Balanced Generalized Weighing Matrices and Optimal Codes

Thomas Pender

University of Lethbridge
Department of Mathematics and Computer Science

Canadian Mathematical Society Winter Meeting
Decemeber 2021

***Joint work with Hadi Kharaghani, Sho Suda, Vlad Zatiev

Codes—Definition

- Finite collection of “strings” of given length over a given finite alphabet.
- Finite alphabet $\mathcal{A}$ with distinguished letter “0” called zero.
- Every $\mathscr{C} \subseteq \mathcal{A}^n$ is a code.
- Write $\mathscr{C}$ is an $(n, M, d)_a$–code, where
  - $M = |\mathscr{C}|$
  - $a = |\mathcal{A}|$
  - d is the Hamming distance (def. below).

Codes—Hamming Weight

- Weight of a codeword $c = c_0 \cdots c_{n-1}$.

$$\mathrm{wt}(c) = \#\{i : c_i \neq 0\}$$

- Weight of $\mathscr{C}$.

$$\mathrm{wt}(\mathscr{C}) = \min_{c \in \mathscr{C}} \mathrm{wt}(c).$$

- $\mathscr{C}$ is constant weight if $\#\{\mathrm{wt}(c) : c \in \mathscr{C}\} = 1$.
- Assume $\mathscr{C}$ is constant weight with $\mathrm{wt}(\mathscr{C}) = w$.

Codes—Hamming Distance

- Distance between code words $c = c_0 \cdots c_{n-1}$ and $c' = c'_0 \cdots c'_{n-1}$.

$$d(c, c') = \#\{i : c_i \neq c'_i\}$$

- Distance of $\mathscr{C}$.

$$d(\mathscr{C}) = \min_{\substack{c,c' \in \mathscr{C}^2 \\ c \neq c'}} d(c, c')$$

- $\mathscr{C}$ is equidistant if $\#\{d(c, c') : c, c' \in \mathscr{C}, c \neq c'\} = 1$.

- Fundamental question to maximize M given n, d, w and a.
- Denote this max by $\mathrm{A}_a(n,d,w)$.

Restricted Johnson Bound

$$\mathrm{A}_a(n,d,w) \leqq \left\lfloor \frac{nd(a-1)}{aw^2 - 2(a-1)nw + nd(a-1)} \right\rfloor \tag{1}$$

Codes—Example

- $\mathcal{A} = \{-, 0, 1\}$, where $-$ represents -1.

Codes—Example

- $\mathcal{A} = \{-, 0, 1\}$, where $-$ represents -1.

$$1\ 1\ 1\ -\ 0\ -\ -\ 1$$

Codes—Example

- $\mathcal{A} = \{-, 0, 1\}$, where $-$ represents -1.

$$\begin{array}{cccccccc} 1 & 1 & 1 & - & 0 & - & - & 1 \\ - & 1 & 1 & 1 & - & 0 & - & - \end{array}$$

Codes—Example

- $\mathcal{A} = \{-, 0, 1\}$, where $-$ represents -1.

$$\begin{array}{cccccccc}
1 & 1 & 1 & - & 0 & - & - & 1 \\
- & 1 & 1 & 1 & - & 0 & - & - \\
1 & - & 1 & 1 & 1 & - & 0 & -
\end{array}$$

- $\mathcal{A} = \{-, 0, 1\}$, where $-$ represents -1.

$$
\begin{array}{cccccccc}
1 & 1 & 1 & - & 0 & - & - & 1 \\
- & 1 & 1 & 1 & - & 0 & - & - \\
1 & - & 1 & 1 & 1 & - & 0 & - \\
1 & 1 & - & 1 & 1 & 1 & - & 0
\end{array}
$$

Codes—Example

- $\mathcal{A} = \{-, 0, 1\}$, where $-$ represents -1.

$$\begin{matrix} 1 & 1 & 1 & - & 0 & - & - & 1 \\ - & 1 & 1 & 1 & - & 0 & - & - \\ 1 & - & 1 & 1 & 1 & - & 0 & - \\ 1 & 1 & - & 1 & 1 & 1 & - & 0 \\ 0 & 1 & 1 & - & 1 & 1 & 1 & - \end{matrix}$$

Codes—Example

- $\mathcal{A} = \{-, 0, 1\}$, where $-$ represents -1.

$$\begin{matrix} 1 & 1 & 1 & - & 0 & - & - & 1 \\ - & 1 & 1 & 1 & - & 0 & - & - \\ 1 & - & 1 & 1 & 1 & - & 0 & - \\ 1 & 1 & - & 1 & 1 & 1 & - & 0 \\ 0 & 1 & 1 & - & 1 & 1 & 1 & - \\ 1 & 0 & 1 & 1 & - & 1 & 1 & 1 \end{matrix}$$

Codes—Example

- $\mathcal{A} = \{-, 0, 1\}$, where $-$ represents -1.

$$\begin{matrix} 1 & 1 & 1 & - & 0 & - & - & 1 \\ - & 1 & 1 & 1 & - & 0 & - & - \\ 1 & - & 1 & 1 & 1 & - & 0 & - \\ 1 & 1 & - & 1 & 1 & 1 & - & 0 \\ 0 & 1 & 1 & - & 1 & 1 & 1 & - \\ 1 & 0 & 1 & 1 & - & 1 & 1 & 1 \\ - & 1 & 0 & 1 & 1 & - & 1 & 1 \end{matrix}$$

Codes—Example

- $\mathcal{A} = \{-, 0, 1\}$, where $-$ represents -1.

$$
\begin{array}{cccccccc}
1 & 1 & 1 & - & 0 & - & - & 1 \\
- & 1 & 1 & 1 & - & 0 & - & - \\
1 & - & 1 & 1 & 1 & - & 0 & - \\
1 & 1 & - & 1 & 1 & 1 & - & 0 \\
0 & 1 & 1 & - & 1 & 1 & 1 & - \\
1 & 0 & 1 & 1 & - & 1 & 1 & 1 \\
- & 1 & 0 & 1 & 1 & - & 1 & 1 \\
- & - & 1 & 0 & 1 & 1 & - & 1
\end{array}
$$

Codes—Example

- $\mathcal{A} = \{-, 0, 1\}$, where $-$ represents -1.

$$
\begin{array}{cccccccc}
1 & 1 & 1 & - & 0 & - & - & 1 \\
- & 1 & 1 & 1 & - & 0 & - & - \\
1 & - & 1 & 1 & 1 & - & 0 & - \\
1 & 1 & - & 1 & 1 & 1 & - & 0 \\
0 & 1 & 1 & - & 1 & 1 & 1 & - \\
1 & 0 & 1 & 1 & - & 1 & 1 & 1 \\
- & 1 & 0 & 1 & 1 & - & 1 & 1 \\
- & - & 1 & 0 & 1 & 1 & - & 1 \\
- & - & - & 1 & 0 & 1 & 1 & - \\
1 & - & - & - & 1 & 0 & 1 & 1 \\
- & 1 & - & - & - & 1 & 0 & 1 \\
- & - & 1 & - & - & - & 1 & 0 \\
0 & - & - & 1 & - & - & - & 1 \\
- & 0 & - & - & 1 & - & - & - \\
1 & - & 0 & - & - & 1 & - & - \\
1 & 1 & - & 0 & - & - & 1 & -
\end{array}
$$

Codes—Example cont.

- $n = 8$, $a = 3$, $d = 5$, $w = 7$.
- Extremal case of (1).
- Consequence of the following result due to Östergård, Svanström [2].

Theorem

If p is an odd prime,

$$\mathrm{A}_3(p^m + 1, (p^m + 3)/2, p^m) = 2p^m + 2, \tag{2}$$

for $m \geqq 1$.

(Balanced) Weighing Matrices—Definition

- $(-1, 0, 1)$-matrix W of order v such that $WW^t = kI_v$, for some k.
- k is the weight of the matrix.
- Denoted $\mathrm{W}(v, k)$.
- The $\mathrm{W}(v, v)$ are the Hadamard matrices, and $\mathrm{W}(v, v-1)$ are the conference matrices.
- If $W * W$ is an SBIBD, then W is balanced.
- Every conference matrix is balanced.

Weighing Matrices—Example

- The first seven codewords of the previous example form a $\mathrm{W}(8,7)$.

$$W = \begin{bmatrix} 1 & 1 & 1 & - & 0 & - & - & 1 \\ - & 1 & 1 & 1 & - & 0 & - & - \\ 1 & - & 1 & 1 & 1 & - & 0 & - \\ 1 & 1 & - & 1 & 1 & 1 & - & 0 \\ 0 & 1 & 1 & - & 1 & 1 & 1 & - \\ 1 & 0 & 1 & 1 & - & 1 & 1 & 1 \\ - & 1 & 0 & 1 & 1 & - & 1 & 1 \\ - & - & 1 & 0 & 1 & 1 & - & 1 \end{bmatrix}$$

BGWs—Definition

- G a finite group.
- $W = [w_{ij}]$ a $(0, G)$-matrix of order v with k nonzero entries in every row such that the multisets

$$\{w_{i\ell} w_{j\ell}^{-1} : w_{i\ell} \neq 0 \neq w_{j\ell}, 0 \leqq \ell < v\}, \qquad i \neq j,$$

  contains each group element $\lambda/|G|$ times, for some λ.
- W is a balanced generalized weighing matrix.
- Denoted as $\mathrm{BGW}(v, k, \lambda; G)$.

BGWs—Classical Parameters

- q a prime power, $d > 1$.
- Take $K = \mathrm{GF}(q)$, $F = \mathrm{GF}(q^d)$.
- Relative trace $\mathrm{Tr}_{F/K} : F \to K$ defined as

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{d-1}}, \qquad \alpha \in F$$

BGWs—Classical Parameters cont.

- α a primitive element of F.
- $m = \frac{q^d-1}{q-1}$.
- Define $\omega = \alpha^{-m}$.
- Form the m dimensional vector

$$u = (\mathrm{Tr}_{F/K}(\alpha^0), \ldots, \mathrm{Tr}_{F/K}(\alpha^{m-1})).$$

- Form the matrix W over K of order m by taking u together with its first $m-1$ ω-shifts.
- Jungnickel, Tonchev [1] showed that W is BGW with parameters

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

with respect to K^*.

BGWs—Example

- Take $K = \mathrm{GF}(7)$ and $d = 2$. Then $m = 8$.

BGWs—Example

- Take $K = \mathrm{GF}(7)$ and $d = 2$. Then $m = 8$.

$$\omega^4 \quad 1 \quad \omega^4 \quad \omega^3 \quad 0 \quad \omega^5 \quad \omega^5 \quad 1$$

BGWs—Example

- Take $K = \mathrm{GF}(7)$ and $d = 2$. Then $m = 8$.

$$\begin{array}{cccccccc} \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 & 1 \\ \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 \end{array}$$

BGWs—Example

- Take $K = \mathrm{GF}(7)$ and $d = 2$. Then $m = 8$.

$$\begin{matrix} \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 & 1 \\ \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 \\ 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 \end{matrix}$$

DRAFT

BGWs—Example

- Take $K = \mathrm{GF}(7)$ and $d = 2$. Then $m = 8$.

$$\begin{matrix}
\omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 & 1 \\
\omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 \\
1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 \\
1 & 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0
\end{matrix}$$

BGWs—Example

- Take $K = \mathrm{GF}(7)$ and $d = 2$. Then $m = 8$.

$$\begin{array}{cccccccc}
\omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 & 1 \\
\omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 \\
1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 \\
1 & 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 \\
0 & 1 & 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3
\end{array}$$

BGWs—Example

- Take $K = \mathrm{GF}(7)$ and $d = 2$. Then $m = 8$.

$$
\begin{matrix}
\omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 & 1 \\
\omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 \\
1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 \\
1 & 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 \\
0 & 1 & 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 \\
\omega^4 & 0 & 1 & 1 & \omega & \omega^4 & 1 & \omega^4
\end{matrix}
$$

BGWs—Example

- Take $K = \mathrm{GF}(7)$ and $d = 2$. Then $m = 8$.

$$
\begin{array}{cccccccc}
\omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 & 1 \\
\omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 \\
1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 \\
1 & 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 \\
0 & 1 & 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 \\
\omega^4 & 0 & 1 & 1 & \omega & \omega^4 & 1 & \omega^4 \\
\omega^5 & \omega^4 & 0 & 1 & 1 & \omega & \omega^4 & 1
\end{array}
$$

BGWs—Example

- Take $K = \mathrm{GF}(7)$ and $d = 2$. Then $m = 8$.

$$
\begin{matrix}
\omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 & 1 \\
\omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 \\
1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 \\
1 & 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 \\
0 & 1 & 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 \\
\omega^4 & 0 & 1 & 1 & \omega & \omega^4 & 1 & \omega^4 \\
\omega^5 & \omega^4 & 0 & 1 & 1 & \omega & \omega^4 & 1 \\
\omega & \omega^5 & \omega^4 & 0 & 1 & 1 & \omega & \omega^4
\end{matrix}
$$

- A $\mathrm{BGW}(8, 7, 6; \mathrm{GF}(7)^*)$.

Codes from BGWs—Example

$$
\left(\begin{array}{cccccccc|cccccccc|cccccccc}
\omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 & 1 & \omega^5 & \omega & \omega^5 & \omega^4 & 0 & 1 & 1 & \omega & 1 & \omega^2 & 1 & \omega^5 & 0 & \omega & \omega & \omega^2 \\
\omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 & \omega^2 & \omega^5 & \omega & \omega^5 & \omega^4 & 0 & 1 & 1 & \omega^3 & 1 & \omega^2 & 1 & \omega^5 & 0 & \omega & \omega \\
1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega & \omega^2 & \omega^5 & \omega & \omega^5 & \omega^4 & 0 & 1 & \omega^2 & \omega^3 & 1 & \omega^2 & 1 & \omega^5 & 0 & \omega \\
1 & 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega & \omega & \omega^2 & \omega^5 & \omega & \omega^5 & \omega^4 & 0 & \omega^2 & \omega^2 & \omega^3 & 1 & \omega^2 & 1 & \omega^5 & 0 \\
0 & 1 & 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^3 & 0 & \omega & \omega & \omega^2 & \omega^5 & \omega & \omega^5 & \omega^4 & 0 & \omega^2 & \omega^2 & \omega^3 & 1 & \omega^2 & 1 & \omega^5 \\
\omega^4 & 0 & 1 & 1 & \omega & \omega^4 & 1 & \omega^4 & \omega^5 & 0 & \omega & \omega & \omega^2 & \omega^5 & \omega & \omega^5 & 1 & 0 & \omega^2 & \omega^2 & \omega^3 & 1 & \omega^2 & 1 \\
\omega^5 & \omega^4 & 0 & 1 & 1 & \omega & \omega^4 & 1 & 1 & \omega^5 & 0 & \omega & \omega & \omega^2 & \omega^5 & \omega & \omega & 1 & 0 & \omega^2 & \omega^2 & \omega^3 & 1 & \omega^2 \\
\omega & \omega^5 & \omega^4 & 0 & 1 & 1 & \omega & \omega^4 & \omega^2 & 1 & \omega^5 & 0 & \omega & \omega & \omega^2 & \omega^5 & \omega^3 & \omega & 1 & 0 & \omega^2 & \omega^2 & \omega^3 & 1 \\
\hline
\omega & \omega^3 & \omega & 1 & 0 & \omega^2 & \omega^2 & \omega^3 & \omega^2 & \omega^4 & \omega^2 & \omega & 0 & \omega^3 & \omega^3 & \omega^4 & \omega^3 & \omega^5 & \omega^3 & \omega^2 & 0 & \omega^4 & \omega^4 & \omega^5 \\
\omega^4 & \omega & \omega^3 & \omega & 1 & 0 & \omega^2 & \omega^2 & \omega^5 & \omega^2 & \omega^4 & \omega^2 & \omega & 0 & \omega^3 & \omega^3 & 1 & \omega^3 & \omega^5 & \omega^3 & \omega^2 & 0 & \omega^4 & \omega^4 \\
\omega^3 & \omega^4 & \omega & \omega^3 & \omega & 1 & 0 & \omega^2 & \omega^4 & \omega^5 & \omega^2 & \omega^4 & \omega^2 & \omega & 0 & \omega^3 & \omega^5 & 1 & \omega^3 & \omega^5 & \omega^3 & \omega^2 & 0 & \omega^4 \\
\omega^3 & \omega^3 & \omega^4 & \omega & \omega^3 & \omega & 1 & 0 & \omega^4 & \omega^4 & \omega^5 & \omega^2 & \omega^4 & \omega^2 & \omega & 0 & \omega^5 & \omega^5 & 1 & \omega^3 & \omega^5 & \omega^3 & \omega^2 & 0 \\
0 & \omega^3 & \omega^3 & \omega^4 & \omega & \omega^3 & \omega & 1 & 0 & \omega^4 & \omega^4 & \omega^5 & \omega^2 & \omega^4 & \omega^2 & \omega & 0 & \omega^5 & \omega^5 & 1 & \omega^3 & \omega^5 & \omega^3 & \omega^2 \\
\omega & 0 & \omega^3 & \omega^3 & \omega^4 & \omega & \omega^3 & \omega & \omega^2 & 0 & \omega^4 & \omega^4 & \omega^5 & \omega^2 & \omega^4 & \omega^2 & \omega^3 & 0 & \omega^5 & \omega^5 & 1 & \omega^3 & \omega^5 & \omega^3 \\
\omega^2 & \omega & 0 & \omega^3 & \omega^3 & \omega^4 & \omega & \omega^3 & \omega^3 & \omega^2 & 0 & \omega^4 & \omega^4 & \omega^5 & \omega^2 & \omega^4 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 & 1 & \omega^3 & \omega^5 \\
\omega^4 & \omega^2 & \omega & 0 & \omega^3 & \omega^3 & \omega^4 & \omega & \omega^5 & \omega^3 & \omega^2 & 0 & \omega^4 & \omega^4 & \omega^5 & \omega^2 & 1 & \omega^4 & \omega^3 & 0 & \omega^5 & \omega^5 & 1 & \omega^3
\end{array}\right)
$$

Codes from BGWs—Example cont.

- $n = 8, w = 7, d = 7$, and $a = 7$.
- Equality in (1).
- $\mathrm{A}_7(8, 7, 7) = 48$.

Main Result

Theorem

If q is a prime power, and if $d > 1$, then

$$\mathrm{A}_q\left(\frac{q^d-1}{q-1}, q^{d-1}, q^{d-1}\right) = q^d - 1.$$

Moreover, the code can be assumed to be completely generated by a single codeword and equidistant.

- If q odd, taking $d = 2$ implies (2) as a corollary.

Thank You!!!

References

Dieter Jungnickel and Vladimir D. Tonchev.
Perfect codes and balanced generalized weighing matrices. II.
Finite Fields Appl., 8(2):155–165, 2002.

Patric R. J. Östergård and Mattias Svanström.
Ternary constant weight codes.
Electron. J. Combin., 9(1):Research Paper 41, 23, 2002.