

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

- Constant weight error-correcting codes.
- Balanced generalized weighing matrices (BGW s).
- Use BGW s to construct optimal constant weight codes.

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- \mathcal{A} has 0.
- Does not assume that \mathcal{A} is endowed with an arithmetic.
- Usually take $\mathcal{A} = GF(q)$.

- Take $\mathcal{A} = GF(5) = \{0, 1, \omega, \omega^2, \omega^3\}$, where ω is some primitive element.

- Take $\mathcal{A} = GF(5) = \{0, 1, \omega, \omega^2, \omega^3\}$, where ω is some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- Take $\mathcal{A} = GF(5) = \{0, 1, \omega, \omega^2, \omega^3\}$, where ω is some primitive element.

$$\underbrace{\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}}_6$$

- Length 6 ($n = 6$).

- Take $\mathcal{A} = GF(5) = \{0, 1, \omega, \omega^2, \omega^3\}$, where ω is some primitive element.

$$2 \left\{ \begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array} \right.$$

- Number of codewords is 2 ($M = 2$).

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$, where ω is some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$, where ω is some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$, where ω is some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- **Constant weight 5.** ($w = 5$)

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$ and ω some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$ and ω some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$ and ω some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$ and ω some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$ and ω some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$ and ω some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$ and ω some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- The codewords are at Hamming distance 5.

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$ and ω some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- The codewords are at Hamming distance 5.
- $d = \min_{\substack{c, c' \in \mathcal{C} \\ c \neq c'}} d(c, c')$.

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$ and ω some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- The codewords are at Hamming distance 5.
- $d = \min_{\substack{c, c' \in \mathcal{C} \\ c \neq c'}} d(c, c')$.
- $d = 5$.

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$ and ω some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- Write $(6, 5, 5)_5$ -code.

- A finite collection of “strings” (say \mathcal{C}) of given length over a given finite alphabet (say \mathcal{A}).
- Take $\mathcal{A} = GF(5)$ and ω some primitive element.

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

- Write $(6, 5, 5)_5$ -code.
- More generally, $(n, d, w)_q$ -code.

- Fundamental Question:

Max M
Given n, w, d, q .

denoted $A_q(n, d, w)$.

- Fundamental Question:

Max M
Given n, w, d, q .

denoted $A_q(n, d, w)$.

Restricted Johnson Bound

$$A_q(n, d, w) \leq \left\lfloor \frac{nd(q-1)}{qw^2 - 2(q-1)nw + nd(q-1)} \right\rfloor, \quad (1)$$

if $qw^2 - 2(q-1)nw + nd(q-1) > 0$.

Optimal Code

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

Optimal Code

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

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ & \omega^3 & & & & \end{array}$$

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ & \omega^3 & 1 & & & \end{array}$$

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ & \omega^3 & 1 & \omega^3 & & \end{array}$$

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ & \omega^3 & 1 & \omega^3 & 0 & \end{array}$$

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

Optimal Code

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \end{array}$$

Optimal Code

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \\ \omega & \omega & \omega^3 & 1 & \omega^3 & 0 \end{array}$$

Optimal Code

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \\ \omega & \omega & \omega^3 & 1 & \omega^3 & 0 \\ 0 & \omega & \omega & \omega^3 & 1 & \omega^3 \end{array}$$

Optimal Code

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \\ \omega & \omega & \omega^3 & 1 & \omega^3 & 0 \\ 0 & \omega & \omega & \omega^3 & 1 & \omega^3 \\ 1 & 0 & \omega & \omega & \omega^3 & 1 \end{array}$$

Optimal Code

ω^3	1	ω^3	0	1	1
ω	ω^3	1	ω^3	0	1
ω	ω	ω^3	1	ω^3	0
0	ω	ω	ω^3	1	ω^3
1	0	ω	ω	ω^3	1
ω	1	0	ω	ω	ω^3

Optimal Code

ω^3	1	ω^3	0	1	1
ω	ω^3	1	ω^3	0	1
ω	ω	ω^3	1	ω^3	0
0	ω	ω	ω^3	1	ω^3
1	0	ω	ω	ω^3	1
ω	1	0	ω	ω	ω^3
<hr/>					
1	ω	1	0	ω	ω
ω^2	1	ω	1	0	ω
ω^2	ω^2	1	ω	1	0
0	ω^2	ω^2	1	ω	1
ω	0	ω^2	ω^2	1	ω
ω^2	ω	0	ω^2	ω^2	1

Optimal Code

ω^3	1	ω^3	0	1	1	ω	ω^2	ω	0	ω^2	ω^2
ω	ω^3	1	ω^3	0	1	ω^3	ω	ω^2	ω	0	ω^2
ω	ω	ω^3	1	ω^3	0	ω^3	ω^3	ω	ω^2	ω	0
0	ω	ω	ω^3	1	ω^3	0	ω^3	ω^3	ω	ω^2	ω
1	0	ω	ω	ω^3	1	ω^2	0	ω^3	ω^3	ω	ω^2
ω	1	0	ω	ω	ω^3	ω^3	ω^2	0	ω^3	ω^3	ω
1	ω	1	0	ω	ω						
ω^2	1	ω	1	0	ω						
ω^2	ω^2	1	ω	1	0						
0	ω^2	ω^2	1	ω	1						
ω	0	ω^2	ω^2	1	ω						
ω^2	ω	0	ω^2	ω^2	1						

Optimal Code

ω^3	1	ω^3	0	1	1	ω	ω^2	ω	0	ω^2	ω^2
ω	ω^3	1	ω^3	0	1	ω^3	ω	ω^2	ω	0	ω^2
ω	ω	ω^3	1	ω^3	0	ω^3	ω^3	ω	ω^2	ω	0
0	ω	ω	ω^3	1	ω^3	0	ω^3	ω^3	ω	ω^2	ω
1	0	ω	ω	ω^3	1	ω^2	0	ω^3	ω^3	ω	ω^2
ω	1	0	ω	ω	ω^3	ω^3	ω^2	0	ω^3	ω^3	ω
1	ω	1	0	ω	ω	ω^2	ω^3	ω^2	0	ω^3	ω^3
ω^2	1	ω	1	0	ω	1	ω^2	ω^3	ω^2	0	ω^3
ω^2	ω^2	1	ω	1	0	1	1	ω^2	ω^3	ω^2	0
0	ω^2	ω^2	1	ω	1	0	1	1	ω^2	ω^3	ω^2
ω	0	ω^2	ω^2	1	ω	ω^3	0	1	1	ω^2	ω^3
ω^2	ω	0	ω^2	ω^2	1	1	ω^3	0	1	1	ω^2

- Parameters: $n = 6, q = 5, d = 5, w = 5, M = 24$.

$$\left\lfloor \frac{nd(q-1)}{qw^2 - 2(q-1)nw + nd(q-1)} \right\rfloor = \left\lfloor \frac{6 \cdot 5 \cdot 4}{5^3 - 2 \cdot 4 \cdot 6 \cdot 5 + 6 \cdot 5 \cdot 4} \right\rfloor = 24$$

- The code is optimal.
- $A_5(6, 5, 5) = 24$.

- G some finite group.
- $W = [w_{ij}]$ a $(0, G)$ -matrix of order v .
- k non-zero entries in every row.
- The multisets

$$\{w_{ih}w_{jh}^{-1} : w_{ih} \neq 0 \neq w_{jh}, 0 \leq h < v\}, \text{ for } i \neq j.$$

contain each group element a constant $\lambda/|G|$ times.

- W is a balanced generalized weighing matrix.
- Write $BGW(v, k, \lambda; G)$.

ω^3	1	ω^3	0	1	1	ω	ω^2	ω	0	ω^2	ω^2
ω	ω^3	1	ω^3	0	1	ω^3	ω	ω^2	ω	0	ω^2
ω	ω	ω^3	1	ω^3	0	ω^3	ω^3	ω	ω^2	ω	0
0	ω	ω	ω^3	1	ω^3	0	ω^3	ω^3	ω	ω^2	ω
1	0	ω	ω	ω^3	1	ω^2	0	ω^3	ω^3	ω	ω^2
ω	1	0	ω	ω	ω^3	ω^3	ω^2	0	ω^3	ω^3	ω
1	ω	1	0	ω	ω	ω^2	ω^3	ω^2	0	ω^3	ω^3
ω^2	1	ω	1	0	ω	1	ω^2	ω^3	ω^2	0	ω^3
ω^2	ω^2	1	ω	1	0	1	1	ω^2	ω^3	ω^2	0
0	ω^2	ω^2	1	ω	1	0	1	1	ω^2	ω^3	ω^2
ω	0	ω^2	ω^2	1	ω	ω^3	0	1	1	ω^2	ω^3
ω^2	ω	0	ω^2	ω^2	1	1	ω^3	0	1	1	ω^2

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega & \omega^3 & 1 & \omega^3 & 0 \end{array}$$

$$\begin{array}{cccccc}
 \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\
 \omega & \omega & \omega^3 & 1 & \omega^3 & 0
 \end{array}$$

$$\begin{array}{cccccc} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega^{-1} & \omega^{-1} & \omega^{-3} & 1 & \omega^{-3} & 0 \end{array}$$

$$\begin{array}{cccccc}
 \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\
 \omega^{-1} & \omega^{-1} & \omega^{-3} & 1 & \omega^{-3} & 0 \\
 \hline
 \omega^2 & \omega^3 & 1 & & \omega &
 \end{array}$$

$$\begin{array}{cccccc}
 \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\
 \omega^{-1} & \omega^{-1} & \omega^{-3} & 1 & \omega^{-3} & 0 \\
 \hline
 \{\omega^2, & \omega^3, & 1, & & \omega\}
 \end{array}$$

Trace Construction

- q a prime power, $m > 1$.
- $K = GF(q)$, $F = GF(q^m)$.
- Relative trace $F \rightarrow K$:

$$\text{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}, \quad \alpha \in F.$$

- $\beta \in F$ a primitive element.
- $\omega = \beta^{-\ell}$, where $\ell = \frac{q^m - 1}{q - 1}$.

- Construct the ℓ -dimensional vector

$$u = (\mathrm{Tr}_{F/K}(\beta^0), \mathrm{Tr}_{F/K}(\beta^1), \dots, \mathrm{Tr}_{F/K}(\beta^{\ell-1})).$$

- Take u as the first row of W .
- Remaining rows are the first $\ell - 1$ ω -shifts of u .
- Jungnickel and Tonchev (2002) showed that these structures are

$$BGW \left(\frac{q^m - 1}{q - 1}, q^{m-1}, q^{m-1} - q^{m-2}; GF(q)^* \right) s.$$

Codes From BGWs

- If W is a classical parameter BGW over $GF(q)^*$, then the rows of $W, \omega W, \dots, \omega^{q-2}W$, form an optimal, constant weight code.
- Can be assumed to be generated by single codeword.
- Parameters:

$$n = \frac{q^m - 1}{q - 1}, d = q^{m-1}, w = q^{m-1}, M = q^m - 1.$$

Theorem

$$A_q \left(\frac{q^m - 1}{q - 1}, q^{m-1}, q^{m-1} \right) = q^m - 1,$$

$$\begin{bmatrix} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \\ \omega & \omega & \omega^3 & 1 & \omega^3 & 0 \\ 0 & \omega & \omega & \omega^3 & 1 & \omega^3 \\ 1 & 0 & \omega & \omega & \omega^3 & 1 \\ \omega & 1 & 0 & \omega & \omega & \omega^3 \end{bmatrix}$$

- A $BGW(6, 5, 4; GF(5)^*)$.

Projections

$$\begin{bmatrix} \omega^3 & 1 & \omega^3 & 0 & 1 & 1 \\ \omega & \omega^3 & 1 & \omega^3 & 0 & 1 \\ \omega & \omega & \omega^3 & 1 & \omega^3 & 0 \\ 0 & \omega & \omega & \omega^3 & 1 & \omega^3 \\ 1 & 0 & \omega & \omega & \omega^3 & 1 \\ \omega & 1 & 0 & \omega & \omega & \omega^3 \end{bmatrix}$$

- A $BGW(6, 5, 4; GF(5)^*)$.
- Apply $\omega \mapsto -1$.

Projections

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

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

- A $BGW(6, 5, 4; \{-1, 1\})$.

- If q is odd, then apply $\omega \mapsto -1$.
- The result is a *BGW* over $\{-1, 1\}$.
- The matrix and its negative form an optimal ternary code.

Theorem

$$A_3 \left(\frac{q^m - 1}{q - 1}, q^{m-2} \left(\frac{q + 3}{2} \right), q^{m-1} \right) = 2 \left(\frac{q^m - 1}{q - 1} \right),$$

for q odd.

- Östergård and Svanström (2002) considered the case $m = 2$.

- Our optimal constant weight $(6, 5, 5)_5$ -code becomes...

-1	1	-1	0	1	1
-1	-1	1	-1	0	1
-1	-1	-1	1	-1	0
0	-1	-1	-1	1	-1
1	0	-1	-1	-1	1
-1	1	0	-1	-1	-1
<hr/>					
1	-1	1	0	-1	-1
1	1	-1	1	0	-1
1	1	1	-1	1	0
0	1	1	1	-1	1
-1	0	1	1	1	-1
1	-1	0	1	1	1

... an optimal constant weight $(6, 3, 5)_3$ -code.

The End!!
Thank You!

- Jungnickel, D. and Tonchev, V. D. (2002). Perfect codes and balanced generalized weighing matrices. II. *Finite Fields Appl.*, 8(2):155–165.
- Östergård, P. R. J. and Svanström, M. (2002). Ternary constant weight codes. *Electron. J. Combin.*, 9(1):Research Paper 41, 23.

Unrestricted Johnson Bound

- ① If $2w < d$, then $A_q(n, d, w) = 1$; and
- ② if $2w \geq d$ and $d \in \{2e - 1, 2e\}$, then

$$A_q(n, d, w) \leq \left\lfloor \frac{n(q-1)}{w} \right\rfloor \left\lfloor \frac{(n-1)(q-1)}{w-1} \right\rfloor \dots \left\lfloor \frac{(n-w+e)(q-1)}{e} \right\rfloor \dots \right\rfloor$$