Perfect Codes and Balanced Generalized Weighing Matrices

Dieter Jungnickel
Lehrstuhl für Diskrete Mathematik, Optimierung
und Operations Research
Universität Augsburg
D–86135 Augsburg, Germany

and

Vladimir D. Tonchev*
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931
USA

March 15, 2001

Abstract

It is proved that any set of representatives of the distinct 1-dimensional subspaces in the dual code of the unique linear perfect single-error-correcting code of length \(\frac{q^d-1}{q-1}\) over \(GF(q)\) is a balanced generalized weighing matrix over the multiplicative group of \(GF(q)\). Moreover, this matrix is characterized as the unique (up to equivalence) weighing matrix for the given parameters with minimum \(q\)-rank. The classical, more involved construction for this type of BGW-matrices is discussed for comparison, and a few monomially inequivalent examples are included.

*Research partially supported by a research grant of the Alexander von Humboldt Foundation.
1 Introduction

We assume familiarity with some basic facts and notions from coding theory and combinatorial design theory ([2], [6], [7]). In particular, we require the following definitions.

**Definition 1.1** A balanced generalized weighing matrix $BGW(m, k, \mu)$ over a group $G$ is an $m \times m$ matrix $W = (w_{ij})$ with entries from $G := G \cup \{0\}$ such that each row of $W$ contains exactly $k$ nonzero entries, and for every $a, b \in \{1, \ldots, m\}$, $a \neq b$, the multiset $\{g_{ai}g_{bi}^{-1} : 1 \leq i \leq m, g_{ai}, g_{bi} \neq 0\}$ contains exactly $\mu/|G|$ copies of each element of $G$.

**Definition 1.2** Two matrices over $GF(q)$ are said to be monomially equivalent if one is obtainable from the other by permutations of rows and columns and multiplying rows and columns by nonzero elements from $GF(q)$.

There are many monomially inequivalent balanced generalized weighing matrices with the same parameters that are distinguishable by their rank over $GF(q)$. Some small examples are listed in the Appendix. These examples, as well as many other ones are obtained by decomposing difference sets with the “classical” parameters $(2^{d+1} - 1, 2^d - 1, 2^{d-1} - 1)$ with respect to a subdesign with classical parameters [4].

It is the aim of this note to give a simple coding-theoretical construction of the balanced generalized weighing matrices with parameters $\left(\frac{q^{d-1}}{q-1}, q^{d-1}, q^{d-1} - q^{d-2}\right)$ of minimum $q$-rank, and to characterize these matrices as the unique (up to monomial equivalence) matrices of minimum $q$-rank.

2 A class of weighing matrices from the simplex code

The $q$-ary simplex code $S_d(q)$ of length $\frac{q^{d-1}}{q-1}$, where $d \geq 2$ and $q$ is a prime power, is defined as a linear code over $GF(q)$ with a generator matrix having as columns representatives of all distinct 1-dimensional subspaces of the $d$-dimensional vector space $GF(q)^d$. In other words, $S_d$ is the dual code of the unique linear perfect single-error-correcting code of length $\frac{q^{d-1}}{q-1}$ over $GF(q)$, that is, the $q$-ary analogue of the Hamming code.

**Lemma 2.1** (i) The Hamming weight enumerator of $S_d(q)$ is given by

$$1 + (q^d - 1)x^{d-1}.$$
(ii) The supports of all nonzero vectors in $S_d(q)$ are the blocks of a symmetric
$2-(q^{d-1}q^{-1}, q^{d-1}, q^{d-1} - q^{d-2})$ design isomorphic to the design with blocks the complements of hyperplanes in $PG(d - 1, q)$.

The statement (i) is a folklore fact. For a proof of (ii), see [8].

**Theorem 2.2** Any $q^{d-1}q^{-1} \times q^{d-1}q^{-1}$ matrix $M$ with rows a set of representatives of the $q^{d-1}q^{-1}$ distinct 1-dimensional subspaces of $S_d(q)$ is a balanced generalized weighing matrix with parameters

$$m = \frac{q^d - 1}{q - 1}, \quad k = q^{d-1}, \quad \mu = q^{d-1} - q^{d-2}$$

over the multiplicative group $GF(q)^*$ of $GF(q)$.

**Proof.** Let $x = (x_1, x_2, \ldots, x_m)$ be a row of $M$. By 2.1, if $y = (y_1, y_2, \ldots, y_m)$ is any other row of $M$, there are exactly $q^{d-1} - q^{d-2}$ indices $i$ such that $x_i \neq 0$ and $y_i \neq 0$. We want to show that the multiset

$$S = \{x_i : y_i^{-1} \mid y_i \neq 0\}$$

contains every nonzero element of $GF(q)$ equally frequently, that is, exactly $q^{d-2}$ times. Note that multiplication of any column or a row of $M$ by a nonzero element of $GF(q)$ preserves the set of frequencies of the elements in $S$. Therefore, multiplying the $i$th column of $M$ by $y_i^{-1}$ for all $i$ such that $y_i \neq 0$, transforms $M$ into a matrix $M'$ in which $x$ is transformed into $x' = (\ldots x_i y_i^{-1} \ldots)$ and $y$ becomes a $(0, 1)$-vector $y'$. By Lemma 2.1,

$$D_H(x', y') = D_H(x, y) = q^{d-1},$$

where $D_H$ denotes the Hamming distance. Let

$$I = \{i \mid x_i' \neq 0 \text{ and } y_i' \neq 0\}.$$ 

In order for $M'$ (and therefore $M$) to be a balanced generalized weighing matrix, the multiset $S' = \{x_i' \mid i \in I\}$ has to contain each of the $q - 1$ nonzero elements of $GF(q)$ the same number of times, that is, $q^{d-2}$ times. Note that $q^{d-2} = (q^{d-1} - q^{d-2})/(q - 1)$ is the average frequency of an element in $S'$. If there is some $\beta \in GF(q)$, $\beta \neq 0$ that occurs more than $q^{d-2}$ times in $S'$ then multiplying the vector $x'$ by $\beta^{-1}$ gives a vector $x''$ such that $D_H(x'', y') < q^{d-1}$; but another application of Lemma 2.1 shows $D_H(x'', y') = q^{d-1}$, a contradiction. \hfill $\square$
Theorem 2.3 Let $M$ be any balanced generalized weighing matrix with parameters $(\frac{q^d-1}{q-1}, q^{d-1}, q^{d-1} - q^{d-2})$ over $GF(q)^\ast$. Then

$$\text{rank}_q M \geq d.$$ 

Moreover, the equality $\text{rank}_q M = d$ holds if and only if $M$ is monomially equivalent to a matrix obtained by the construction of Theorem 2.2.

Proof. Since the rows of $M$ and their nonzero multiples constitute $q^d - 1$ distinct nonzero vectors in the row space $C$ of $M$ over $GF(q)$, the rank of $M$ over $GF(q)$, $\text{rank}_q(M)$, is at least $d$. If $\text{rank}_q(M) = d$ then $C$ consists of the zero vector and all nonzero multiples of the rows of $M$. Since the supports of the rows, as well as the columns of $M$ are the blocks of a symmetric design with parameters $2-(\frac{q^d-1}{q-1}, q^{d-1}, q^{d-1} - q^{d-2})$, that is, a 2-design with $k > \lambda$, any two columns of $M$ are linearly independent over $GF(q)$. Consequently, the orthogonal subspace (or dual code) $C^\perp$ has minimum Hamming distance at least 3. Thus, $C^\perp$ is a linear single-error-correcting code of length $\frac{q^d-1}{q-1}$ and dimension $\frac{q^d-1}{q-1} - d$ that meets the Hamming (sphere packing) bound, hence $C^\perp$ must be monomially equivalent to the unique linear perfect code with these parameters, namely, the $q$-ary Hamming code. Any basis of $C$ formed by rows of $M$ consists of $d$ linearly independent rows. By the remarks about $C^\perp$, the set of columns of $B$ is a set of distinct representatives of all 1-dimensional subspaces of the $d$-dimensional vector space $GF(q)^d$. Consequently, the matrix $B$ is unique up to monomial equivalence over $GF(q)$.

$\Box$

3 A comparison with the classical construction

There is a “classical” construction for balanced generalized weighing matrices with parameters

$$m = \frac{q^{d+1} - 1}{q - 1}, \quad k = q^d, \quad \mu = q^d - q^{d-1}$$

over the multiplicative group $GF(q)^\ast \cong \mathbb{Z}_{q-1}$ of $GF(q)$ which we will now recall; see [3] and [5] for background. We warn the reader that the notation used by us differs from that in [3], where we used $\lambda = \mu/n$ instead of $\mu$ as the third parameter of a $BGW$-matrix.
Let $R$ be the set of elements of $GF(q^{d+1})$ of trace 1 relative to $GF(q)$. Then $R$ is a classical relative difference set with parameters $(\frac{q^{d+1}-1}{q-1}, q-1, q^d, q^{d-1})$ in $GF(q^{d+1})$ relative to $N = GF(q)^*$. Let $\beta$ be a primitive element of $GF(q^{d+1})$ and define a $(\frac{q^{d+1}-1}{q-1} \times \frac{q^{d+1}-1}{q-1})$-matrix $W = (w_{ij})$ with entries in $GF(q)$ as follows. If there is a (necessarily unique) element $r$ of $R \beta^i$ in the coset $N \beta^j$, then set $w_{ij} = \beta^{-j} r$, and otherwise set $w_{ij} = 0$. Then $W$ is the desired BGW-matrix. Actually, this construction gives BGW-matrices of a special form, namely $\omega$-circulant matrices, where $\omega = \beta^{-1}$. Recall that an $\omega$-circulant matrix is defined by the following property: each row of $W$ is obtained from the preceding row by shifting every entry but the one in the final column one position to the right, whereas the entry in the final column is first multiplied by $\omega$ and then the result is put in the first position of the shifted row. Formally, we have

$$w_{i,j} = w_{i+1,j+1} \text{ for } j = 1, \ldots, m-1 \text{ and } w_{i+1,1} = \omega w_{i,m}.$$  

By a result of [3], $\omega$-circulant BGW-matrices over a cyclic group and cyclic relative difference sets are actually equivalent concepts:

**Result 3.1** Let $N$ be a cyclic group of order $n$, and let $\omega$ be a generator for $N$. Then the existence of a $\omega$-circulant BGW-matrix with parameters $(m, k, \mu)$ over $N$ is equivalent to the existence of an $(m, n, k, \lambda)$-difference set in the cyclic group $G$ of order $v = mn$ relative to the unique subgroup of order $n$ (which may, of course, be identified with $N$), where $\lambda = \mu/n$. \hfill \Box

It is also known that the classical BGW-matrices can be put into circulant form whenever $(q-1, \frac{q^{d+1}-1}{q-1}) = 1$. This is an easy consequence of the following analogue of Result 3.1, see [3]. Here a matrix $A = (a_{g,h})$ whose rows and columns are indexed by the elements of a group $H$ is called $H$-invariant provided that

$$a_{g,h} = a_{g+k,h+k} \text{ for all } g, h, k \in H.$$  

In particular, $A$ is circulant if and only if it is $H$-invariant for a cyclic group $H$.

**Result 3.2** Let $H$ and $N$ be groups of orders $m$ and $n$, respectively, and let $G = H \times N$. Then the existence of an $H$-invariant BGW-matrix with parameters $(m, k, \mu)$ over $N$ is equivalent to the existence of an $(m, n, k, \lambda)$-difference set in $G$ relative to $N$, where $\lambda = \mu/n$. \hfill \Box

For obvious reasons, relative difference sets of the form described in Result 3.2 are called **splitting**. We now have the following result.
Proposition 3.3 The matrices constructed in Theorem 2.2 can be put into \( \omega \)-circulant form. They can also be put circulant form whenever \((q - 1, \frac{2^{p-1}-1}{q-1}) = 1\).

Proof. The second assertion follows from the well-known fact that the \( q \)-ary Hamming code (and hence its dual, the simplex code) is a cyclic code in these cases. In general, the matrices of Theorem 2.2 can be put into \( \omega \)-circulant form, since the \( q \)-ary Hamming code always is a constacyclic code; see, for instance, [1], p. 303.

It is an open problem whether or not our construction gives the same matrices (up to monomial equivalence) as the classical construction outlined in this section, though the few small examples we have checked out suggest this to be the case. Although the \( p \)-ranks of the classical affine difference sets are known, this does not seem to imply a simple formula for the rank of the corresponding BGW-matrices over \( GF(q) \). In any case, the construction presented here is obviously much simpler to implement than the classical one.

4 Appendix

In Table 4.1 we use the following notation: if \( \alpha \) is a primitive root of \( GF(q) \) then \( i \) denotes \( \alpha^{i-1} \) for \( 1 \leq i \leq q - 1 \), and 0 is the zero in \( GF(q) \).
Table 4.1 Some inequivalent BGW-matrices

<table>
<thead>
<tr>
<th>No.</th>
<th>((m, k, \mu))</th>
<th>(q)</th>
<th>(q)-rank</th>
<th>first row</th>
<th>(\omega)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>((9, 8, 7))</td>
<td>8</td>
<td>2</td>
<td>(161266510)</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>((9, 8, 7))</td>
<td>8</td>
<td>4</td>
<td>(517745750)</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>((73, 64, 56))</td>
<td>8</td>
<td>3</td>
<td>(0040454035374520737753643)</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>52771305453044774322157</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>327110424362360373577234</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>((73, 64, 56))</td>
<td>8</td>
<td>9</td>
<td>(0040556047572240657427645)</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>131551012270415413452351</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>716630647176650465141444</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>((85, 64, 48))</td>
<td>4</td>
<td>4</td>
<td>(1111310122310031030322011000)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2211301210321333102101002030</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>231331331320021231110223321220</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>((85, 64, 48))</td>
<td>4</td>
<td>16</td>
<td>(32333220233313002302032102300)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3322202320133211201302001010</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1222231323003332232320112232130</td>
<td></td>
</tr>
</tbody>
</table>

Acknowledgment The second author wishes to thank the university of Augsburg, Germany, for the hospitality during his visit as a research fellow of the Alexander von Humboldt Foundation.

References


