH^t = gI_g + (4(\lambda - r) + g)(J_g - I_g), \tag{6}$$

$$HJ = (2r - g)J. \tag{7}$$

Then $F = \frac{1}{2}D(I \otimes H)$ is a $(0, \pm 1)$-matrix satisfying

$$FF^t = wn^2(r-\lambda) I_{\frac{mng(n-1)}{2}} - \frac{wn^2(r-\lambda)}{g} I_{\frac{mn(n-1)}{2}} \otimes J_g. \qquad (8)$$

Moreover, $F(N \otimes J_g) = 0$ for any matrix N of order $\frac{mn(n-1)}{2}$. Therefore we have the following result.

Theorem 8 *Given a $GH(n, G)$, an $SBIBD(g, r, \lambda)$, a $W(m, w)$ and a $W(\frac{mn(n-1)}{2}, w(\frac{n}{g})^2(r-\lambda))$, there is a $W(mng(n-1), wn^2(r-\lambda))$.*

Proof: Let V be the second weighing matrix and set $E = V \otimes J_g$. Then

$$\begin{pmatrix} E & F \\ F & E \end{pmatrix}$$

is the desired weighing matrix. □

This result may be generalized further by the use of orthogonal sets as in theorem 7. We may also apply the other method to the matrix F and obtain the following.

Theorem 9 *Given a $GH(n, G)$, a $W(m, w)$, an $SBIBD(g, r, \lambda)$ and a $W(\frac{mn(n-1)}{2}, \frac{wn^2(r-\lambda)}{g})$, there is a $W(\frac{mn(n-1)(g+1)}{2}, wn^2(r-\lambda))$.*

Proof: Analogous to theorem 6. □

Again, another result analogous to theorem 4 may be obtained using F instead of D, but it requires a couple of additional preconditions, and so we refrain from stating it here.

References

[1] R. Craigen, *Orthogonal sets and orthogonal designs*, Tech. Rep. CORR #90–19, University of Waterloo, 1990.

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

[3] A. Geramita and J. Seberry, *Quadratic Forms, Orthogonal Designs, and Hadamard Matrices*, vol. 45 of Lecture Notes in Pure and Applied Mathematics, Marcel Dekker Inc., New York and Basel, 1979.

[4] M. Newman, *Integral Matrices*, Academic Press, New York and London, 1972.

[5] D. G. Sarvate and J. Seberry, *On weighing matrices with square weights*, in Proceedings of the Symposium on Optimization, Design of Experiments and Graph Theory, Indian Institute of Technology, Bombay, 1988, pp. 71–76.