0.1. Definitions. Imagine, for a moment, the simple senario in which you need to weigh several objects, say, four objects (see **?**, Chapter 2). Imagine further that you are using a simple balance with two pans that makes an error ϵ everytime that it is used, where ϵ is random with mean 0 and variance σ^2.

Assume the actual weights are a, b, c, and d. If we weigh them seperately with measurements y_1, y_2, y_3, and y_4, and if the errors are $\epsilon_1, \epsilon_2, \epsilon_3$, and ϵ_4, then we obtain the four equations

$$a = y_1 + \epsilon_1, \qquad b = y_2 + \epsilon_2, \qquad c = y_3 + \epsilon_3, \qquad d = y_4 + \epsilon_4.$$

The estimates of the weights are then

$$\hat{a} = y_1 = a - \epsilon_1, \quad \hat{b} = y_2 = b - \epsilon_2, \quad \hat{c} = y_3 = c - \epsilon_3, \quad \hat{d} = y_4 = d - \epsilon_4,$$

each having variance σ^2.

Now, we will weigh the objects together in the following way.

$$\begin{aligned} a + b + c + d &= y_1 + \epsilon_1, \\ a - b + c - d &= y_2 + \epsilon_2, \\ a + b - d - d &= y_3 + \epsilon_3, \\ a - b - c + d &= y_4 + \epsilon_4, \end{aligned}$$

where we have used $+1$ to indicate being placed on the right pan, and we have used -1 to indicate being placed on the left pan.

One can see that the coefficient matrix for the weighing configuration is non-singular. As such, we can solve for the variables; for example, we show the estimate for a:

$$\hat{a} = \frac{y_1 + y_2 + y_3 + y_4}{4}.$$

From this, we can see that the variance of $\hat{a}$ is given by $\sigma^2/4$, a large improvement from the initial configuration in which each weight was weighed independently.

In general, if there are n weights, and if there is a non-singular ternary (-1,0,1)-matrix of order n with a constant number of non-zero entries in each row, then that matrix can be used as a weighing configuration for the collection of objects in which the variance of the errors can be reduced.

All this motivates the following definition.

0.1. Definition. Let W be a $(-1, 0, 1)$-matrix of order n. W is a *weighing matrix* of *order* n and *weight* k iff

(0.1.a) If $WW^t = kI_n$.

If $n = k$, then we say that W is a *Hadamard matrix*. If $n - 1 = k$, then we say that W is a *conference matrix*. In any event, we write $\mathrm{W}(n, k)$ to denote this property.

0.2. Example. The following can be verified directly to be a $\mathrm{W}(13,9)$ (NB: We have used $-$ in place of -1 and $+$ in place of $+1$)

$$\text{(0.2.a)}\qquad \begin{pmatrix} 0&0&-&+&0&+&-&-&-&-&-&0&- \\ +&0&+&+&+&0&-&+&0&-&0&-&+ \\ +&0&0&-&+&+&+&0&-&+&-&-&0 \\ -&0&+&0&-&+&0&+&-&0&-&+&+ \\ -&-&-&+&0&+&+&+&0&0&+&-&0 \\ -&-&0&0&0&0&-&-&+&+&-&-&+ \\ +&+&-&+&0&+&0&0&+&+&0&+&+ \\ +&-&+&0&-&+&-&0&0&+&+&0&- \\ 0&+&0&+&-&-&0&+&0&+&-&-&- \\ 0&+&-&-&-&0&-&0&-&0&+&-&+ \\ 0&+&+&0&-&+&+&-&+&-&0&-&0 \\ -&+&0&-&+&+&-&+&+&0&0&0&- \\ +&-&-&-&-&0&0&+&+&-&-&0&0 \end{pmatrix}.$$

The weighing matrix of the previous example is indicative of a more general construction that uses relative difference sets (see §§3.4). Note that upon changing the nonzero entries of (0.2.a), one obtains the incidence matrix of the complement design of (**??**).

* * *

0.2. Necessary Conditions on Existence. The conditions placed on a matrix in order for it to be a weighing matrix are none too restrictive: One only needs orthogonality of the rows, a constant number of nonzero entries in every row, and the non-zero entries to have absolute value 1. Usually, in order to construct these objects one must assume some further combinatorial and/or algebraic properties. So-called cocyclic matrices, for example, are studied extensively in **?** and **?**. Nevertheless, we can say a few things at the outset.

By Cauchy's property of the determinant,cauchy-det $\det(W)^2 = k^n I_n$, for any $\mathrm{W}(n,k)$. In particular, if $n \equiv 1 \bmod 2$, then k is a square. This leaves the case that $n \equiv 0 \bmod 2$. It turns out, though we will not show it here, that if $n \equiv 2 \bmod 4$, then it must be the case that $k = a^2 + b^2$, for some $a, b \in \mathbf{Z}$.hasse-minkowski Much is not known about the case $n \equiv 0 \bmod 4$, though **?** conjectures that a $\mathrm{W}(4n,k)$ exists for every n and $k \leq 4n$.

Considering the weights, if $k = n-1$, then it is clear that $n \equiv 0 \bmod 2$; for otherwise, if n is odd, then there will be $n-2$ instances of $\binom{+}{+}$, $\binom{+}{-}$, or their negatives, in the product between any two distinct rows. Therefore, the product will resolve to a sum of $n-2$ terms each consisting of ± 1. Since $n-2 \equiv 1 \bmod 2$, this can never be zero.

In the case that $n = k$, we can assume (see §3.5) the first three rows have the following form.

$$\overbrace{\begin{matrix}+&\dots&+\\+&\dots&+\\+&\dots&+\end{matrix}}^{a}\quad\overbrace{\begin{matrix}+&\dots&+\\+&\dots&+\\-&\dots&-\end{matrix}}^{b}\quad\overbrace{\begin{matrix}+&\dots&+\\-&\dots&-\\+&\dots&+\end{matrix}}^{c}\quad\overbrace{\begin{matrix}+&\dots&+\\-&\dots&-\\-&\dots&-\end{matrix}}^{d}$$

Evidently, this configuration yields the following linear system.

$$\begin{aligned} a+b+c+d &= n,\\ a+b-c-d &= 0,\\ a-b+c-d &= 0,\\ a-b-c+d &= 0, \end{aligned}$$

whose solution is $a = b = c = d = n/4$. As these are integers, it must be the case, outside of the trivial cases $n = 1$ or 2, that $n \equiv 0 \bmod 4$ whenever $n = k$.

Finally, it follows by the definition and the above remarks that W is non-singular with $W^{-1} = k^{-1}W^t$, hence $W^tW = kI_n$. We record these result below.

0.3. Proposition. If there exists a W(n, k), say, W, then the following must hold.

(0.3.a) If $n - 1 = k$, then n is even;

(0.3.b) if $n = k$, then n is 1, 2, or a multiple of 4;

(0.3.c) if n is odd, then k is a square;

(0.3.d) if 2 exactly divides n, then k is the sum of two squares; and

(0.3.e) W is non-singular and $WW^t = W^tW = kI_n$.

* * *

0.3. Complex Weighing Matrices. There are many useful generalizations of weighing matrices. We will take this up generally in the next section, but for now we note the following special case, where we use A^* to denote the conjugate (Hermitian) transpose of a complex matrix A.

0.4. Definition. Let $G = \{\exp(\frac{2\pi im}{p}) : 0 \le m < p\}$, and let W be a $(0, G)$-matrix of order v. We say that W is a *Butson weighing matrix* of *order* v and *weight* k iff

(0.4.a) $WW^* = kI_n$,

and we write BW$(v, k; p)$ to denote this property.

0.5. Example. Let $\xi = \exp(\frac{2\pi i}{7})$, and let $H = (h_{ij})$, for $0 \le i, j < 7$, be defined by $h_{ij} = \xi^{ij}$. It follows easily that H is a Butson weighing matrix (see **?**, §2.5); in fact, it is a Butson Hadamard matrix as $n = k$. To be concrete, the following is a BW$(7, 7; 7)$

(0.5.a)
$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & \xi & \xi^2 & \xi^3 & \xi^4 & \xi^5 & \xi^6\\ 1 & \xi^2 & \xi^4 & \xi^6 & \xi & \xi^3 & \xi^5\\ 1 & \xi^3 & \xi^6 & \xi^2 & \xi^5 & \xi & \xi^4\\ 1 & \xi^4 & \xi & \xi^5 & \xi^2 & \xi^6 & \xi^3\\ 1 & \xi^5 & \xi^3 & \xi & \xi^6 & \xi^4 & \xi^2\\ 1 & \xi^6 & \xi^5 & \xi^4 & \xi^3 & \xi^2 & \xi \end{pmatrix}.$$

The next result, to be used later, is Lemma 2.8.5. of **?**.

0.6. Lemma. Let p be a prime, and let ξ be a primitive complex p-th root of unity. Then $\sum_{i=0}^{n} a_i \xi^i = 0$ for some $n < p$ and $a_i \in \mathbf{N}$ iff $n = p-1$ and $a_0 = \cdots = a_n$.

Proof. Let $f(x) = \sum_{i=0}^{n} a_i \xi^i \in \mathbf{Z}[x]$. The minimal polynomial of ξ over $\mathbf{Q}$ is the p-th cyclotomic polynomial $h(x) = 1 + x + \cdots + x^{p-1}$. Therefore, since the degree of f is at most p, we conclude that if $f(\xi) = 0$, then it must be an integer multiple of h. ■

* * *

0.4. Difference Set Construction II. Let G be some additive, finite group. In Definition **??**, a subset $D \in \binom{G}{k}$ was said to be a difference set if $\Delta(D)$ contained each element of $G \backslash \{0\}$ a constant number of times. Of course, we needn't restrict ourselves to omitting only the identity element; in fact, if we omit elements from a proper normal subgroup, we are left with a most useful object.

0.7. Definition. Let G be an additive, finite group for which $|G| = mn$, $N \subset G$ a normal subgroup of order n, and let $R \in \binom{G}{k}$ with $k < mn$. We say that R is a *relative difference set* in G with *forbidden subgroup* N iff

(0.7.a) If $\Delta(R) = \lambda(G \backslash N)$, for some $\lambda \in \mathbf{N}$.

If N is a direct factor of G, then we call R a *splitting* relative difference set. In any case, we write R is an RDS(m, n, k, λ) in G relative to N.

0.8. Example. The set $R = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}\}$ is an RDS$(5, 3, 4, 1)$ in $\mathbf{Z}/15\mathbf{Z}$ relative to $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}$.

0.9. Example. Let G be the direct product of $\mathbf{Z}/13\mathbf{Z}$ and S_3, and let $a = (1, 2)$ and $b = (1, 2, 3)$. Then $R = \{\overline{1}a, \overline{2}, \overline{3}ab, \overline{5}, \overline{6}, \overline{7}ab^2, \overline{8}a, \overline{9}ab^2, \overline{11}ab\}$ is an RDS$(13, 6, 9, 1)$ in G relative to S_3.

Though we do not show it here, just as difference sets are equivalent to square designs admitting a sharply transitive automorphism group, relative difference sets can be shown to be equivalent to group divisible designs admitting a sharply transitive automorphism group in which each element either fixes all or no point classes (see **?**).

For our purposes, however, we are interested in the application of differences sets to weighing matrices and their generalizations. By far the most important family of such relative difference sets are found in the next result which is Theorem 9.6.12 of **?**, and are called the *classical* relative difference sets.

0.10. Proposition. Let q be a prime power and $n > 1$. Let $f : \mathrm{GF}(q^n) \to \mathrm{GF}(q)$ be some nondegenerate linear map over $\mathrm{GF}(q)$. Then

(0.10.a) $R = \{x \in \mathrm{GF}(q^n) : f(x) = 1\}$ is an RDS in $\mathrm{GF}(q^n)^*$ relative to $\mathrm{GF}(q^*)$.

Moreover, the parameters of R are given by

(0.10.b) $\left(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2}\right)$.

Proof. Since f is nondegenerate, the Rank–Nullity Theoremrank-null implies that the dimension of $\ker(f)$ is $n-1$.

Suppose, for $x, y \in R$, that $xy^{-1} \in \mathrm{GF}(q)$. Then $1 = f(x) = af(y) = a$, hence $\mathrm{GF}(q)^* \cap \Delta(R) = \{1\}$.

It remains to verify that $\Delta(R) = q^{n-2}(\mathrm{GF}(q^n)^* \backslash \mathrm{GF}(q)^*)$. Let $t \in \mathrm{GF}(q^n)^* \backslash \mathrm{GF}(q)^*$, and define $g : \mathrm{GF}(q^n) \to \mathrm{GF}(q)$ by $g(y) = f(ty)$. It then suffices to show that there are q^{n-2} elements $y \in \mathrm{GF}(q^n)^*$ such that $f(y) = g(y) = 1$.

Since g is a nondegenerate linear map, the set $Y = g^{-1}(1)$ is an $(n-1)$-dimensional space over $\mathrm{GF}(q)$. Now, $\ker(g) = t^{-1}\ker(f)$, and, since $t \notin \mathrm{GF}(q)$, $\ker(g) \neq \ker(f)$. Therefore, $\dim(R \cap Y) = n-2$, and we're done. ■

0.11. Example. Take $K = \mathrm{GF}(3)$ and $F = \mathrm{GF}(27)$ with the usual polynomial representation, and let $\mathrm{Tr} : F \to K$ be the absolute trace function.trace-func By Proposition (0.10.a),

(0.11.a) $R = \{x \in F : \mathrm{Tr}(x) = 1\} = \{2x^2+x+2, 2x^2+2, 2x^2, 2x^2+x, 2x^2+2x+2, 2x^2+x+1, 2x^2+2x, 2x^2+2x+1, 2x^2+1\}$.

is an $\mathrm{RDS}(13, 2, 9, 3)$ in F^* relative to K^*.

The following result is standard, and we do not pause to prove it (see **?**).

0.12. Proposition. Let R be an $\mathrm{RDS}(m, n, k, \lambda)$ in a group G relative to a normal subgroup N, and let $\varphi : G \to H$ be a group epimorphism. Take $U = \ker(\varphi)$ and $|U| = u$. If $U \subseteq N$, then $\varphi(R)$ is an $\mathrm{RDS}(m, n/u, k, \lambda u)$ in H relative to $\varphi(N)$. In particular, if $U = N$, then $f(R)$ is a $\mathrm{DS}(m, k, \lambda u)$ in H.

We now present a construction of weighing matrices using relative difference sets. This construction is a special case of a more general result to be proven later, so we omit the proof.

0.13. Theorem. Let R be an $\mathrm{RDS}(m, 2, k, \lambda)$ in a group G relative to a normal subgroup $N = \{1, t\}$. Let $g_0, \ldots, g_{m-1}$ be distinct coset representatives of N in G. Let W be a $(-1, 0, 1)$-matrix of order m defined by

(0.13.a) $$W_{ij} = \begin{cases} 1 & \text{if } g_i g_j^{-1} \in R; \\ -1 & \text{if } t g_i g_j^{-1} \in R; \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Then W is a $\mathrm{W}(m, k)$.

Speaking of the relative difference sets (0.10.a) for odd q, we see that the forbidden subgroup is cyclic of even order, hence it has a unique normal subgroup of order 2. Proposition 0.12 and Theorem 0.13 then imply the existence of a $W((q^n-1)/(q-1), q^{n-1})$ for every $n > 1$. We record this result as a corollary.

0.14. Corollary. For every odd prime power q, there is a $W((q^n-1)/(q-1), q^{n-1})$, for every $n > 1$.

The case in which q is even, **?** showed that there is a $W((q^n-1)/(q-1), q^{n-1})$ whenever n is odd.

0.15. Example. Let R be as in (0.11.a). Using the coset representatives $1, 2x^2+2x, 2x^2+2x+1, x^2+x+1, x^2+2x, x^2+2x+2, 2x^2+x+2, 2x^2, 2x, 2x+1, 2x$ of GF$(3)^*$ in GF$(27)^*$, we can construct the weighing matrix in (0.2.a).

We will require one further result. Due to its length, we omit the proof; but the interested reader is refered to Chapter 9 of **?**.

0.16. Proposition. Let q be a prime power, α a primitve element of GF(q^2), and $G = \{g_0, \ldots, g_{q-1}\}$ a group of order q. Let $C_i = \{a\alpha^i : a \in \text{GF}(q)^*\}$, for each $i \in \{0, \ldots, q\}$. Define

(0.16.a) $R = \{(0, 1_g)\} \cup \{(a, 1_g) : a \in C_0\} \cup \bigcup_{i=1}^{q} \{(a, g_{i-1}) : a \in C_i\}$.

Then R is an RDS(q^2, q, q^2, q) in GF$(q^2)^+ \times G$ relative to $\{0\} \times G$.

Proposition 0.12 then yields the following.

0.17. Corollary. Let p be a prime, and let $m \leq n$ be positive integers. Let $A =$ GF$(q^{2m})^+$, and let G be any group of order p^n. Then there is an RDS$(p^{2m}, p^n, p^{2m}, p^{2m-n})$ in $A \times G$ relative to $\{0\} \times G$.

* * *

0.5. Isomorphisms of Weighing Matrices. Let W be some W(v, k), and let P and Q be signed permutation matrices of order v. It is then clear that PWQ is again a W(v, k). We have the following.

0.18. Definition. Two weighing matrices W_1 and W_2 are *Hadamard equivalent* if there are two signed permutation matrices P and Q such that

(0.18.a) $PW_1Q = W_2$.wreath-prod

0.19. Example. The weighing matrix (0.2.a) is Hadamard equivalent to the following.

(0.19.a)
$$\begin{pmatrix}
0&0&+&+&0&+&+&+&+&+&0&+\\
0&+&0&+&-&-&0&-&0&-&+&-&+\\
0&+&+&-&-&0&+&0&+&0&-&-&-\\
0&+&-&0&-&+&-&+&-&+&0&-&0\\
+&0&-&+&+&0&+&-&0&+&0&+&-&-\\
+&0&0&-&+&+&-&0&+&-&+&-&0\\
+&0&+&0&+&-&0&+&-&0&-&-&+\\
+&+&-&-&0&-&+&+&0&0&+&+&0\\
+&+&0&0&0&0&-&-&+&+&-&+&+\\
+&+&+&+&0&+&0&0&-&-&0&+&-\\
+&-&-&0&-&+&+&0&0&-&-&0&+\\
+&-&0&+&-&-&-&+&+&0&0&0&-\\
+&-&+&-&-&0&0&-&-&+&+&0&0
\end{pmatrix}$$

The above example motivates the following definition.

0.20. Definition. A $\mathrm{W}(v,k)$ is said to be in *normal form* if it has the form

(0.20.a)
$$\begin{pmatrix} \mathbf{0}_{v-k} & A_1 \\ \mathbf{1}_k & A_2 \end{pmatrix}.$$

Similar to designs, we call A_1 the *residual part* and A_2 the *derived part* of the weighing matrix.

As a consequence of (0.20.a), we have

(0.20.b) $A_1 A_1^t = kI_{v-k}$ and

(0.20.c) $A_2 A_2^t = kI_k - J_k$.