0.1. Generalized weighing matrices

In the previous section, we defined a weighing matrix as a square matrix over $\{-1, 0, 1\}$. We then extended this definition to include those matrices over 0 together with the complex p-th roots of unity. More generally, we can have weighing matrices over any finite group.

Before we can do this, however, we need to extend the conjugate transpose to group matrices. To accomplish this, let $A = (a_{ij})$ be some matrix over a finite group G. Take $\overline{A} = (a_{ij}^{-1})$ to be the matrix obtained by taking the group inverse of the elements. Finally, define $A^* = \overline{A}^t$. We then have the following.

0.1 Definition. Let G be some finite group not containing the symbol 0, and let W be a $(0, G)$-matrix of order v. If $WW^* = kI_n$ modulo the ideal $\mathbf{Z}G$, then we say that W is a generalized weighing matrix of order v and weight k. We write $\mathrm{GW}(v, k; G)$ to denote this property.group-ring

0.2 Example. A real $\mathrm{W}(v, k)$ is a $\mathrm{GW}(v, k; C_2)$, and a $\mathrm{BW}(v, k; p)$ is a $\mathrm{GW}(v, k; C_p)$, were C_p denotes the cyclic group of prime order p.

0.3 Example. In the case that one has $\mathrm{BW}(v, k; C_n)$, where n is composite, one does not in general have a generalized weighing matrix. Consider the $\mathrm{BW}(6, 6; 4)$ given by

$$\begin{pmatrix} i & + & + & + & + & + \\ + & i & - & + & - & + \\ + & - & i & - & + & + \\ + & + & - & i & + & - \\ + & - & + & + & i & - \\ + & + & + & - & - & i \end{pmatrix}. \tag{0.3.a}$$

Clearly, this is a Hadamard matrix; however, $\pm i$ each appear only once in the conjugate inner product between distinct rows, hence it is not a generalized weighing matrix.

0.4 Example. The following is a $\mathrm{GW}(15, 7; C_3)$, where the nonzero elements are the logarithms of a generator of C_3.

$$\begin{pmatrix}
0&3&3&3&3&3&3&3&0&0&0&0&0&0&0\\
0&3&2&0&1&0&0&0&0&0&2&0&2&2&3\\
0&0&3&2&0&1&0&0&3&0&0&2&0&2&2\\
0&0&0&3&2&0&1&0&2&3&0&0&2&0&2\\
0&0&0&0&3&2&0&1&2&2&3&0&0&2&0\\
0&1&0&0&0&3&2&0&0&2&2&3&0&0&2\\
0&0&1&0&0&0&3&2&2&0&2&2&3&0&0\\
0&2&0&1&0&0&0&3&0&2&0&2&2&3&0\\
3&3&1&0&2&0&0&0&3&2&0&1&0&0&0\\
3&0&3&1&0&2&0&0&0&3&2&0&1&0&0\\
3&0&0&3&1&0&2&0&0&0&3&2&0&1&0\\
3&0&0&0&3&1&0&2&0&0&0&3&2&0&1\\
3&2&0&0&0&3&1&0&1&0&0&0&3&2&0\\
3&0&2&0&0&0&3&1&0&1&0&0&0&3&2\\
3&1&0&2&0&0&0&3&2&0&1&0&0&0&3
\end{pmatrix} \tag{0.4.a}$$

0.2. Generalized Bhaskar Rao Designs

Our goal in introducing weighing matrices over arbitrary finite groups is to synthesis the ideas of weighing matrices and balanced incomplete block designs. We combine these concepts thus.

0.5 Definition. Let G be some finite group, and let A be a $v \times b$ $(0, G)$-matrix such that

$$\text{(0.5.a)} \quad AA^* = rI_v + \frac{\lambda}{|G|}\left(\sum_{g \in G} g\right)(J_v - I_v),$$

for some positive integers r and λ, and such that there are k non-zero entries in every column. We then say that A is a *generalized Bhaskar Rao design* (henceforth GBRD), and we write GBRD$(v, k, \lambda; G)$ to denote this property. If we need to stress the remaining parameters, then we write GBRD$(v, b, r, k, \lambda; G)$.

Often it is helpful to give a combinatorial definition of GBRDs that is equivalent to the one just given. Again let $A = (a_{ij})$ be a $v \times b$ $(0, G)$-matrix that has k nonzero entries in every column. If the multisets $\{a_{i\ell}a_{j\ell}^{-1} : a_{i\ell} \neq 0 \neq a_{j\ell}$ and $0 \leq \ell < b\}$, for $i, j \in \{0, \ldots, v-1\}$, $i \neq j$, have $\lambda/|G|$ copies of every group element in G, then we say that A is a GBRD$(v, k, \lambda; G)$.

A few things are rather immediate. If $\breve{A}$ denotes the matrix obtained from A by changing each non-zero entry to 1, then condition (**??**) implies that $\breve{A}$ is a also a BIBD. Conversely, a BIBD is a GBRD over the trivial group $\{1\}$.

Evidently, Fisher's inequality applies, hence $b \geq v$. We single out the extremal case of Fisher's inequality again.

0.6 Definition. A *balanced generalized weighing matrix* is a GBRD$(v, b, r, k, \lambda; G)$ in which $v = b$ (equiv. $k = r$). We use the denotation BGW$(v, k, \lambda; G)$. A BGW$(v, k, \lambda; G)$ in which $v = k = \lambda$ is called a *generalized Hadamard matrix*, and we denote this as GH(G, λ) where $\lambda = v/|G|$. If $G = \mathrm{EA}(q)$, the elementary abelian group of order q, then we write GH(q, λ) instead.ea-group

0.7 Example. The generalized weighing matrix **??** is a BGW$(15, 7, 3; C_3)$.

0.8 Example. Let $G = \langle \alpha, \beta : \alpha^2 = \beta^2 = 1, \alpha\beta = \beta\alpha \rangle$. Then

$$\text{(0.8.a)} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha & \beta & \alpha\beta \\ 1 & \beta & \alpha\beta & \alpha \\ 1 & \alpha\beta & \alpha & \beta \end{pmatrix}$$

is a GH$(4, 1)$.

Moreover, the necessary conditions of Proposition **??** also hold for the parameters of GBRDs. However, since we are now dealing with group matrices that are balanced with respect to the group, the next result is clear.

0.9 Proposition. Let $A = [a_{ij}]$ be a GBRD$(v, k, \lambda; G)$, and let $\phi : G \to H$ be some group epimorphism. Then $[\phi(a_{ij})]$ is a GBRD(v, k, λ) over H with the same parameters.

Again, the extremal case of Fisher's inequality presents interesting problems; futher, the case in which $v = k$ and $b = r$ is interesting as well.

A balanced weighing matrix is a BGW$(v, k, \lambda; \{-1, 1\})$.

0.10 Example. The generalized weighing matrix of Example **??** can be seen to be a BGW$(15, 7, 3, ; C_3)$.

Our work from the previous section, namely, Lemma **??** yields the following.

0.11 Proposition. A Butson weighing matrix W is a BGW if and only if $\check{W}$ is a BIBD.

The remainder of this chapter will focus on BGW matrices and will follow Chapter 10 of **?** closely. We first present a few simple constructions, where we use GF(q) for the Galois field of order q. GF$(q)^+$ and GF$(q)^*$ denote, respectively, the additive and multiplicative groups of GF(q). Moreover, recall that GF$(q)^+ \simeq$ EA(q).

0.12 Proposition. Let GF$(q) = \{a_0, \ldots, a_{q-1}\}$, and define $H = [h_{ij}]$ of order q by $h_{ij} = a_i a_j$. Then H is a GH$(q, 1)$.

Proof. Let H be so defined, and let $i, j \in \{0, \ldots, q-1\}$, $i \neq j$. Observe $\sum_k (a_i a_k - a_j a_k) = (a_i - a_j) \sum_k a_k$, hence each group element appears precisely once in $\{h_{ik} h_{jk}^{-1} : 0 \leq k < q\}$. ■

0.13 Proposition. Let GF$(q) = \{a_0, \ldots, a_{q-1}\}$, and define $W = [w_{ij}]$ of order $q + 1$ by

$$w_{ij} = \begin{cases} 0 & \text{if } i = j = 0; \\ 1 & \text{if } i = 0 \text{ or } j = 0, \text{ but } i \neq j; \text{ and} \\ a_{i-1} - a_{j-1} & \text{otherwise.} \end{cases}$$

Then W is a BGW$(q + 1, q, q - 1; \text{GF}(q)^*)$.

Proof. Let $i, j \in \{1, \ldots, q\}$, $i \neq j$. Then, for $k \neq j$,

$$w_{ik} w_{jk}^{-1} = \frac{a_{i-1} - a_{k-1}}{a_{j-1} - a_{k-1}}^{-1} = \frac{a_{i-1} - a_{j-1}}{a_{j-1} - a_{k-1}} + 1.$$

As k ranges over $\{1, \ldots, q\} - \{j\}$, the difference $a_{j-1} - a_{k-1}$ ranges over GF(q^*. Since $w_{i0} = w_{j0} = 1$, the multiset $\{w_{ik} w_{jk}^{-1} : w_{ik} \neq 0 \neq w_{jk}$ and $0 \leq k < q+1\}$ contains each element of GF$(q)^*$ once. The remaining cases in which $i = 0$ or $j = 0$ are trivial. ■

0.14 Example. The matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha & \beta & \alpha\beta \\ 1 & \beta & \alpha\beta & \alpha \\ 1 & \alpha\beta & \alpha & \beta \end{bmatrix}$$

is a GH$(G; 1)$, where $G = \langle \alpha, \beta : \alpha^2 = \beta^2 = 1 \rangle \simeq$ EA(4).

0.15 Example. A BGW$(8, 7, 6;$ GF$(7)^*)$ formed from the proposition is given below

$$\begin{bmatrix} 0 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 3 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 0 & 3 & 1 & 6 & 2 & 5 \\ 3 & 5 & 6 & 0 & 4 & 2 & 1 & 3 \\ 3 & 6 & 4 & 1 & 0 & 5 & 3 & 2 \\ 3 & 1 & 3 & 5 & 2 & 0 & 6 & 4 \\ 3 & 2 & 5 & 4 & 6 & 3 & 0 & 1 \\ 3 & 3 & 2 & 6 & 5 & 1 & 4 & 0 \end{bmatrix},$$

where the nonzero elements are the logarithms of some generator of GF$(7)^*$. One can see that the matrix is skew-symmetric.

We present one final construction due to **?**, which we do not prove here, that yields what are called the classical family of BGWs; more than that, however, the matrices so constructed are what is termed ω-circulant, a simple generalization of cirulant matrices.

Let $G = \langle \omega \rangle$ be a finite cyclic group, and let $W = [w_{ij}]$ be a matrix over $\mathbf{Z}[G]$ with first row $(\alpha_0, \ldots, \alpha_{n-1})$. W is ω-circulant if and only if $w_{ij} = \alpha_{j-i}$ if $i \leq j$ and $w_{ij} = \omega \alpha_{j-i}$ if $i > j$, where the indices are calculated modulo n.

Finally, we are ready to present this very useful construction.

0.16 Proposition. Let q be a prime power, and let β be a primitive element of the extension of order d of the field GF(q). Further, take $m = (q^d - 1)/(q - 1)$, and define $\omega = \beta^{-m} \in \mathrm{GF}(q)$, i.e. the norm of β. Finally, we claim that the ω-circulant matrix with first row $(\mathrm{Tr}\beta^k)_{k=0}^{m-1}$ is a $\mathrm{BGW}(m, q^{d-1}, q^{d-1} - q^{d-2}; \mathrm{GF}(q)^*)$.[a]

0.17 Example. The matrix

$$\begin{bmatrix} 0&2&2&2&0&1&2&2&1&2&0&2&0 \\ 0&0&2&2&2&0&1&2&2&1&2&0&2 \\ 1&0&0&2&2&2&0&1&2&2&1&2&0 \\ 0&1&0&0&2&2&2&0&1&2&2&1&2 \\ 1&0&1&0&0&2&2&2&0&1&2&2&1 \\ 2&1&0&1&0&0&2&2&2&0&1&2&2 \\ 1&2&1&0&1&0&0&2&2&2&0&1&2 \\ 1&1&2&1&0&1&0&0&2&2&2&0&1 \\ 2&1&1&2&1&0&1&0&0&2&2&2&0 \\ 0&2&1&1&2&1&0&1&0&0&2&2&2 \\ 1&0&2&1&1&2&1&0&1&0&0&2&2 \\ 1&1&0&2&1&1&2&1&0&1&0&0&2 \\ 1&1&1&0&2&1&1&2&1&0&1&0&0 \end{bmatrix}$$

is an ω-circulant $\mathrm{BGW}(13, 9, 6; \mathrm{GF}(4)^*)$, where the nonzero elements are the logarithms of some generator of $\mathrm{GF}(4)^*$.

We present a few brief remarks on the conjugate transpose and similar operations on BGWs.

0.18 Proposition. If W is a $\mathrm{BGW}(v, k, \lambda; G)$, then W^* is also a $\mathrm{BGW}(v, k, \lambda; G)$.

Proof. Consider $W = [w_{ij}]$ as a matrix over the ring $\mathbf{Q}[G]$ so that it satisfies (**??**) over $\mathbf{Q}[G]$. Let $\pi : \mathbf{Q}[G] \to \mathbf{Q}[G]/\mathbf{Q}G$ be the natural ring epimorphism. If πW denotes the matrix $[\pi w_{ij}]$, then (**??**) becomes $(\pi W)(\pi W^*) = kI_v$, and hence $(\pi W)^{-1} = k^{-1}(\pi W^*)$. Therefore, $(\pi W^*)(\pi W) = kI_v$ so that $W^*W = kI_v + A$ for some $A = [a_{ij} \sum_{g \in G} g]$ over the ideal $\mathbf{Q}G$. Moreover, since $\check{W}^t$ is a BIBD, there exist integers a_g such that, for $i \neq j$, $\sum_k w_{ki} w_{kj}^{-1} = \sum_{g \in G} a_g g$ where $\sum_{g \in G} a_g = \lambda$. Evidently, then, $A = \frac{\lambda}{|G|}(\sum_{g \in G} g)(J_v - I_v)$, and the result follows. ■

0.19 Corollary. If W is a $\mathrm{BGW}(v, k, \lambda; G)$ where G is abelian, then $\overline{W}$ and W^t are also $\mathrm{BGW}(v, k, \lambda; G)$s.

Proof. Since the group is abelian, the map $g \mapsto g^{-1}$ is an automorphism; hence, by Proposition **??**, $\overline{W}$ is also a $\mathrm{BGW}(v, k, \lambda; G)$. Then, by the proposition, $(\overline{W})^* = W^t$ is also a $\mathrm{BGW}(v, k, \lambda; G)$. ■

[a] Recall that for a finite field K with finite extension F of order d, the trace function is the linear epimorphism $F \to K$ defined by $\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{d-1}}$, for $\alpha \in F$. Furthermore, the norm function is the linear epimorphism $F \to K$ defined by $\mathrm{N}_{F/K}(\alpha) = \alpha^{\frac{q^d - 1}{q-1}}$ for $\alpha \in F$. See **?** for details.

As before, we can impose an equivalence on the set A of all GBRD$(v, b, r, k, \lambda; G)$s. Specifically, the matrices that reside in the intersection of any orbit of the left action of $G \wr S_v$ on A with any orbit of the right action of $G \wr S_b$ on A are said to be monomially equivalent.

We conclude by altering somewhat Definition **??** as in (**?**, Part V).

0.20 Definition. let G be some finite group, and let A be a $v \times b$ $(0, G)$-matrix. If there is an element $c \in \mathbf{Z}[G]$ such that

(0.20.a) $AA^* = rI_v + c(J_v - I_v)$,

and if $\breve{A}$ is a BIBD, then we say that A is a c-GBRD, or a c-GBRD if more precision required.

Of course, a c-GBRD is a GBRD precisely when $c = \frac{\lambda}{|G|}\left(\sum_{g \in G} g\right)$.

0.4. Difference Set Construction III