Perfect Codes and Balanced Generalized Weighing Matrices

Dieter Jungnickel
Institut für Mathematik
Universität Augsburg

December 5, 2013

Overview

1. BGW-matrices
2. The classical family and codes
3. Background: Relative difference sets
4. BGW-matrices and relative difference sets
5. Monomially inequivalent BGW-matrices
6. Problems

The talk is based on joint work with Vladimir D. Tonchev (Michigan Technological University).

BGW-matrices

A **balanced generalized weighing matrix** $BGW(m, k, \mu)$ over a (multiplicative) group G is an $(m \times m)$-matrix

$$W = (w_{ij}) \quad \text{with entries from} \quad \overline{G} := G \cup \{0\}$$

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

$$\{w_{ai} w_{bi}^{-1} : 1 \leq i \leq m, w_{ai}, w_{bi} \neq 0\}$$

contains exactly $\mu/|G|$ copies of each element of G.

If G is cyclic, we denote a fixed generator by ω.

Special cases

Generalised Hadamard matrices:

Here $m = k$ (so there are no entries 0). Notation: $GH(n, \lambda)$, where $n = |G|$ and $\lambda = m/n$. Existence is known for $G = EA(q)$ and parameters $(q, 1)$, $(q, 2)$, $(q, 4)$, etc.

Generalised conference matrices:

Here $m = k + 1$, with entries 0 on the main diagonal. Notation: $GC(n, \lambda)$, where $n = |G|$ and $\lambda = (k - 1)/n$. Existence is known for $G = \mathbb{Z}_s$, s is a divisor of $q - 1$, $k = q$ a prime power.

The classical family:

$$BGW\left(\frac{q^d - 1}{q - 1}, q^{d-1}, q^{d-1} - q^{d-2}\right) \text{ over } \mathbb{Z}_s,$$

where q is a prime power, $s|q - 1$, and $d \geq 2$.

Examples

For $|G| = 2$, one has *Hadamard matrices* and *conference matrices*.

A $GH(3,2)$:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \omega & \omega^2 & 1 & \omega^2 & 1 & \omega \\ \omega & 1 & \omega^2 & \omega^2 & \omega & 1 \\ 1 & \omega^2 & \omega^2 & 1 & \omega & \omega \\ \omega^2 & \omega^2 & 1 & \omega & \omega & 1 \\ \omega^2 & 1 & \omega^2 & \omega & 1 & \omega \end{pmatrix}$$

A $GC(3,1)$:

$$\begin{pmatrix} 0 & 1 & \omega & \omega & 1 \\ 1 & 0 & 1 & \omega & \omega \\ \omega & 1 & 0 & 1 & \omega \\ \omega & \omega & 1 & 0 & 1 \\ 1 & \omega & \omega & 1 & 0 \end{pmatrix}$$

Some general results

Proposition. The existence of a $BGW(m, k, \mu)$ over some group G of order m implies that of a symmetric (m, k, μ)-design.

Let $D^{(-1)}$ be the matrix arising from D by replacing each group element g by its inverse g^{-1}, and D^* the transpose of $D^{(-1)}$.

Lemma. Let G be a finite group. A matrix D of order m with entries from $G \cup \{0\}$ is a $BGW(m, k, \mu)$ if and only if the following matrix equation holds over the group ring $\mathbb{Z}G$:

$$DD^* = \left(k - \frac{\mu}{|G|}G\right) I + \frac{\mu}{|G|}GJ,$$

where J denotes the all 1 matrix.

Some general results II

Proposition. (Cameron, Delsarte and Goethals 1979)
If D is a $BGW(m,k,\mu)$ over G, then so is D^*.

Theorem. (De Launey 1984)
Suppose the existence of a $BGW(m,k,\mu)$ over a group G of order n. Then:

- If m is odd and n is even, k must be a square.
- If G admits an epimorphism onto a cyclic group of odd prime order p and if h is an integer which divides the squarefree part of k but is not a multiple of p, then the order of h modulo p must be odd.

Universität Augsburg University

Related geometries

Theorem. (DJ 1982)

- The existence of a $BGW(m, k, \mu)$ over a group G of order n is equivalent to that of a symmetric divisible design with parameters (m, n, k, λ) admitting G as a class regular automorphism group, where $\lambda = \mu/n$.
- The existence of a generalized Hadamard matrix $GH(n, 1)$ over a group G of order n is equivalent to that of a finite projective plane of order n which admits G as the group of all (p, L)-elations for some flag (p, L).
- The existence of a generalized conference matrix $GC(n-1, 1)$ over G of order $n-1$ is equivalent to that of a finite projective plane of order n which admits G as the group of all (p, L)-homologies for some antiflag (p, L).

Background: Simplex codes

The q-ary **simplex code** $S_d(q)$ of length $\frac{q^d-1}{q-1}$ is the 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 $GF(q)^d$.

NB: $S_d(q)$ 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, of the q-ary analogue of the Hamming code.

Lemma. Each non-zero vector in $S_d(q)$ has Hamming weight q^{d-1}. Moreover, the supports of all these vectors form the blocks of a symmetric $(\frac{q^d-1}{q-1}, q^{d-1}, q^{d-1} - q^{d-2})$ design which is isomorphic to the complement of the classical point-hyperplane design in the projective space $PG(d-1, q)$.

The classical family via codes

Theorem. Any $\frac{q^d-1}{q-1} \times \frac{q^d-1}{q-1}$ matrix M with rows a set of representatives of the $\frac{q^d-1}{q-1}$ distinct 1-dimensional subspaces of $S_d(q)$ is a BGW-matrix with parameters

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

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

Moreover, such a matrix has rank d over $GF(q)$.

A characterization

Theorem. Let M be any BGW-matrix with parameters

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

over $GF(q)^*$. Then

$$rank_q M \geq d.$$

Moreover, the equality $rank_q M = d$ holds if and only if M is monomially equivalent to a matrix obtained from the simplex code.

ω-circulant matrices

An $m \times m$ matrix W is called ω-**circulant** provided that for $i = 1, \ldots, m-1$:

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

and

$$w_{i+1,1} \;=\; \omega w_{i,v}.$$

Proposition. The BGW-matrices above can always be put into into ω-circulant form. They can also be put into circulant form whenever $(q-1, \frac{q^{d+1}-1}{q-1}) = 1$.

An explicit description

Let β be a primitive element β for $GF(q^d)$ and $\omega = \beta^{-m}$. Let W be the ω-circulant $(m \times m)$-matrix with first row

$$\mathbf{w} \;=\; (\operatorname{Tr}\beta^0, \operatorname{Tr}\beta^1, \ldots, \operatorname{Tr}\beta^{m-1}). \tag{1}$$

Then, with $v = m(q-1) = q^d - 1$,

$$W \;=\; \begin{pmatrix} \operatorname{Tr}\beta^0 & \operatorname{Tr}\beta^1 & \operatorname{Tr}\beta^2 & \ldots & \operatorname{Tr}\beta^{m-1} \\ \operatorname{Tr}\beta^{v-1} & \operatorname{Tr}\beta^0 & \operatorname{Tr}\beta^1 & \ldots & \operatorname{Tr}\beta^{m-2} \\ \operatorname{Tr}\beta^{v-2} & \operatorname{Tr}\beta^{v-1} & \operatorname{Tr}\beta^0 & \ldots & \operatorname{Tr}\beta^{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ \operatorname{Tr}\beta^{v-(m-1)} & \operatorname{Tr}\beta^{v-(m-2)} & \ldots & \ldots & \operatorname{Tr}\beta^0 \end{pmatrix}.$$

NB: By the linearity of the trace function and the definition of ω,

$$\omega \mathrm{Tr}\, \beta^j = \mathrm{Tr}(\omega\beta^j) = \mathrm{Tr}\, \beta^{j-m} = \mathrm{Tr}\, \beta^{m(q-2)+j}.$$

Proof. The rows of W have weight q^{d-1}. Thus it suffices to check that W has q-rank d.

Note that W is the submatrix formed by the first m rows and columns of the circulant $v \times v$ matrix C with first row

$$\mathbf{c} = (\mathrm{Tr}\, \beta^0, \mathrm{Tr}\, \beta^1, \ldots, \mathrm{Tr}\, \beta^{v-1}) = (\mathbf{w}, \lambda\mathbf{w}, \ldots, \lambda^{q-2}\mathbf{w}).$$

This is the first period of an m-sequence, as β is a primitive element for $GF(q^d)$. Hence the circulant matrix C has q-rank d. But then W also has q-rank d.

Background: Relative difference sets

Let G be an additively written group of order $v = mn$, and let N be a normal subgroup of order n and index m of G. A k-element subset R is called a **relative difference set** with parameters (m, n, k, λ), if the list of differences

$$(r - r' : r, r' \in R, r \neq r')$$

contains no element of N and covers every element in $G \backslash N$ exactly λ times.

Example: Let R be the set of elements of $GF(q^d)$ of trace 1 (relative to $GF(q)$). Then R is an RDS with parameters

$$(\frac{q^d - 1}{q - 1}, q - 1, q^{d-1}, q^{d-2})$$

in the cyclic group $G = GF(q^d)^*$ relative to $N = GF(q)^*$.

BGW-matrices via relative difference sets

Proposition. Let N be a cyclic group of order n with generator ω. Then the existence of an ω-circulant BGW-matrix with parameters (m, k, μ) over N is equivalent to that of an (m, n, k, λ)-difference set in the cyclic group G of order $v = mn$ relative to the unique subgroup of order n, where $\lambda = \mu/n$.

Proposition. Let R be the trace 1-RDS, and define an $(m \times m)$-matrix $X = (x_{ij})_{i,j=0,\dots,m-1}$ with entries in $GF(q)$ as follows:

> If there is a (necessarily unique) element $r \in R\beta^j \cap N\beta^i$, then set $x_{ij} = \beta^{-j}r$, and otherwise set $x_{ij} = 0$.

Then X is an ω-circulant BGW-matrix with classical parameters.

The relation to the perfect code construction

Theorem. Let W be the BGW-matrix with classical parameters and q-rank d constructed via the simplex code, and let X be the ω-circulant matrix associated with the trace 1-RDS. Then $X = W^*$.

Problem: Determine the q-rank of the "classical" BGW-matrix $X = W^*$.

Equivalently, determine the q-rank of $X^T = W^{(-1)} = W^{(q-2)}$.

More generally, determine the q-rank of *all* BGW-matrices of the form $W^{(t)}$.

Monomially inequivalent BGW-matrices

Theorem. Let W be the BGW-matrix with classical parameters and q-rank d constructed via the simplex code, and let t be a positive integer in the range $1 \leq t \leq q-2$.

Write $q = p^r$, where p is prime, and let $\sum_{i=0}^{r-1} t_i p^i$ be the p-ary expansion of t (thus $0 \leq t_i < p$ for all i). Then

$$\mathrm{rank}_q W^{(t)} = \prod_{i=0}^{r-1} \binom{d-1+t_i}{d-1}.$$

Sketch of proof.

As before, the ω-circulant matrix $W^{(t)}$ is a submatrix of a larger circulant matrix, $C^{(t)}$, with first row

$$\mathbf{c}^{(t)} = ((\mathrm{Tr}\,\beta^0)^t, (\mathrm{Tr}\,\beta^1)^t, \ldots, (\mathrm{Tr}\,\beta^{v-1})^t).$$

The periodic sequences with first period $\mathbf{c}^{(t)}$ are twisted versions of m-sequences; their linear complexity and hence the rank of the matrices $C^{(t)}$ were determined by Antweiler and Bömer (1992).

Now one shows that $W^{(t)}$ has the same rank, using some results on linear shift register sequences.

Two consequences

- Let $X = \left(W^{(q-2)}\right)^T$ be the classical balanced generalized weighing matrix from the RDS-construction. Then, with $q = p^r$,

$$\mathrm{rank}_q X \;=\; \binom{d+p-3}{d-1}\binom{d+p-2}{d-1}^{r-1}.$$

- Let W be the BGW-matrix with classical parameters and q-rank d constructed via the simplex code, and let t be a positive integer in the range $1 \leq t \leq q-2$ satisfying $(t, q-1) = 1$. Write $q = p^r$, where p is prime. Then the matrix $W^{(t)}$ is monomially equivalent to W if and only if the mapping $x \mapsto x^t$ is an automorphism of $GF(q)$, that is, if and only if $t = p^h$ for some integer h.

A few problems

- There exist further examples of inequivalent BGW-matrices with classical parameters, e.g. an example with parameters (85,64,48) and rank 16 over $GF(4)$. Problem: Find further general constructions or even a classification.

- Find families of ω-circulant BGW-matrices over other but cyclic groups.

- The only other known family of parameters is

$$m = k + 1,\ k = n(2n - 1),\ \mu = k - 1$$

  over the cyclic group of order n, where $n = 2^{d-1} - 1$ and $d \geq 3$. Find an infinite family of BGW-matrices with new parameters. Even better, find a new family of cyclic relative difference sets.

Thanks for your attention.