Alberta-Montana Combinatorics and Algorithms Days at BIRS

A class of optimal constant weight ternary codes

Vlad Zaitsev

University of Lethbridge

Joint work with Hadi Kharaghani and Sho Suda

June 4, 2022

An overview of codes

An overview of codes

- Let $S_q = \{0, 1, \cdots, q-1\}$.

An overview of codes

- Let $S_q = \{0, 1, \cdots, q-1\}$.
- A *q-ary* code of length n is any subset C of S_q^n, where elements of C are called *codewords*.

An overview of codes

- Let $S_q = \{0, 1, \cdots, q-1\}$.
- A *q-ary* code of length n is any subset C of S_q^n, where elements of C are called *codewords*.
- M denotes the number of codewords in C.

An overview of codes

- Let $S_q = \{0, 1, \cdots, q-1\}$.
- A *q-ary* code of length n is any subset C of S_q^n, where elements of C are called *codewords*.
- M denotes the number of codewords in C.
- If all codewords have the same number of nonzero entires (denoted w) the code is said to be of *constant weight*.

An overview of codes

- Let $S_q = \{0, 1, \cdots, q-1\}$.
- A *q-ary* code of length n is any subset C of S_q^n, where elements of C are called *codewords*.
- M denotes the number of codewords in C.
- If all codewords have the same number of nonzero entires (denoted w) the code is said to be of *constant weight*.
- The *Hamming distance* between two q-ary codes of length n is the number of coordinates in which they differ.

An overview of codes

- Let $S_q = \{0, 1, \cdots, q-1\}$.
- A *q-ary* code of length n is any subset C of S_q^n, where elements of C are called *codewords*.
- M denotes the number of codewords in C.
- If all codewords have the same number of nonzero entires (denoted w) the code is said to be of *constant weight*.
- The *Hamming distance* between two q-ary codes of length n is the number of coordinates in which they differ.
- A constant weight q-ary code of length n, having minimum Hamming distance d and weight w is denoted as an $(n, d, w)_q$-code.

An example

- As an example, take $S = \{0, -1, 1\}$.

An example

- As an example, take $S = \{0, -1, 1\}$.

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

An example

- As an example, take $S = \{0, -1, 1\}$.

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

- The number of codewords is 2 ($M = 2$).

An example

- As an example, take $S = \{0, -1, 1\}$.

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

- The number of codewords is 2 ($M = 2$).
- The above code has length 5 ($n = 5$).

An example

- As an example, take $S = \{0, -1, 1\}$.

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

- The number of codewords is 2 ($M = 2$).
- The above code has length 5 ($n = 5$).
- The Hamming distance between the codewords is 4 ($d = 4$).

An example

- As an example, take $S = \{0, -1, 1\}$.

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

- The number of codewords is 2 ($M = 2$).
- The above code has length 5 ($n = 5$).
- The Hamming distance between the codewords is 4 ($d = 4$).
- The code has constant weight 4 ($w = 4$).

An example

- As an example, take $S = \{0, -1, 1\}$.

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

- The number of codewords is 2 ($M = 2$).
- The above code has length 5 ($n = 5$).
- The Hamming distance between the codewords is 4 ($d = 4$).
- The code has constant weight 4 ($w = 4$).
- We denote this as a $(5, 4, 4)_3$-code.

An example

- As an example, take $S = \{0, -1, 1\}$.

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

- The number of codewords is 2 ($M = 2$).
- The above code has length 5 ($n = 5$).
- The Hamming distance between the codewords is 4 ($d = 4$).
- The code has constant weight 4 ($w = 4$).
- We denote this as a $(5, 4, 4)_3$-code.
- How many codewords can we have with $n = 5$, $d = 4$, $w = 4$ (Maximize M)?

Upper bounds for M

Upper bounds for M

- The largest value of M for which there is a q-ary code of length n, minimum distance d and constant weight w is denoted by $A_q(n, d, w)$ and the code is said to be *optimal* if $M = A_q(n, d, w)$.

Upper bounds for M

- The largest value of M for which there is a q-ary code of length n, minimum distance d and constant weight w is denoted by $A_q(n, d, w)$ and the code is said to be *optimal* if $M = A_q(n, d, w)$.

The Johnson bounds for the constant weight q-ary codes:

Upper bounds for M

- The largest value of M for which there is a q-ary code of length n, minimum distance d and constant weight w is denoted by $A_q(n,d,w)$ and the code is said to be *optimal* if $M = A_q(n,d,w)$.

The Johnson bounds for the constant weight q-ary codes:

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

$$A_q(n,d,w) \leq \left\lfloor \frac{nd(q-1)}{qw^2 - 2(q-1)nw + nd(q-1)} \right\rfloor, a = qw^2 - 2(q-1)nw + nd(q-1) > 0. \tag{2}$$

Upper bounds for M

- The largest value of M for which there is a q-ary code of length n, minimum distance d and constant weight w is denoted by $A_q(n, d, w)$ and the code is said to be *optimal* if $M = A_q(n, d, w)$.

The Johnson bounds for the constant weight q-ary codes:

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

$$A_q(n, d, w) \leq \left\lfloor \frac{nd(q-1)}{qw^2 - 2(q-1)nw + nd(q-1)} \right\rfloor, a = qw^2 - 2(q-1)nw + nd(q-1) > 0. \quad (2)$$

- For $q = 3$, $n = 5$, $d = 4$ and $w = 4$ we have $a = 3(4)^2 - 2(2)(5)(4) + 2(5)(4) = 8 > 0$. Since the condition is met, we can use bound (2) to compute $A_3(5, 4, 4) \leq \lfloor \frac{2nd}{3w^2 - 4nw + 2nd} \rfloor = \frac{40}{8} = 5$.

Weighing matrices

Weighing matrices

Definition

A weighing matrix, W, is a matrix of order n and weight w with entries from $\{0, -1, 1\}$, such that $WW^T = wI_n$. Often denoted by $W(n, w)$.

Weighing matrices

Definition

A weighing matrix, W, is a matrix of order n and weight w with entries from $\{0, -1, 1\}$, such that $WW^T = wI_n$. Often denoted by $W(n, w)$.

Example

A weighing matrix of order 6 and weight 5: a $W(6, 5)$

Weighing matrices

Definition

A weighing matrix, W, is a matrix of order n and weight w with entries from $\{0, -1, 1\}$, such that $WW^T = wI_n$. Often denoted by $W(n, w)$.

Example

A weighing matrix of order 6 and weight 5: a $W(6, 5)$

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

Weighing matrices

Definition

A weighing matrix, W, is a matrix of order n and weight w with entries from $\{0, -1, 1\}$, such that $WW^T = wI_n$. Often denoted by $W(n, w)$.

Example

A weighing matrix of order 6 and weight 5: a $W(6, 5)$

$$W = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{bmatrix}, WW^T = \begin{bmatrix} 5&0&0&0&0&0 \\ 0&5&0&0&0&0 \\ 0&0&5&0&0&0 \\ 0&0&0&5&0&0 \\ 0&0&0&0&5&0 \\ 0&0&0&0&0&5 \end{bmatrix}$$

Codes from weighing matrices

Codes from weighing matrices

Using the rows of any weighing matrix we can form an optimal constant weight ternary code.

Codes from weighing matrices

Using the rows of any weighing matrix we can form an optimal constant weight ternary code. Consider the rows of $W(6,5)$:

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

Codes from weighing matrices

Using the rows of any weighing matrix we can form an optimal constant weight ternary code. Consider the rows of $W(6,5)$:

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

There are six codewords of length $n = 6$, distance $d = 4$ and weight $w = 5$.

Codes from weighing matrices

Using the rows of any weighing matrix we can form an optimal constant weight ternary code. Consider the rows of $W(6,5)$:

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

There are six codewords of length $n = 6$, distance $d = 4$ and weight $w = 5$. Calculating the condition for Johnson Bound (2) $a = 3(5^2) - 4(6)(5) + 2(6)(4) = 3 > 0$

Codes from weighing matrices

Using the rows of any weighing matrix we can form an optimal constant weight ternary code. Consider the rows of $W(6,5)$:

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

There are six codewords of length $n = 6$, distance $d = 4$ and weight $w = 5$. Calculating the condition for Johnson Bound (2) $a = 3(5^2) - 4(6)(5) + 2(6)(4) = 3 > 0$. Using Johnson bound (2) the upper bound is

$$A_3(6,4,5) = \left\lfloor \frac{nd(q-1)}{qw^2 - 2(q-1)nw + nd(q-1)} \right\rfloor = \frac{48}{3} = 16$$

Codes from weighing matrices

Using the rows of any weighing matrix we can form an optimal constant weight ternary code. Consider the rows of $W(6,5)$:

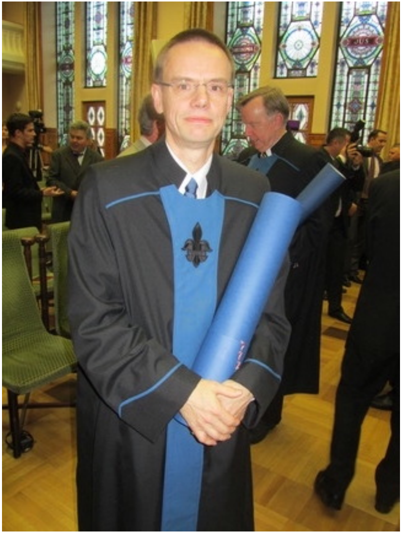
$$\begin{matrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{matrix}$$

There are six codewords of length $n = 6$, distance $d = 4$ and weight $w = 5$. Calculating the condition for Johnson Bound (2) $a = 3(5^2) - 4(6)(5) + 2(6)(4) = 3 > 0$. Using Johnson bound (2) the upper bound is

$$A_3(6,4,5) = \left\lfloor \frac{nd(q-1)}{qw^2 - 2(q-1)nw + nd(q-1)} \right\rfloor = \frac{48}{3} = 16$$

There are only 6 codewords and it is hard to find 10 more.

A 2002 Electronic Journal of Combinatorics result of



Patric *Östergård*

$\ddot{O}sterg\dot{a}rd's$ result

Showed that an optimal constant weight ternary code having length $n = 6$, distance $d = 4$ and constant weight $w = 5$ consists of 12 codewords:

Östergård's result

Showed that an optimal constant weight ternary code having length $n = 6$, distance $d = 4$ and constant weight $w = 5$ consists of 12 codewords:

Theorem (E.J.C. 2002)

If $p \geq 3$ is a prime power and $m \geq 1$, then

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

Östergȧrd's result

Showed that an optimal constant weight ternary code having length $n = 6$, distance $d = 4$ and constant weight $w = 5$ consists of 12 codewords:

Theorem (E.J.C. 2002)

If $p \geq 3$ is a prime power and $m \geq 1$, then

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

Let $p = 5$, $m = 1$, then $A_3(6, 4, 5) = 12$.

An extension of *Östergård*'s result

We begin by looking at the Derived part of W:

We begin by looking at the Derived part of W:

$$W = \left[\begin{array}{c|cccccc} 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{array}\right]$$

Ternary code from the Derived part of W

Ternary code from the Derived part of W

Consider $(5, 4, 4)_3$ code consisting of the rows of the Derived part:

Ternary code from the Derived part of W

Consider $(5, 4, 4)_3$ code consisting of the rows of the Derived part:

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

Ternary code from the Derived part of W

Consider $(5, 4, 4)_3$ code consisting of the rows of the Derived part:

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

Calculating the condition for Johnson bound (2) $a = 3(4)^2 - 4(5)(4) + 2(5)(4) = 8 > 0$. Applying Johnson bound (2) we see that $A_3(5, 4, 4) \leq 5$.

Ternary code from the Derived part of W

Consider $(5,4,4)_3$ code consisting of the rows of the Derived part:

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

Calculating the condition for Johnson bound (2) $a = 3(4)^2 - 4(5)(4) + 2(5)(4) = 8 > 0$. Applying Johnson bound (2) we see that $A_3(5,4,4) \leq 5$. The code is optimal.

Consider $(5,4,4)_3$ code consisting of the rows of the Derived part:

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

Calculating the condition for Johnson bound (2)
$a = 3(4)^2 - 4(5)(4) + 2(5)(4) = 8 > 0$. Applying Johnson bound (2) we see that $A_3(5,4,4) \leq 5$. The code is optimal.
We now use Johnson bound (1):

$$A_3(6,4,5) \leq \left\lfloor \frac{n(q-1)}{w} A_q(n-1,d,w-1) \right\rfloor = \frac{2(6)}{5}(5) = 12$$

and conclude that $A_3(6,4,5) \leq 12$.

Constructing the optimal code

Constructing the optimal code

We add the rows of $-W$ to the rows of W:

Constructing the optimal code

We add the rows of $-W$ to the rows of W:

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

Constructing the optimal code

We add the rows of $-W$ to the rows of W:

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

There we have the desired 12 codewords.

The extension

Theorem

Let C be a conference matrix of order $n+1$ (ie $W(n+1,n)$ with 0 diagonal). Then the rows of C and $-C$ together form an optimal constant weight ternary code and so

$$A_3(n+1, \frac{n+3}{2}, n) = 2(n+1).$$

The extension

Theorem

Let C be a conference matrix of order $n+1$ (ie $W(n+1,n)$ with 0 diagonal). Then the rows of C and $-C$ together form an optimal constant weight ternary code and so

$$A_3(n+1, \frac{n+3}{2}, n) = 2(n+1).$$

The 2002 E.J.C. result follows:

Theorem

Let C be a conference matrix of order $n+1$ (ie $W(n+1,n)$ with 0 diagonal). Then the rows of C and $-C$ together form an optimal constant weight ternary code and so

$$A_3(n+1, \frac{n+3}{2}, n) = 2(n+1).$$

The 2002 E.J.C. result follows:

Corollary

If $p \geq 3$ is a prime power and $m \geq 1$, then

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

Remark: There is a $W(16,15)$ and 15 is a composite number.

The new class of optimal ternary codes

The new class of optimal ternary codes

Next we try to show that for every odd prime power p and positive integer m:

Theorem

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

We begin with the definition and some examples of *Orthogonal Arrays*

Orthogonal Array

Orthogonal Array

Definition

We say an $n^2 \times m$ matrix with entries in a set S of n symbols is an orthogonal array on S, denoted $OA(n, m)$, if superimposition of each row on a different row will show exactly one common symbol in the same column.

Orthogonal Array

Definition

We say an $n^2 \times m$ matrix with entries in a set S of n symbols is an orthogonal array on S, denoted $OA(n, m)$, if superimposition of each row on a different row will show exactly one common symbol in the same column.

Example

Let $n = 3$ and $m = 4$, then

$$O = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 \\ 1 & 3 & 3 & 3 \\ 2 & 1 & 2 & 3 \\ 2 & 3 & 1 & 2 \\ 2 & 2 & 3 & 1 \\ 3 & 1 & 3 & 2 \\ 3 & 2 & 1 & 3 \\ 3 & 3 & 2 & 1 \end{bmatrix}$$

is an $OA(3, 4)$ on $S = \{1, 2, 3\}$.

The orthogonal array O for $n = 5$, $m = 6$

The orthogonal array O for $n = 5$, $m = 6$

$$O = \begin{bmatrix} 1&1&1&1&1&1\\ 1&2&2&2&2&2\\ 1&3&3&3&3&3\\ 1&4&4&4&4&4\\ 1&5&5&5&5&5\\ 2&1&2&3&4&5\\ 2&2&3&4&5&1\\ 2&3&4&5&1&2\\ 2&4&5&1&2&3\\ 2&5&1&2&3&4\\ 3&1&3&5&2&4\\ 3&3&5&2&4&1\\ 3&5&2&4&1&3\\ 3&2&4&1&3&5\\ 3&4&1&3&5&2\\ 4&1&4&2&5&3\\ 4&4&2&5&3&1\\ 4&2&5&3&1&4\\ 4&5&3&1&4&2\\ 4&3&1&4&2&5\\ 5&1&5&4&3&2\\ 5&5&4&3&2&1\\ 5&4&3&2&1&5\\ 5&3&2&1&5&4\\ 5&2&1&5&4&3 \end{bmatrix}$$

The orthogonal array O for $n = 5,\ m = 6$

$$O = \begin{bmatrix} 1&1&1&1&1&1\\ 1&2&2&2&2&2\\ 1&3&3&3&3&3\\ 1&4&4&4&4&4\\ 1&5&5&5&5&5\\ 2&1&2&3&4&5\\ 2&2&3&4&5&1\\ 2&3&4&5&1&2\\ 2&4&5&1&2&3\\ 2&5&1&2&3&4\\ 3&1&3&5&2&4\\ 3&3&5&2&4&1\\ 3&5&2&4&1&3\\ 3&2&4&1&3&5\\ 3&4&1&3&5&2\\ 4&1&4&2&5&3\\ 4&4&2&5&3&1\\ 4&2&5&3&1&4\\ 4&5&3&1&4&2\\ 4&3&1&4&2&5\\ 5&1&5&4&3&2\\ 5&5&4&3&2&1\\ 5&4&3&2&1&5\\ 5&3&2&1&5&4\\ 5&2&1&5&4&3 \end{bmatrix}$$

O is an $OA(5,6)$ on $S = \{1,2,3,4,5\}$.

The orthogonal array O for $n = 5$, $m = 6$

$$O = \begin{bmatrix} 1&1&1&1&1&1 \\ 1&2&2&2&2&2 \\ 1&3&3&3&3&3 \\ 1&4&4&4&4&4 \\ 1&5&5&5&5&5 \\ 2&1&2&3&4&5 \\ 2&2&3&4&5&1 \\ 2&3&4&5&1&2 \\ 2&4&5&1&2&3 \\ 2&5&1&2&3&4 \\ 3&1&3&5&2&4 \\ 3&3&5&2&4&1 \\ 3&5&2&4&1&3 \\ 3&2&4&1&3&5 \\ 3&4&1&3&5&2 \\ 4&1&4&2&5&3 \\ 4&4&2&5&3&1 \\ 4&2&5&3&1&4 \\ 4&5&3&1&4&2 \\ 4&3&1&4&2&5 \\ 5&1&5&4&3&2 \\ 5&5&4&3&2&1 \\ 5&4&3&2&1&5 \\ 5&3&2&1&5&4 \\ 5&2&1&5&4&3 \end{bmatrix}$$

O is an $OA(5,6)$ on $S = \{1,2,3,4,5\}$. The superimposition of any two distinct rows of O will have exactly one common symbol.

The orthogonal array O for $n = 5$, $m = 6$

$$O = \begin{bmatrix} 1&1&1&1&1&1\\ 1&2&2&2&2&2\\ 1&3&3&3&3&3\\ 1&4&4&4&4&4\\ 1&5&5&5&5&5\\ 2&1&2&3&4&5\\ 2&2&3&4&5&1\\ 2&3&4&5&1&2\\ 2&4&5&1&2&3\\ 2&5&1&2&3&4\\ 3&1&3&5&2&4\\ 3&3&5&2&4&1\\ 3&5&2&4&1&3\\ 3&2&4&1&3&5\\ 3&4&1&3&5&2\\ 4&1&4&2&5&3\\ 4&4&2&5&3&1\\ 4&2&5&3&1&4\\ 4&5&3&1&4&2\\ 4&3&1&4&2&5\\ 5&1&5&4&3&2\\ 5&5&4&3&2&1\\ 5&4&3&2&1&5\\ 5&3&2&1&5&4\\ 5&2&1&5&4&3 \end{bmatrix}$$

$$\begin{matrix} 2 & 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 2 & 3 & 4 \end{matrix}$$

O is an $OA(5, 6)$ on $S = \{1, 2, 3, 4, 5\}$. The superimposition of any two distinct rows of O will have exactly one common symbol.

The orthogonal array O for $n = 5$, $m = 6$

$$O = \begin{bmatrix} 1&1&1&1&1&1 \\ 1&2&2&2&2&2 \\ 1&3&3&3&3&3 \\ 1&4&4&4&4&4 \\ 1&5&5&5&5&5 \\ 2&1&2&3&4&5 \\ 2&2&3&4&5&1 \\ 2&3&4&5&1&2 \\ 2&4&5&1&2&3 \\ 2&5&1&2&3&4 \\ 3&1&3&5&2&4 \\ 3&3&5&2&4&1 \\ 3&5&2&4&1&3 \\ 3&2&4&1&3&5 \\ 3&4&1&3&5&2 \\ 4&1&4&2&5&3 \\ 4&4&2&5&3&1 \\ 4&2&5&3&1&4 \\ 4&5&3&1&4&2 \\ 4&3&1&4&2&5 \\ 5&1&5&4&3&2 \\ 5&5&4&3&2&1 \\ 5&4&3&2&1&5 \\ 5&3&2&1&5&4 \\ 5&2&1&5&4&3 \end{bmatrix}$$

3	1	3	5	2	4
5	5	4	3	2	1

O is an $OA(5, 6)$ on $S = \{1, 2, 3, 4, 5\}$. The superimposition of any two distinct rows of O will have exactly one common symbol.

Overview of BGWs

Overview of BGWs

- Let G be some multiplicative group.

Overview of BGWs

- Let G be some multiplicative group.
- A $BGW(v, k, \lambda)$ over G is a matrix $W = [w_{ij}]$ of order v with entries from $\{G \cup 0\}$.

Overview of BGWs

- Let G be some multiplicative group.
- A $BGW(v, k, \lambda)$ over G is a matrix $W = [w_{ij}]$ of order v with entries from $\{G \cup 0\}$.
- Every row of W contains exactly k non-zero entries.

Overview of BGWs

- Let G be some multiplicative group.
- A $BGW(v, k, \lambda)$ over G is a matrix $W = [w_{ij}]$ of order v with entries from $\{G \cup 0\}$.
- Every row of W contains exactly k non-zero entries.
- For every $i, j \in \{1, \cdots, v\}$, $i \neq j$ the multisets

$$\{w_{ik} w_{jk}^{-1} : w_{ik} \neq 0 \neq w_{jk}, 0 \leq k \leq v, i \neq j\}$$

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

Overview of BGWs

- Let G be some multiplicative group.
- A $BGW(v, k, \lambda)$ over G is a matrix $W = [w_{ij}]$ of order v with entries from $\{G \cup 0\}$.
- Every row of W contains exactly k non-zero entries.
- For every $i, j \in \{1, \cdots, v\}$, $i \neq j$ the multisets

  $$\{w_{ik} w_{jk}^{-1} : w_{ik} \neq 0 \neq w_{jk}, 0 \leq k \leq v, i \neq j\}$$

  contain each group element exactly $\lambda/|G|$ times.
- Namely, the conjugate inner product of any two distinct rows of W contains each element of G exactly $\lambda/|G|$ times.

Example of a BGW

Example of a BGW

Example

Let $v = 6$, $k = 5$ and $\lambda = 4$, then

$$W = \begin{bmatrix} 0 & 4 & 4 & 4 & 4 & 4 \\ 2 & 0 & 3 & 4 & 1 & 2 \\ 2 & 1 & 0 & 3 & 2 & 4 \\ 2 & 2 & 1 & 0 & 4 & 3 \\ 2 & 3 & 4 & 2 & 0 & 1 \\ 2 & 4 & 2 & 1 & 3 & 0 \end{bmatrix}$$

is a $BGW(6,5,4)$ over $\mathbb{Z}_4$.

Example of a BGW

Example

Let $v = 6$, $k = 5$ and $\lambda = 4$, then

$$W = \begin{bmatrix} 0 & 4 & 4 & 4 & 4 & 4 \\ 2 & 0 & 3 & 4 & 1 & 2 \\ 2 & 1 & 0 & 3 & 2 & 4 \\ 2 & 2 & 1 & 0 & 4 & 3 \\ 2 & 3 & 4 & 2 & 0 & 1 \\ 2 & 4 & 2 & 1 & 3 & 0 \end{bmatrix}$$

is a $BGW(6,5,4)$ over $\mathbb{Z}_4$. Note that the entries of W are powers of some primitive element of $GF(5)$, say α.

Example of a BGW

Example

Let $v = 6$, $k = 5$ and $\lambda = 4$, then

$$W = \begin{bmatrix} 0 & 4 & 4 & 4 & 4 & 4 \\ 2 & 0 & 3 & 4 & 1 & 2 \\ 2 & 1 & 0 & 3 & 2 & 4 \\ 2 & 2 & 1 & 0 & 4 & 3 \\ 2 & 3 & 4 & 2 & 0 & 1 \\ 2 & 4 & 2 & 1 & 3 & 0 \end{bmatrix}$$

is a $BGW(6,5,4)$ over $\mathbb{Z}_4$. Note that the entries of W are powers of some primitive element of $GF(5)$, say α.

Example of a BGW

0	4	4	4	4	4
2	2	1	0	4	3

Example of a BGW

$$\begin{matrix} 0 & \alpha^4 & \alpha^4 & \alpha^4 & \alpha^4 & \alpha^4 \\ \alpha^2 & \alpha^2 & \alpha^1 & 0 & \alpha^4 & \alpha^3 \end{matrix}$$

Example of a BGW

$$\begin{matrix} 0 & \alpha^4 & \alpha^4 & \alpha^4 & \alpha^4 & \alpha^4 \\ \alpha^2 & \alpha^2 & \alpha^1 & 0 & \alpha^4 & \alpha^3 \end{matrix}$$

Example of a BGW

$$\begin{matrix} \alpha^4 & \alpha^4 & \alpha^4 & \alpha^4 \\ \alpha^2 & \alpha^1 & \alpha^4 & \alpha^3 \end{matrix}$$

Example of a BGW

$$\begin{array}{cccc} \alpha^4 & \alpha^4 & \alpha^4 & \alpha^4 \\ \alpha^{-2} & \alpha^{-1} & \alpha^{-4} & \alpha^{-3} \end{array}$$

Example of a BGW

$$\begin{array}{cccc} \alpha^4 & \alpha^4 & \alpha^4 & \alpha^4 \\ \alpha^{-2} & \alpha^{-1} & \alpha^{-4} & \alpha^{-3} \\ \hline \{\alpha^2 & \alpha^3 & \alpha^0 & \alpha^1\} \end{array}$$

Example of a BGW

$$
\begin{array}{cccc}
\alpha^4 & \alpha^4 & \alpha^4 & \alpha^4 \\
\alpha^{-2} & \alpha^{-1} & \alpha^{-4} & \alpha^{-3} \\
\hline
\{\alpha^2 & \alpha^3 & \alpha^0 & \alpha^1\}
\end{array}
$$

- Each element of $\mathbb{Z}_4$ appears exactly $\lambda/|G| = 4/4 = 1$ time.

The core of W(6,5)

The core of W(6,5)

- Recall our weighing matrix $W(6,5)$:

$$W = \left[\begin{array}{c|ccccc} 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{array}\right]$$

The core of W(6,5)

- Recall our weighing matrix $W(6,5)$:

$$W = \left[\begin{array}{c|ccccc} 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{array}\right]$$

- The *core* of the matrix is:

The core of W(6,5)

- Recall our weighing matrix $W(6,5)$:

$$W = \left[\begin{array}{c|ccccc} 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{array}\right]$$

- The *core* of the matrix is:

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

The core of W(6,5)

- Recall our weighing matrix $W(6,5)$:

$$W = \left[\begin{array}{c|ccccc} 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{array}\right]$$

- The *core* of the matrix is:

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

- Recall that the five rows of C provide an optimal $(5,4,4)_3$ code as $A_3(5,4,4) \leq 5 = M$.

An application

An application

- Using the weighing matrix $W(6,5)$ and O, the $OA(5,6)$ we can construct a $BGW(31,25,20)$ over $\mathbb{Z}_2$.

An application

- Using the weighing matrix $W(6,5)$ and O, the $OA(5,6)$ we can construct a $BGW(31,25,20)$ over $\mathbb{Z}_2$.
- Changing the entry i in O with the i-th row of C results in the *Derived* part of the $BGW(31,25,20)$ over $\mathbb{Z}_2$.

An application

- Using the weighing matrix $W(6,5)$ and O, the $OA(5,6)$ we can construct a $BGW(31,25,20)$ over $\mathbb{Z}_2$.
- Changing the entry i in O with the i-th row of C results in the *Derived* part of the $BGW(31,25,20)$ over $\mathbb{Z}_2$.
- Using $W(6,5)$ we compute $W \otimes (11111)$ which results in the *Residual* part of the following BGW.

A $BGW(31, 25, 20)$ over $\mathbb{Z}_2$

A $BGW(31, 25, 20)$ over $\mathbb{Z}_2$

$$
B = \left[\begin{array}{c|cccccccccccccccccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - & - & - & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - & - & - \\
0 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - \\
0 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - & - & - & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - & - & - & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
\hline
1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 \\
1 & 0 & 1 & - & - & 1 & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - \\
1 & 0 & 1 & - & - & 1 & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - \\
1 & 0 & 1 & - & - & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 \\
1 & 0 & 1 & - & - & 1 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 \\
1 & 1 & 0 & 1 & - & - & 0 & 1 & - & - & 1 & 1 & 0 & 1 & - & - & - & 1 & 0 & 1 & - & - & - & 1 & 0 & 1 & 1 & - & - & 1 & 0 \\
1 & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & - & - & 1 & 0 & 1 & - & - & - & 1 & 0 & 1 & 1 & - & - & 1 & 0 & 0 & 1 & - & - & 1 \\
1 & 1 & 0 & 1 & - & - & - & 1 & 0 & 1 & - & - & - & 1 & 0 & 1 & 1 & - & - & 1 & 0 & 0 & 1 & - & - & 1 & 1 & 0 & 1 & - & - \\
1 & 1 & 0 & 1 & - & - & - & - & 1 & 0 & 1 & 1 & - & - & 1 & 0 & 0 & 1 & - & - & 1 & 1 & 0 & 1 & - & - & - & 1 & 0 & 1 & - \\
1 & 1 & 0 & 1 & - & - & 1 & - & - & 1 & 0 & 0 & 1 & - & - & 1 & 1 & 0 & 1 & - & - & - & 1 & 0 & 1 & - & - & - & 1 & 0 & 1 \\
1 & - & 1 & 0 & 1 & - & 0 & 1 & - & - & 1 & - & 1 & 0 & 1 & - & 1 & - & - & 1 & 0 & 1 & 0 & 1 & - & - & - & - & 1 & 0 & 1 \\
1 & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & - & 1 & - & - & 1 & 0 & 1 & 0 & 1 & - & - & - & - & 1 & 0 & 1 & 0 & 1 & - & - & 1 \\
1 & - & 1 & 0 & 1 & - & 1 & - & - & 1 & 0 & 1 & 0 & 1 & - & - & - & - & 1 & 0 & 1 & 0 & 1 & - & - & 1 & - & 1 & 0 & 1 & - \\
1 & - & 1 & 0 & 1 & - & 1 & 0 & 1 & - & - & - & - & 1 & 0 & 1 & 0 & 1 & - & - & 1 & - & 1 & 0 & 1 & - & 1 & - & - & 1 & 0 \\
1 & - & 1 & 0 & 1 & - & - & - & 1 & 0 & 1 & 0 & 1 & - & - & 1 & - & 1 & 0 & 1 & - & 1 & - & - & 1 & 0 & 1 & 0 & 1 & - & - \\
1 & - & - & 1 & 0 & 1 & 0 & 1 & - & - & 1 & - & - & 1 & 0 & 1 & 1 & 0 & 1 & - & - & 1 & - & - & 1 & 0 & - & 1 & 0 & 1 & - \\
1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & 1 & 1 & 0 & 1 & - & - & 1 & - & - & 1 & 0 & - & 1 & 0 & 1 & - & 0 & 1 & - & - & 1 \\
1 & - & - & 1 & 0 & 1 & 1 & 0 & 1 & - & - & 1 & - & - & 1 & 0 & - & 1 & 0 & 1 & - & 0 & 1 & - & - & 1 & - & - & 1 & 0 & 1 \\
1 & - & - & 1 & 0 & 1 & 1 & - & - & 1 & 0 & - & 1 & 0 & 1 & - & 0 & 1 & - & - & 1 & - & - & 1 & 0 & 1 & 1 & 0 & 1 & - & - \\
1 & - & - & 1 & 0 & 1 & - & 1 & 0 & 1 & - & 0 & 1 & - & - & 1 & - & - & 1 & 0 & 1 & 1 & 0 & 1 & - & - & 1 & - & - & 1 & 0 \\
1 & 1 & - & - & 1 & 0 & 0 & 1 & - & - & 1 & 1 & - & - & 1 & 0 & - & - & 1 & 0 & 1 & - & 1 & 0 & 1 & - & 1 & 0 & 1 & - & - \\
1 & 1 & - & - & 1 & 0 & 1 & - & - & 1 & 0 & - & - & 1 & 0 & 1 & - & 1 & 0 & 1 & - & 1 & 0 & 1 & - & - & 0 & 1 & - & - & 1 \\
1 & 1 & - & - & 1 & 0 & - & - & 1 & 0 & 1 & - & 1 & 0 & 1 & - & 1 & 0 & 1 & - & - & 0 & 1 & - & - & 1 & 1 & - & - & 1 & 0 \\
1 & 1 & - & - & 1 & 0 & - & 1 & 0 & 1 & - & 1 & 0 & 1 & - & - & 0 & 1 & - & - & 1 & 1 & - & - & 1 & 0 & - & - & 1 & 0 & 1 \\
1 & 1 & - & - & 1 & 0 & 1 & 0 & 1 & - & - & 0 & 1 & - & - & 1 & 1 & - & - & 1 & 0 & - & - & 1 & 0 & 1 & - & 1 & 0 & 1 & -
\end{array}\right].
$$

An application of the $BGW(31, 25, 20)$ over $\mathbb{Z}_2$ to optimal ternary codes

An application of the $BGW(31, 25, 20)$ over $\mathbb{Z}_2$ to optimal ternary codes

The derived part $\mathcal{D}$ of the $BGW(31, 25, 20)$ over $\mathbb{Z}_2$ forms an *optimal constant weight ternary code* with parameters $n = 30$, $d = 20$, and $w = 24$.

An application of the $BGW(31, 25, 20)$ over $\mathbb{Z}_2$ to optimal ternary codes

The derived part $\mathcal{D}$ of the $BGW(31, 25, 20)$ over $\mathbb{Z}_2$ forms an *optimal constant weight ternary code* with parameters $n = 30$, $d = 20$, and $w = 24$.

$$\mathcal{D} = \left[\begin{array}{*{30}{c}}
0&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0&1&-&-&1 \\
0&1&-&-&1&1&0&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0&1&-&- \\
0&1&-&-&1&-&1&0&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0&1&- \\
0&1&-&-&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0&1 \\
0&1&-&-&1&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0&1&-&-&1&0 \\
1&0&1&-&-&0&1&-&-&1&1&0&1&-&-&-&1&0&1&-&-&-&1&0&1&1&-&-&1&0 \\
1&0&1&-&-&1&0&1&-&-&-&1&0&1&-&-&-&1&0&1&1&-&-&1&0&0&1&-&-&1 \\
1&0&1&-&-&-&1&0&1&-&-&-&1&0&1&1&-&-&1&0&0&1&-&-&1&1&0&1&-&- \\
1&0&1&-&-&-&-&1&0&1&1&-&-&1&0&0&1&-&-&1&1&0&1&-&-&-&1&0&1&- \\
1&0&1&-&-&1&-&-&1&0&0&1&-&-&1&1&0&1&-&-&-&1&0&1&-&-&-&1&0&1 \\
-&1&0&1&-&0&1&-&-&1&-&1&0&1&-&1&-&-&1&0&1&0&1&-&-&-&-&1&0&1 \\
-&1&0&1&-&-&1&0&1&-&1&-&-&1&0&1&0&1&-&-&-&-&1&0&1&0&1&-&-&1 \\
-&1&0&1&-&1&-&-&1&0&1&0&1&-&-&-&-&1&0&1&0&1&-&-&1&-&1&0&1&- \\
-&1&0&1&-&1&0&1&-&-&-&-&1&0&1&0&1&-&-&1&-&1&0&1&-&1&-&-&1&0 \\
-&1&0&1&-&-&-&1&0&1&0&1&-&-&1&-&1&0&1&-&1&-&-&1&0&1&0&1&-&- \\
-&-&1&0&1&0&1&-&-&1&-&-&1&0&1&1&0&1&-&-&1&-&-&1&0&-&1&0&1&- \\
-&-&1&0&1&-&-&1&0&1&1&0&1&-&-&1&-&-&1&0&-&1&0&1&-&0&1&-&-&1 \\
-&-&1&0&1&1&0&1&-&-&1&-&-&1&0&-&1&0&1&-&0&1&-&-&1&-&-&1&0&1 \\
-&-&1&0&1&1&-&-&1&0&-&1&0&1&-&0&1&-&-&1&-&-&1&0&1&1&0&1&-&- \\
-&-&1&0&1&-&1&0&1&-&0&1&-&-&1&-&-&1&0&1&1&0&1&-&-&1&-&-&1&0 \\
1&-&-&1&0&0&1&-&-&1&1&-&-&1&0&-&-&1&0&1&-&1&0&1&-&1&0&1&-&- \\
1&-&-&1&0&1&-&-&1&0&-&-&1&0&1&-&1&0&1&-&1&0&1&-&-&0&1&-&-&1 \\
1&-&-&1&0&-&-&1&0&1&-&1&0&1&-&1&0&1&-&-&0&1&-&-&1&1&-&-&1&0 \\
1&-&-&1&0&-&1&0&1&-&1&0&1&-&-&0&1&-&-&1&1&-&-&1&0&-&-&1&0&1 \\
1&-&-&1&0&1&0&1&-&-&0&1&-&-&1&1&-&-&1&0&-&-&1&0&1&-&1&0&1&-
\end{array}\right].$$

An application to ternary codes

An application to ternary codes

Example

The 25 rows of $\mathcal{D}$ form an optimal constant weight $(30, 20, 24)_3$ code.

An application to ternary codes

Example

The 25 rows of $\mathcal{D}$ form an optimal constant weight $(30, 20, 24)_3$ code.

Proof.

Each row of $\mathcal{D}$ consists of 6 rows of C (recall C is the core of $W(6, 5)$).

An application to ternary codes

Example

The 25 rows of $\mathcal{D}$ form an optimal constant weight $(30, 20, 24)_3$ code.

Proof.

Each row of $\mathcal{D}$ consists of 6 rows of C (recall C is the core of $W(6,5)$). Any two distinct rows of $\mathcal{D}$ share one row of C in the same column.

An application to ternary codes

Example

The 25 rows of $\mathcal{D}$ form an optimal constant weight $(30, 20, 24)_3$ code.

Proof.

Each row of $\mathcal{D}$ consists of 6 rows of C (recall C is the core of $W(6,5)$). Any two distinct rows of $\mathcal{D}$ share one row of C in the same column. Any two distinct rows of C have a Hamming distance 4.

An application to ternary codes

Example

The 25 rows of $\mathcal{D}$ form an optimal constant weight $(30, 20, 24)_3$ code.

Proof.

Each row of $\mathcal{D}$ consists of 6 rows of C (recall C is the core of $W(6,5)$). Any two distinct rows of $\mathcal{D}$ share one row of C in the same column. Any two distinct rows of C have a Hamming distance 4. Therefore the distance of the code is 20.

An application to ternary codes

Example

The 25 rows of $\mathcal{D}$ form an optimal constant weight $(30, 20, 24)_3$ code.

Proof.

Each row of $\mathcal{D}$ consists of 6 rows of C (recall C is the core of $W(6,5)$). Any two distinct rows of $\mathcal{D}$ share one row of C in the same column. Any two distinct rows of C have a Hamming distance 4. Therefore the distance of the code is 20. Since $a = qw^2 - 2(q-1)nw + (q-1)nd = 3(24)^2 - 2(2)(30)(24) + 2(30)(20) = 48 > 0$ we can apply Johnson Bound (2) to obtain

$$\begin{aligned} A_3(30,20,24) &\leq \left\lfloor \frac{nd(q-1)}{qw^2 - 2(q-1)nw + (q-1)nd} \right\rfloor \\ &= \left\lfloor \frac{2(30)(20)}{3(24)^2 - 2(2)(30)(24) + 2(30)(20)} \right\rfloor . \\ &= \left\lfloor \frac{1200}{48} \right\rfloor = 25 \end{aligned}$$

An application to ternary codes

Example

The 25 rows of $\mathcal{D}$ form an optimal constant weight $(30, 20, 24)_3$ code.

Proof.

Each row of $\mathcal{D}$ consists of 6 rows of C (recall C is the core of $W(6,5)$). Any two distinct rows of $\mathcal{D}$ share one row of C in the same column. Any two distinct rows of C have a Hamming distance 4. Therefore the distance of the code is 20. Since $a = qw^2 - 2(q-1)nw + (q-1)nd = 3(24)^2 - 2(2)(30)(24) + 2(30)(20) = 48 > 0$ we can apply Johnson Bound (2) to obtain

$$\begin{aligned} A_3(30,20,24) &\leq \left\lfloor \frac{nd(q-1)}{qw^2 - 2(q-1)nw + (q-1)nd} \right\rfloor \\ &= \left\lfloor \frac{2(30)(20)}{3(24)^2 - 2(2)(30)(24) + 2(30)(20)} \right\rfloor. \\ &= \left\lfloor \frac{1200}{48} \right\rfloor = 25 \end{aligned}$$

Since $\mathcal{D}$ consists of 25 codewords, it follows that $A_3(30,20,24) \leq 25 = M$ and the constant weight code is optimal. □

Another application to ternary codes

Another application to ternary codes

Example

Let B_{31} be the $BGW(31, 25, 20)$ over $\mathbb{Z}_2$. The rows of the matrix $\begin{bmatrix} B_{31} \\ -B_{31} \end{bmatrix}$ form an *optimal constant weight* $(31, 20, 25)_3$ *code*.

Another application to ternary codes

Example

Let B_{31} be the $BGW(31, 25, 20)$ over $\mathbb{Z}_2$. The rows of the matrix $\begin{bmatrix} B_{31} \\ -B_{31} \end{bmatrix}$ form an *optimal constant weight* $(31, 20, 25)_3$ *code*.

Proof.

Using the properties of $BGW(31, 25, 20)$ the Hamming distance of any two distinct rows of $\pm B_{31}$ is 20.

Another application to ternary codes

Example

Let B_{31} be the $BGW(31, 25, 20)$ over $\mathbb{Z}_2$. The rows of the matrix $\begin{bmatrix} B_{31} \\ -B_{31} \end{bmatrix}$ form an *optimal constant weight* $(31, 20, 25)_3$ *code*.

Proof.

Using the properties of $BGW(31, 25, 20)$ the Hamming distance of any two distinct rows of $\pm B_{31}$ is 20. Similarly, a row from B_{31} and a row from $-B_{31}$ will also have minimum Hamming distance 20.

Another application to ternary codes

Example

Let B_{31} be the $BGW(31,25,20)$ over $\mathbb{Z}_2$. The rows of the matrix $\begin{bmatrix} B_{31} \\ -B_{31} \end{bmatrix}$ form an *optimal constant weight* $(31,20,25)_3$ *code*.

Proof.

Using the properties of $BGW(31,25,20)$ the Hamming distance of any two distinct rows of $\pm B_{31}$ is 20. Similarly, a row from B_{31} and a row from $-B_{31}$ will also have minimum Hamming distance 20. We apply Johnson Bound (1) to obtain

$$A_3(31,20,25) \leq \left\lfloor \frac{n(q-1)}{w} A_q(n-1,d,w-1) \right\rfloor \leq \left\lfloor \frac{2(31)}{25} A_3(30,20,24) \right\rfloor$$
$$= \left\lfloor \frac{62}{25}(25) \right\rfloor = 62.$$

Another application to ternary codes

Example

Let B_{31} be the $BGW(31, 25, 20)$ over $\mathbb{Z}_2$. The rows of the matrix $\begin{bmatrix} B_{31} \\ -B_{31} \end{bmatrix}$ form an *optimal constant weight* $(31, 20, 25)_3$ *code*.

Proof.

Using the properties of $BGW(31, 25, 20)$ the Hamming distance of any two distinct rows of $\pm B_{31}$ is 20. Similarly, a row from B_{31} and a row from $-B_{31}$ will also have minimum Hamming distance 20. We apply Johnson Bound (1) to obtain

$$A_3(31, 20, 25) \leq \left\lfloor \frac{n(q-1)}{w} A_q(n-1, d, w-1) \right\rfloor \leq \left\lfloor \frac{2(31)}{25} A_3(30, 20, 24) \right\rfloor$$
$$= \left\lfloor \frac{62}{25}(25) \right\rfloor = 62.$$

As $B_{31} \cup -B_{31}$ consists of 62 codewords, it follows that $A_3(31, 20, 25) \leq 62 = M$ and the constant weight code is optimal. □

The new class of optimal ternary codes

Theorem

If p is an odd prime power and m is a positive integer, then

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

The new class of optimal ternary codes

Theorem

If p is an odd prime power and m is a positive integer, then

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

Example

We have seen the case for $p = 5$ and $m = 2$. For $m = 3$ we would recursively construct the matrix $B_{156} = BGW(156, 125, 100)$ over $\mathbb{Z}_2$.

The new class of optimal ternary codes

Theorem

If p is an odd prime power and m is a positive integer, then

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

Example

We have seen the case for $p = 5$ and $m = 2$. For $m = 3$ we would recursively construct the matrix $B_{156} = BGW(156, 125, 100)$ over $\mathbb{Z}_2$. The rows of $B_{156} \cup -B_{156}$ form an optimal constant weight $(156, 100, 125)_3$ code.

The new class of optimal ternary codes

Theorem

If p is an odd prime power and m is a positive integer, then

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

Example

We have seen the case for $p = 5$ and $m = 2$. For $m = 3$ we would recursively construct the matrix $B_{156} = BGW(156, 125, 100)$ over $\mathbb{Z}_2$. The rows of $B_{156} \cup -B_{156}$ form an optimal constant weight $(156, 100, 125)_3$ code. The derived part of B_{156} forms an optimal constant weight $(155, 100, 124)_3$ code.

The End!
Thank You!