

A new family of 3-designs of degree 3^*

Vedran Krčadinac

University of Zagreb, Croatia

(joint work with Lucija Relić)

10th Slovenian Conference on Graph Theory

18-24 June, 2023, Kranjska Gora, Slovenia

* This work was partially supported by the Croatian Science Foundation under the project 9752.

Assumptions:

Assumptions:

- Everybody knows the definition of a t - (v, k, λ) design

Assumptions:

- Everybody knows the definition of a t - (v, k, λ) design
- All designs are simple

Assumptions:

- Everybody knows the definition of a t - (v, k, λ) design
- All designs are simple
- $k \leq \frac{1}{2}v$ (complementing the blocks does not change t and d)

Assumptions:

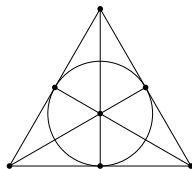
- Everybody knows the definition of a t - (v, k, λ) design
- All designs are simple
- $k \leq \frac{1}{2}v$ (complementing the blocks does not change t and d)

The **degree** of a design is the number of distinct block intersection sizes:

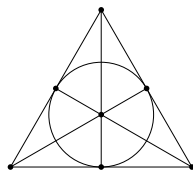
$$d = |\{ |B_1 \cap B_2| : B_1 \neq B_2 \text{ are blocks} \}|$$

$d = 1$: **Symmetric designs** ($v = b$, $t = 2$)

$d = 1$: **Symmetric designs** ($v = b$, $t = 2$)

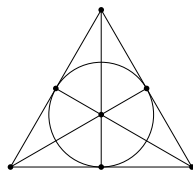


$d = 1$: **Symmetric designs** ($v = b$, $t = 2$)



$d = 2$: **Quasi-symmetric designs** ($t \leq 4$)

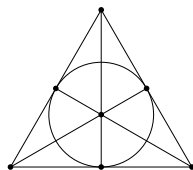
$d = 1$: **Symmetric designs** ($v = b$, $t = 2$)



$d = 2$: **Quasi-symmetric designs** ($t \leq 4$)

R. Vlahović Kruc, *Some results on quasi-symmetric designs with exceptional parameters*, PhD thesis, University of Zagreb, 2019.

$d = 1$: **Symmetric designs** ($v = b$, $t = 2$)



$d = 2$: **Quasi-symmetric designs** ($t \leq 4$)

R. Vlahović Kruc, *Some results on quasi-symmetric designs with exceptional parameters*, PhD thesis, University of Zagreb, 2019.

$d = 3$: ?

Designs of degree $d = 3$

Intersection numbers: $x < y < z$

Designs of degree $d = 3$

Intersection numbers: $x < y < z$

Ray-Chaudhuri, Wilson: $t \leq 6$

Designs of degree $d = 3$

Intersection numbers: $x < y < z$

Ray-Chaudhuri, Wilson: $t \leq 6$

$t = 6$: Do not exist!

C. Peterson, *On tight 6-designs*, Osaka J. Math. **14** (1977), 417–435.

Designs of degree $d = 3$

Intersection numbers: $x < y < z$

Ray-Chaudhuri, Wilson: $t \leq 6$

$t = 6$: Do not exist!

C. Peterson, *On tight 6-designs*, Osaka J. Math. **14** (1977), 417–435.

$t = 5$: The Witt 5-(24, 8, 1) design, $x = 0$, $y = 2$, $z = 4$

Y. J. Ionin, M. S. Shrikhande, *5-designs with three intersection numbers*, J. Combin. Theory Ser. A **69** (1995), no. 1, 36–50.

Designs of degree $d = 3$

Intersection numbers: $x < y < z$

Ray-Chaudhuri, Wilson: $t \leq 6$

$t = 6$: Do not exist!

C. Peterson, *On tight 6-designs*, Osaka J. Math. **14** (1977), 417–435.

$t = 5$: The Witt 5-(24, 8, 1) design, $x = 0$, $y = 2$, $z = 4$

Y. J. Ionin, M. S. Shrikhande, *5-designs with three intersection numbers*, J. Combin. Theory Ser. A **69** (1995), no. 1, 36–50.

$t = 4$:

V. Krčadinac, R. Vlahović Kruc, *Schematic 4-designs*, Discrete Math. **346** (2023), no. 7, Paper No. 113385, 7 pp.

Designs of degree $d = 3$ and strength $t = 4$

| No. | v | k | λ | x | y | z | \exists |
|-----|-----|-----|-----------|-----|-----|-----|-----------|
| 1 | 11 | 5 | 1 | 1 | 2 | 3 | |
| 2 | 23 | 8 | 4 | 0 | 2 | 4 | |
| 3 | 23 | 11 | 48 | 3 | 5 | 7 | |
| 4 | 24 | 8 | 5 | 0 | 2 | 4 | |
| 5 | 47 | 11 | 8 | 1 | 3 | 5 | |
| 6 | 71 | 35 | 264 | 14 | 17 | 20 | |
| 7 | 199 | 99 | 2328 | 44 | 49 | 54 | |
| 8 | 391 | 195 | 9264 | 90 | 97 | 104 | |
| 9 | 647 | 323 | 25680 | 152 | 161 | 170 | |
| 10 | 659 | 329 | 390874 | 153 | 164 | 175 | |
| 11 | 967 | 483 | 57720 | 230 | 241 | 252 | |

Designs of degree $d = 3$ and strength $t = 4$

| No. | v | k | λ | x | y | z | \exists |
|-----|-----|-----|-----------|-----|-----|-----|-----------|
| 1 | 11 | 5 | 1 | 1 | 2 | 3 | ✓ |
| 2 | 23 | 8 | 4 | 0 | 2 | 4 | ✓ |
| 3 | 23 | 11 | 48 | 3 | 5 | 7 | ✓ |
| 4 | 24 | 8 | 5 | 0 | 2 | 4 | ✓ |
| 5 | 47 | 11 | 8 | 1 | 3 | 5 | ✓ |
| 6 | 71 | 35 | 264 | 14 | 17 | 20 | |
| 7 | 199 | 99 | 2328 | 44 | 49 | 54 | |
| 8 | 391 | 195 | 9264 | 90 | 97 | 104 | |
| 9 | 647 | 323 | 25680 | 152 | 161 | 170 | |
| 10 | 659 | 329 | 390874 | 153 | 164 | 175 | |
| 11 | 967 | 483 | 57720 | 230 | 241 | 252 | |

Designs of degree $d = 3$ and strength $t = 4$

| No. | v | k | λ | x | y | z | \exists |
|-----|-----|-----|-----------|-----|-----|-----|-----------|
| 1 | 11 | 5 | 1 | 1 | 2 | 3 | ✓ |
| 2 | 23 | 8 | 4 | 0 | 2 | 4 | ✓ |
| 3 | 23 | 11 | 48 | 3 | 5 | 7 | ✓ |
| 4 | 24 | 8 | 5 | 0 | 2 | 4 | ✓ |
| 5 | 47 | 11 | 8 | 1 | 3 | 5 | ✓ |
| 6 | 71 | 35 | 264 | 14 | 17 | 20 | |
| 7 | 199 | 99 | 2328 | 44 | 49 | 54 | |
| 8 | 391 | 195 | 9264 | 90 | 97 | 104 | |
| 9 | 647 | 323 | 25680 | 152 | 161 | 170 | |
| 10 | 659 | 329 | 390874 | 153 | 164 | 175 | |
| 11 | 967 | 483 | 57720 | 230 | 241 | 252 | |

$QR(11, 3): [11, 6, 5]_3$

$QR(23, 2): [23, 12, 7]_2$

$QR(23, 2): [23, 12, 7]_2$

$\widehat{QR}(23, 2): [24, 12, 8]_2$

$QR(47, 2): [47, 24, 11]_2$

Designs of degree $d = 3$ and strength $t = 4$

| No. | v | k | λ | x | y | z | \exists |
|-----|-----|-----|-----------|-----|-----|-----|-----------|
| 1 | 11 | 5 | 1 | 1 | 2 | 3 | ✓ |
| 2 | 23 | 8 | 4 | 0 | 2 | 4 | ✓ |
| 3 | 23 | 11 | 48 | 3 | 5 | 7 | ✓ |
| 4 | 24 | 8 | 5 | 0 | 2 | 4 | ✓ |
| 5 | 47 | 11 | 8 | 1 | 3 | 5 | ✓ |
| 6 | 71 | 35 | 264 | 14 | 17 | 20 | ? |
| 7 | 199 | 99 | 2328 | 44 | 49 | 54 | ? |
| 8 | 391 | 195 | 9264 | 90 | 97 | 104 | ? |
| 9 | 647 | 323 | 25680 | 152 | 161 | 170 | ? |
| 10 | 659 | 329 | 390874 | 153 | 164 | 175 | ? |
| 11 | 967 | 483 | 57720 | 230 | 241 | 252 | ? |

$QR(11, 3): [11, 6, 5]_3$

$QR(23, 2): [23, 12, 7]_2$

$QR(23, 2): [23, 12, 7]_2$

$\widehat{QR}(23, 2): [24, 12, 8]_2$

$QR(47, 2): [47, 24, 11]_2$

Designs of degree $d = 3$ and strength $t = 4$

| No. | v | k | λ | x | y | z | \exists |
|-----|-----|-----|-----------|-----|-----|-----|-----------|
| 1 | 11 | 5 | 1 | 1 | 2 | 3 | ✓ |
| 2 | 23 | 8 | 4 | 0 | 2 | 4 | ✓ |
| 3 | 23 | 11 | 48 | 3 | 5 | 7 | ✓ |
| 4 | 24 | 8 | 5 | 0 | 2 | 4 | ✓ |
| 5 | 47 | 11 | 8 | 1 | 3 | 5 | ✓ |
| 6 | 71 | 35 | 264 | 14 | 17 | 20 | ? |
| 7 | 199 | 99 | 2328 | 44 | 49 | 54 | ? |
| 8 | 391 | 195 | 9264 | 90 | 97 | 104 | ? |
| 9 | 647 | 323 | 25680 | 152 | 161 | 170 | ? |
| 10 | 659 | 329 | 390874 | 153 | 164 | 175 | ? |
| 11 | 967 | 483 | 57720 | 230 | 241 | 252 | ? |

$QR(11, 3)$: $[11, 6, 5]_3$

$QR(23, 2)$: $[23, 12, 7]_2$

$QR(23, 2)$: $[23, 12, 7]_2$

$\widehat{QR}(23, 2)$: $[24, 12, 8]_2$

$QR(47, 2)$: $[47, 24, 11]_2$

Designs of degree $d = 3$ and strength $t = 4$

Admissible parameters:

$$v = 8n^2 - 1$$

$$k = 4n^2 - 1 = (2n - 1)(2n + 1)$$

$$\lambda = 4n^4 - 7n^2 + 3 = (n - 1)(n + 1)(4n^2 - 3)$$

$$x = 2n^2 - n - 1 = (n - 1)(2n + 1)$$

$$y = 2n^2 - 1$$

$$z = 2n^2 + n - 1 = (n + 1)(2n - 1)$$

$n \geq 3$ odd

Designs of degree $d = 3$ and strength $t = 4$

Admissible parameters:

$$v = 8n^2 - 1$$

$$k = 4n^2 - 1 = (2n - 1)(2n + 1)$$

$$\lambda = 4n^4 - 7n^2 + 3 = (n - 1)(n + 1)(4n^2 - 3)$$

$$x = 2n^2 - n - 1 = (n - 1)(2n + 1)$$

$$y = 2n^2 - 1$$

$$z = 2n^2 + n - 1 = (n + 1)(2n - 1)$$

$n \geq 3$ odd

Theorem (Cameron, Delsarte, 1973)

In a design of degree d and strength $t \geq 2d - 2$, the blocks form a symmetric association scheme with d classes.

\rightsquigarrow Schematic designs

Designs of degree $d = 3$ and strength $t = 3$

$d = 3, t = 3$:

Designs of degree $d = 3$ and strength $t = 3$

$d = 3, t = 3$: Lots of admissible parameters, e.g. all Steiner 3-designs.

Designs of degree $d = 3$ and strength $t = 3$

$d = 3, t = 3$: Lots of admissible parameters, e.g. all Steiner 3-designs.

| v | k | λ | x | y | z | \exists |
|-----|-----|-----------|-----|-----|-----|-----------|
| 16 | 4 | 1 | 0 | 1 | 2 | ✓ |
| 16 | 6 | 4 | 1 | 2 | 3 | ✓ |
| 32 | 8 | 7 | 0 | 2 | 4 | ✓ |
| 32 | 12 | 22 | 2 | 4 | 6 | ✓ |
| 64 | 16 | 35 | 0 | 4 | 8 | ✓ |
| 64 | 28 | 156 | 10 | 12 | 14 | ✓ |
| 128 | 32 | 155 | 0 | 8 | 16 | ✓ |
| 128 | 56 | 660 | 20 | 24 | 28 | ✓ |
| 256 | 64 | 651 | 0 | 16 | 32 | ✓ |
| 256 | 120 | 3304 | 52 | 56 | 60 | ✓ |
| 512 | 128 | 2667 | 0 | 32 | 64 | ✓ |
| 512 | 240 | 13384 | 104 | 112 | 120 | ✓ |

Designs of degree $d = 3$ and strength $t = 3$

$d = 3, t = 3$: Lots of admissible parameters, e.g. all Steiner 3-designs.

| v | k | λ | x | y | z | \exists | |
|-----|-----|-----------|-----|-----|-----|-----------|--|
| 16 | 4 | 1 | 0 | 1 | 2 | ✓ | $AG_2(4, 2), RM(2, 4): [16, 11, 4]_2$ |
| 16 | 6 | 4 | 1 | 2 | 3 | ✓ | |
| 32 | 8 | 7 | 0 | 2 | 4 | ✓ | $AG_3(5, 2), RM(2, 5): [32, 16, 8]_2$ |
| 32 | 12 | 22 | 2 | 4 | 6 | ✓ | |
| 64 | 16 | 35 | 0 | 4 | 8 | ✓ | $AG_4(6, 2), RM(2, 6): [64, 22, 16]_2$ |
| 64 | 28 | 156 | 10 | 12 | 14 | ✓ | |
| 128 | 32 | 155 | 0 | 8 | 16 | ✓ | $AG_5(7, 2), RM(2, 7): [128, 29, 32]_2$ |
| 128 | 56 | 660 | 20 | 24 | 28 | ✓ | |
| 256 | 64 | 651 | 0 | 16 | 32 | ✓ | $AG_6(8, 2), RM(2, 8): [256, 37, 64]_2$ |
| 256 | 120 | 3304 | 52 | 56 | 60 | ✓ | |
| 512 | 128 | 2667 | 0 | 32 | 64 | ✓ | $AG_7(9, 2), RM(2, 9): [512, 46, 128]_2$ |
| 512 | 240 | 13384 | 104 | 112 | 120 | ✓ | |

Designs of degree $d = 3$ and strength $t = 3$

$d = 3, t = 3$: Lots of admissible parameters, e.g. all Steiner 3-designs.

| v | k | λ | x | y | z | \exists | |
|-----|-----|-----------|-----|-----|-----|-----------|--|
| 16 | 4 | 1 | 0 | 1 | 2 | ✓ | $AG_2(4, 2), RM(2, 4): [16, 11, 4]_2$ |
| 16 | 6 | 4 | 1 | 2 | 3 | ✓ | Nordstrom-Robinson: $(16, 2^8, 6)_2$ |
| 32 | 8 | 7 | 0 | 2 | 4 | ✓ | $AG_3(5, 2), RM(2, 5): [32, 16, 8]_2$ |
| 32 | 12 | 22 | 2 | 4 | 6 | ✓ | |
| 64 | 16 | 35 | 0 | 4 | 8 | ✓ | $AG_4(6, 2), RM(2, 6): [64, 22, 16]_2$ |
| 64 | 28 | 156 | 10 | 12 | 14 | ✓ | Kerdock code: $(64, 2^{12}, 28)_2$ |
| 128 | 32 | 155 | 0 | 8 | 16 | ✓ | $AG_5(7, 2), RM(2, 7): [128, 29, 32]_2$ |
| 128 | 56 | 660 | 20 | 24 | 28 | ✓ | |
| 256 | 64 | 651 | 0 | 16 | 32 | ✓ | $AG_6(8, 2), RM(2, 8): [256, 37, 64]_2$ |
| 256 | 120 | 3304 | 52 | 56 | 60 | ✓ | Kerdock code: $(256, 2^{16}, 120)_2$ |
| 512 | 128 | 2667 | 0 | 32 | 64 | ✓ | $AG_7(9, 2), RM(2, 9): [512, 46, 128]_2$ |
| 512 | 240 | 13384 | 104 | 112 | 120 | ✓ | |

Designs of degree $d = 3$ and strength $t = 3$

$d = 3, t = 3$: Lots of admissible parameters, e.g. all Steiner 3-designs.

| v | k | λ | x | y | z | \exists | |
|-----|-----|-----------|-----|-----|-----|-----------|--|
| 16 | 4 | 1 | 0 | 1 | 2 | ✓ | $AG_2(4, 2), RM(2, 4): [16, 11, 4]_2$ |
| 16 | 6 | 4 | 1 | 2 | 3 | ✓ | Nordstrom-Robinson: $(16, 2^8, 6)_2$ |
| 32 | 8 | 7 | 0 | 2 | 4 | ✓ | $AG_3(5, 2), RM(2, 5): [32, 16, 8]_2$ |
| 32 | 12 | 22 | 2 | 4 | 6 | ✓ | ? |
| 64 | 16 | 35 | 0 | 4 | 8 | ✓ | $AG_4(6, 2), RM(2, 6): [64, 22, 16]_2$ |
| 64 | 28 | 156 | 10 | 12 | 14 | ✓ | Kerdock code: $(64, 2^{12}, 28)_2$ |
| 128 | 32 | 155 | 0 | 8 | 16 | ✓ | $AG_5(7, 2), RM(2, 7): [128, 29, 32]_2$ |
| 128 | 56 | 660 | 20 | 24 | 28 | ✓ | ? |
| 256 | 64 | 651 | 0 | 16 | 32 | ✓ | $AG_6(8, 2), RM(2, 8): [256, 37, 64]_2$ |
| 256 | 120 | 3304 | 52 | 56 | 60 | ✓ | Kerdock code: $(256, 2^{16}, 120)_2$ |
| 512 | 128 | 2667 | 0 | 32 | 64 | ✓ | $AG_7(9, 2), RM(2, 9): [512, 46, 128]_2$ |
| 512 | 240 | 13384 | 104 | 112 | 120 | ✓ | ? |

Commercial break

Combinatorial Constructions Conference

April 7-13, 2024, Dubrovnik, Croatia



Combinatorial Constructions Conference (CCC) will take place at the Centre for Advanced Academic Studies in Dubrovnik, Croatia.

April 7-13, 2024

Invited speakers:

| | |
|---------------------------|----------------------------|
| Marco Buratti, Italy | Michael Kiermaier, Germany |
| Eimear Byrne, Ireland | Patric Östergård, Finland |
| Dean Crnković, Croatia | Kai-Uwe Schmidt, Germany |
| Daniel Horsley, Australia | |

<https://web.math.pmf.unizg.hr/acco/meetings.php>

Known series of 3-designs of degree 3

The known series:

$$v = 2^m$$

$$k = 2^{m-1} - 2^{(m-2)/2}$$

$$\lambda = 2^{(m-8)/2} \left(2^{m/2} - 2 \right) \left(2^m - 2^{m/2} - 4 \right)$$

$$x = 2^{(m-4)/2} \left(2^{m/2} - 3 \right)$$

$$y = 2^{(m-4)/2} \left(2^{m/2} - 2 \right)$$

$$z = 2^{(m-4)/2} \left(2^{m/2} - 1 \right)$$

$m \geq 4$ even

Known series of 3-designs of degree 3

The known series:

$$v = 2^m$$

$$k = 2^{m-1} - 2^{(m-2)/2}$$

$$\lambda = 2^{(m-8)/2} \left(2^{m/2} - 2 \right) \left(2^m - 2^{m/2} - 4 \right)$$

$$x = 2^{(m-4)/2} \left(2^{m/2} - 3 \right)$$

$$y = 2^{(m-4)/2} \left(2^{m/2} - 2 \right)$$

$$z = 2^{(m-4)/2} \left(2^{m/2} - 1 \right)$$

Points: $AG(m, 2)$

$m \geq 4$ **even**

Known series of 3-designs of degree 3

The known series:

$$v = 2^m$$

$$k = 2^{m-1} - 2^{(m-2)/2}$$

$$\lambda = 2^{(m-8)/2} \left(2^{m/2} - 2 \right) \left(2^m - 2^{m/2} - 4 \right)$$

$$x = 2^{(m-4)/2} \left(2^{m/2} - 3 \right)$$

$$y = 2^{(m-4)/2} \left(2^{m/2} - 2 \right)$$

$$z = 2^{(m-4)/2} \left(2^{m/2} - 1 \right)$$

Points: $AG(m, 2)$

$m \geq 4$ **even**

Blocks: incidence functions $f : AG(m, 2) \rightarrow \{0, 1\}$

Known series of 3-designs of degree 3

The known series:

$$v = 2^m$$

$$k = 2^{m-1} - 2^{(m-2)/2}$$

$$\lambda = 2^{(m-8)/2} \left(2^{m/2} - 2 \right) \left(2^m - 2^{m/2} - 4 \right)$$

$$x = 2^{(m-4)/2} \left(2^{m/2} - 3 \right)$$

$$y = 2^{(m-4)/2} \left(2^{m/2} - 2 \right)$$

$$z = 2^{(m-4)/2} \left(2^{m/2} - 1 \right)$$

Points: $AG(m, 2)$

$m \geq 4$ **even**

Blocks: incidence functions $f : AG(m, 2) \rightarrow \{0, 1\}$

$RM(1, m)$

Known series of 3-designs of degree 3

The known series:

$$v = 2^m$$

$$k = 2^{m-1} - 2^{(m-2)/2}$$

$$\lambda = 2^{(m-8)/2} \left(2^{m/2} - 2 \right) \left(2^m - 2^{m/2} - 4 \right)$$

$$x = 2^{(m-4)/2} \left(2^{m/2} - 3 \right)$$

$$y = 2^{(m-4)/2} \left(2^{m/2} - 2 \right)$$

$$z = 2^{(m-4)/2} \left(2^{m/2} - 1 \right)$$

Points: $AG(m, 2)$

$m \geq 4$ **even**

Blocks: incidence functions $f : AG(m, 2) \rightarrow \{0, 1\}$

$RM(1, m)$

$RM(2, m)$

Known series of 3-designs of degree 3

The known series:

$$v = 2^m$$

$$k = 2^{m-1} - 2^{(m-2)/2}$$

$$\lambda = 2^{(m-8)/2} \left(2^{m/2} - 2 \right) \left(2^m - 2^{m/2} - 4 \right)$$

$$x = 2^{(m-4)/2} \left(2^{m/2} - 3 \right)$$

$$y = 2^{(m-4)/2} \left(2^{m/2} - 2 \right)$$

$$z = 2^{(m-4)/2} \left(2^{m/2} - 1 \right)$$

Points: $AG(m, 2)$

$m \geq 4$ **even**

Blocks: incidence functions $f : AG(m, 2) \rightarrow \{0, 1\}$

$$RM(1, m) \subset K(m) \subset RM(2, m)$$

Kerdock code $K(m)$: $(2^m, 2^{2m}, 2^{m-1} - 2^{(m-2)/2})$

Known series of 3-designs of degree 3

The known series:

$$v = 2^m$$

$$k = 2^{m-1} - 2^{(m-2)/2}$$

$$\lambda = 2^{(m-8)/2} (2^{m/2} - 2) (2^m - 2^{m/2} - 4)$$

$$x = 2^{(m-4)/2} (2^{m/2} - 3)$$

$$y = 2^{(m-4)/2} (2^{m/2} - 2)$$

$$z = 2^{(m-4)/2} (2^{m/2} - 1)$$

Points: $AG(m, 2)$

$m \geq 4$ **even**

Weight (distance) distribution of $RM(1, m) \subset K(m)$:

| | | | | | |
|----|---|-------------------------|---------------|-------------------------|-------|
| wt | 0 | $2^{m-1} - 2^{(m-2)/2}$ | 2^{m-1} | $2^{m-1} + 2^{(m-2)/2}$ | 2^m |
| # | 1 | $2^m(2^{m-1} - 1)$ | $2^{m+1} - 2$ | $2^m(2^{m-1} - 1)$ | 1 |

Known series of 3-designs of degree 3

The known series:

$$v = 2^m$$

$$k = 2^{m-1} - 2^{(m-2)/2}$$

$$\lambda = 2^{(m-8)/2} (2^{m/2} - 2) (2^m - 2^{m/2} - 4)$$

$$x = 2^{(m-4)/2} (2^{m/2} - 3)$$

$$y = 2^{(m-4)/2} (2^{m/2} - 2)$$

$$z = 2^{(m-4)/2} (2^{m/2} - 1)$$

Points: $AG(m, 2)$

$m \geq 4$ **even**

Weight (distance) distribution of $RM(1, m) \subset K(m)$:

| | | | | | |
|----|---|-------------------------|---------------|-------------------------|-------|
| wt | 0 | $2^{m-1} - 2^{(m-2)/2}$ | 2^{m-1} | $2^{m-1} + 2^{(m-2)/2}$ | 2^m |
| # | 1 | $2^m(2^{m-1} - 1)$ | $2^{m+1} - 2$ | $2^m(2^{m-1} - 1)$ | 1 |

Known series of 3-designs of degree 3

The known series:

$$v = 2^m$$

$$k = 2^{m-1} - 2^{(m-2)/2}$$

$$\lambda = 2^{(m-8)/2} (2^{m/2} - 2) (2^m - 2^{m/2} - 4)$$

$$x = 2^{(m-4)/2} (2^{m/2} - 3)$$

$$y = 2^{(m-4)/2} (2^{m/2} - 2)$$

$$z = 2^{(m-4)/2} (2^{m/2} - 1)$$

Points: $AG(m, 2)$

$m \geq 4$ **even**

Weight (distance) distribution of $RM(1, m) \subset K(m)$:

| | | | | | |
|----|---|-------------------------|---------------|-------------------------|-------|
| wt | 0 | $2^{m-1} - 2^{(m-2)/2}$ | 2^{m-1} | $2^{m-1} + 2^{(m-2)/2}$ | 2^m |
| # | 1 | $2^m(2^{m-1} - 1)$ | $2^{m+1} - 2$ | $2^m(2^{m-1} - 1)$ | 1 |

Known series of 3-designs of degree 3

The known series:

$$v = 2^m$$

Points: $AG(m, 2)$

$$k = 2^{m-1} - 2^{(m-2)/2}$$

$$\lambda = 2^{(m-8)/2} (2^{m/2} - 2) (2^m - 2^{m/2} - 4)$$

$m \geq 4$ even

$$x = 2^{(m-4)/2} (2^{m/2} - 3)$$

$$y = 2^{(m-4)/2} (2^{m/2} - 2) \rightsquigarrow \text{equivalence relation}$$

$$z = 2^{(m-4)/2} (2^{m/2} - 1)$$

Weight (distance) distribution of $RM(1, m) \subset K(m)$:

| | | | | | |
|----|---|-------------------------|---------------|-------------------------|-------|
| wt | 0 | $2^{m-1} - 2^{(m-2)/2}$ | 2^{m-1} | $2^{m-1} + 2^{(m-2)/2}$ | 2^m |
| # | 1 | $2^m(2^{m-1} - 1)$ | $2^{m+1} - 2$ | $2^m(2^{m-1} - 1)$ | 1 |

Known series of 3-designs of degree 3

The known series:

$$v = 2^m$$

Points: $AG(m, 2)$

$$k = 2^{m-1} - 2^{(m-2)/2}$$

$$\lambda = 2^{(m-8)/2} (2^{m/2} - 2) (2^m - 2^{m/2} - 4)$$

$m \geq 4$ even

$$x = 2^{(m-4)/2} (2^{m/2} - 3)$$

$$y = 2^{(m-4)/2} (2^{m/2} - 2) \rightsquigarrow \text{equivalence relation}$$

$$z = 2^{(m-4)/2} (2^{m/2} - 1) \quad 2^{m-1} - 1 \quad \text{LSSD}(v, k, y)_s$$

Weight (distance) distribution of $RM(1, m) \subset K(m)$:

| | | | | | |
|----|---|-------------------------|---------------|-------------------------|-------|
| wt | 0 | $2^{m-1} - 2^{(m-2)/2}$ | 2^{m-1} | $2^{m-1} + 2^{(m-2)/2}$ | 2^m |
| # | 1 | $2^m(2^{m-1} - 1)$ | $2^{m+1} - 2$ | $2^m(2^{m-1} - 1)$ | 1 |

Known series of 3-designs of degree 3

The known series:

$$v = 2^m$$

Points: $AG(m, 2)$

$$k = 2^{m-1} - 2^{(m-2)/2}$$

$$\lambda = 2^{(m-8)/2} (2^{m/2} - 2) (2^m - 2^{m/2} - 4)$$

$m \geq 4$ **even**

$$x = 2^{(m-4)/2} (2^{m/2} - 3)$$

$$y = 2^{(m-4)/2} (2^{m/2} - 2)$$

Schematic!

$$z = 2^{(m-4)/2} (2^{m/2} - 1)$$

Weight (distance) distribution of $RM(1, m) \subset K(m)$:

| | | | | | |
|----|---|-------------------------|---------------|-------------------------|-------|
| wt | 0 | $2^{m-1} - 2^{(m-2)/2}$ | 2^{m-1} | $2^{m-1} + 2^{(m-2)/2}$ | 2^m |
| # | 1 | $2^m(2^{m-1} - 1)$ | $2^{m+1} - 2$ | $2^m(2^{m-1} - 1)$ | 1 |

Known series of 3-designs of degree 3 – wherefrom?

A. W. Nordstrom, J. P. Robinson, *An optimum nonlinear code*,
Information and Control **11** (1967), 613–616.

Known series of 3-designs of degree 3 – wherefrom?

A. W. Nordstrom, J. P. Robinson, *An optimum nonlinear code*, Information and Control **11** (1967), 613–616.

F. P. Preparata, *A class of optimum nonlinear double-error-correcting codes*, Information and Control **13** (1968), 378–400.

A. M. Kerdock, *A class of low-rate nonlinear binary codes*, Information and Control **20** (1972), 182–187.

Known series of 3-designs of degree 3 – wherefrom?

A. W. Nordstrom, J. P. Robinson, *An optimum nonlinear code*, Information and Control **11** (1967), 613–616.

F. P. Preparata, *A class of optimum nonlinear double-error-correcting codes*, Information and Control **13** (1968), 378–400.

A. M. Kerdock, *A class of low-rate nonlinear binary codes*, Information and Control **20** (1972), 182–187.

P. J. Cameron, *On groups with several doubly-transitive permutation representations*, Math. Z. **128** (1972), 1–14.

P. J. Cameron, J. J. Seidel, *Quadratic forms over $GF(2)$* , Nederl. Akad. Wetensch. Proc. Ser. A **76**=Indag. Math. **35** (1973), 1–8.

Known series of 3-designs of degree 3 – wherefrom?

A. W. Nordstrom, J. P. Robinson, *An optimum nonlinear code*, Information and Control **11** (1967), 613–616.

F. P. Preparata, *A class of optimum nonlinear double-error-correcting codes*, Information and Control **13** (1968), 378–400.

A. M. Kerdock, *A class of low-rate nonlinear binary codes*, Information and Control **20** (1972), 182–187.

P. J. Cameron, *On groups with several doubly-transitive permutation representations*, Math. Z. **128** (1972), 1–14.

P. J. Cameron, J. J. Seidel, *Quadratic forms over $GF(2)$* , Nederl. Akad. Wetensch. Proc. Ser. A **76**=Indag. Math. **35** (1973), 1–8.

R. Noda, *On homogeneous systems of linked symmetric designs*, Math. Z. **138** (1974), 15–20.

Known series of 3-designs of degree 3 – wherefrom?

W. M. Kantor, *Spreads, translation planes and Kerdock sets. I; II*, SIAM J. Algebraic Discrete Methods **3** (1982), no. 2; 3, 151–165; 308–318.

W. M. Kantor, *An exponential number of generalized Kerdock codes*, Inform. and Control **53** (1982), no. 1-2, 74–80.

W. M. Kantor, *Codes, quadratic forms and finite geometries*, Proc. Sympos. Appl. Math. **50** (1995), Amer. Math. Soc., 153–177.

Known series of 3-designs of degree 3 – wherefrom?

W. M. Kantor, *Spreads, translation planes and Kerdock sets. I; II*, SIAM J. Algebraic Discrete Methods **3** (1982), no. 2; 3, 151–165; 308–318.

W. M. Kantor, *An exponential number of generalized Kerdock codes*, Inform. and Control **53** (1982), no. 1-2, 74–80.

W. M. Kantor, *Codes, quadratic forms and finite geometries*, Proc. Sympos. Appl. Math. **50** (1995), Amer. Math. Soc., 153–177.

A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

Known series of 3-designs of degree 3 – wherefrom?

W. M. Kantor, *Spreads, translation planes and Kerdock sets. I; II*, SIAM J. Algebraic Discrete Methods **3** (1982), no. 2; 3, 151–165; 308–318.

W. M. Kantor, *An exponential number of generalized Kerdock codes*, Inform. and Control **53** (1982), no. 1-2, 74–80.

W. M. Kantor, *Codes, quadratic forms and finite geometries*, Proc. Sympos. Appl. Math. **50** (1995), Amer. Math. Soc., 153–177.

A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

K. Yang, T. Helleseht, *Two new infinite families of 3-designs from Kerdock codes over \mathbb{Z}_4* , Des. Codes Cryptogr. **15** (1998), no. 2, 201–214.

$v = 2^m$, $k = 2^{m-1} + 2^{m-2} \pm 2^{(m-3)/2}$, $\lambda = k(k-1)(k-2)/(2^m-2)$,
 $m \geq 3$ **odd**

New series of 3-designs of degree 3

The new series:

$$v = 2^m$$

Points: $AG(m, 2)$

$$k = 2^{m-1} - 2^{(m-1)/2}$$

$$\lambda = 2^{(m-7)/2} \left(2^{(m-1)/2} - 2 \right) \left(2^m - 2^{(m+1)/2} - 2 \right)$$

$m \geq 5$ **odd**

$$x = 2^{(m-3)/2} \left(2^{(m-1)/2} - 3 \right)$$

$$y = 2^{(m-3)/2} \left(2^{(m-1)/2} - 2 \right)$$

$$z = 2^{(m-3)/2} \left(2^{(m-1)/2} - 1 \right)$$

New series of 3-designs of degree 3

The new series:

$$\begin{aligned}v &= 2^m && \text{Points: } AG(m, 2) \\k &= 2^{m-1} - 2^{(m-1)/2} \\ \lambda &= 2^{(m-7)/2} \left(2^{(m-1)/2} - 2 \right) \left(2^m - 2^{(m+1)/2} - 2 \right) \\x &= 2^{(m-3)/2} \left(2^{(m-1)/2} - 3 \right) \\y &= 2^{(m-3)/2} \left(2^{(m-1)/2} - 2 \right) \\z &= 2^{(m-3)/2} \left(2^{(m-1)/2} - 1 \right)\end{aligned}$$

$m \geq 5$ **odd**

Corresponding code: $(2^m, 2^{2m+1}, 2^{m-1} - 2^{(m-1)/2})$

$$RM(1, m) \subset C \subset RM(2, m)$$

New series of 3-designs of degree 3

The new series:

$$\begin{aligned}v &= 2^m && \text{Points: } AG(m, 2) \\k &= 2^{m-1} - 2^{(m-1)/2} \\ \lambda &= 2^{(m-7)/2} \left(2^{(m-1)/2} - 2 \right) \left(2^m - 2^{(m+1)/2} - 2 \right) \\x &= 2^{(m-3)/2} \left(2^{(m-1)/2} - 3 \right) \\y &= 2^{(m-3)/2} \left(2^{(m-1)/2} - 2 \right) \\z &= 2^{(m-3)/2} \left(2^{(m-1)/2} - 1 \right)\end{aligned}$$

$m \geq 5$ **odd**

Corresponding code: $(2^m, 2^{2m+1}, 2^{m-1} - 2^{(m-1)/2})$

| | | | | | |
|----|---|-------------------------|--------------------|-------------------------|-------|
| wt | 0 | $2^{m-1} - 2^{(m-1)/2}$ | 2^{m-1} | $2^{m-1} + 2^{(m-1)/2}$ | 2^m |
| # | 1 | $2^{m-1}(2^m - 1)$ | $2^m(2^m + 1) - 2$ | $2^{m-1}(2^m - 1)$ | 1 |

New series of 3-designs of degree 3

The new series:

$$\begin{aligned}v &= 2^m && \text{Points: } AG(m, 2) \\k &= 2^{m-1} - 2^{(m-1)/2} \\ \lambda &= 2^{(m-7)/2} \left(2^{(m-1)/2} - 2 \right) \left(2^m - 2^{(m+1)/2} - 2 \right) \\x &= 2^{(m-3)/2} \left(2^{(m-1)/2} - 3 \right) \\y &= 2^{(m-3)/2} \left(2^{(m-1)/2} - 2 \right) \\z &= 2^{(m-3)/2} \left(2^{(m-1)/2} - 1 \right)\end{aligned}$$

$m \geq 5$ **odd**

Corresponding code: $(2^m, 2^{2m+1}, 2^{m-1} - 2^{(m-1)/2})$

| | | | | | |
|----|---|-------------------------|--------------------|-------------------------|-------|
| wt | 0 | $2^{m-1} - 2^{(m-1)/2}$ | 2^{m-1} | $2^{m-1} + 2^{(m-1)/2}$ | 2^m |
| # | 1 | $2^{m-1}(2^m - 1)$ | $2^m(2^m + 1) - 2$ | $2^{m-1}(2^m - 1)$ | 1 |

New series of 3-designs of degree 3

The new series:

$$\begin{aligned}v &= 2^m && \text{Points: } AG(m, 2) \\k &= 2^{m-1} - 2^{(m-1)/2} \\ \lambda &= 2^{(m-7)/2} \left(2^{(m-1)/2} - 2 \right) \left(2^m - 2^{(m+1)/2} - 2 \right) \\x &= 2^{(m-3)/2} \left(2^{(m-1)/2} - 3 \right) \\y &= 2^{(m-3)/2} \left(2^{(m-1)/2} - 2 \right) \\z &= 2^{(m-3)/2} \left(2^{(m-1)/2} - 1 \right)\end{aligned}$$

$m \geq 5$ **odd**

Corresponding code: $(2^m, 2^{2m+1}, 2^{m-1} - 2^{(m-1)/2})$

| | | | | | |
|----|---|-------------------------|--------------------|-------------------------|-------|
| wt | 0 | $2^{m-1} - 2^{(m-1)/2}$ | 2^{m-1} | $2^{m-1} + 2^{(m-1)/2}$ | 2^m |
| # | 1 | $2^{m-1}(2^m - 1)$ | $2^m(2^m + 1) - 2$ | $2^{m-1}(2^m - 1)$ | 1 |

New series of 3-designs of degree 3

The new series:

$$v = 2^m$$

Points: $AG(m, 2)$

$$k = 2^{m-1} - 2^{(m-1)/2}$$

$$\lambda = 2^{(m-7)/2} \left(2^{(m-1)/2} - 2 \right) \left(2^m - 2^{(m+1)/2} - 2 \right)$$

$m \geq 5$ **odd**

$$x = 2^{(m-3)/2} \left(2^{(m-1)/2} - 3 \right)$$

$$y = 2^{(m-3)/2} \left(2^{(m-1)/2} - 2 \right)$$

Not schematic 😞

$$z = 2^{(m-3)/2} \left(2^{(m-1)/2} - 1 \right)$$

Corresponding code: $\left(2^m, 2^{2m+1}, 2^{m-1} - 2^{(m-1)/2} \right)$

| | | | | | |
|----|---|-------------------------|--------------------|-------------------------|-------|
| wt | 0 | $2^{m-1} - 2^{(m-1)/2}$ | 2^{m-1} | $2^{m-1} + 2^{(m-1)/2}$ | 2^m |
| # | 1 | $2^{m-1}(2^m - 1)$ | $2^m(2^m + 1) - 2$ | $2^{m-1}(2^m - 1)$ | 1 |

New series of 3-designs of degree 3

The new series:

$$v = 2^m$$

Points: $AG(m, 2)$

$$k = 2^{m-1} - 2^{(m-1)/2}$$

$$\lambda = 2^{(m-7)/2} \left(2^{(m-1)/2} - 2 \right) \left(2^m - 2^{(m+1)/2} - 2 \right)$$

$m \geq 5$ **odd**

$$x = 2^{(m-3)/2} \left(2^{(m-1)/2} - 3 \right)$$

$$y = 2^{(m-3)/2} \left(2^{(m-1)/2} - 2 \right)$$

Not schematic 😞

$$z = 2^{(m-3)/2} \left(2^{(m-1)/2} - 1 \right)$$

Corresponding code: $(2^m, 2^{2m+1}, 2^{m-1} - 2^{(m-1)/2})$ May be linear 😞

| | | | | | |
|----|---|-------------------------|--------------------|-------------------------|-------|
| wt | 0 | $2^{m-1} - 2^{(m-1)/2}$ | 2^{m-1} | $2^{m-1} + 2^{(m-1)/2}$ | 2^m |
| # | 1 | $2^{m-1}(2^m - 1)$ | $2^m(2^m + 1) - 2$ | $2^{m-1}(2^m - 1)$ | 1 |

Kerdock sets

Quadratic forms over $GF(2)$:

$$B(x_1, \dots, x_m) = \sum_{1 \leq i < j \leq m} b_{ij} x_i x_j \iff B = \begin{bmatrix} 0 & & b_{ij} \\ & \ddots & \\ b_{ji} & & 0 \end{bmatrix}$$

Kerdock sets

Quadratic forms over $GF(2)$:

$$B(x_1, \dots, x_m) = \sum_{1 \leq i < j \leq m} b_{ij} x_i x_j \iff B = \begin{bmatrix} 0 & & b_{ij} \\ & \ddots & \\ b_{ji} & & 0 \end{bmatrix}$$

The rank of B is even: $rk(B) = 2r$

Kerdock sets

Quadratic forms over $GF(2)$:

$$B(x_1, \dots, x_m) = \sum_{1 \leq i < j \leq m} b_{ij} x_i x_j \longleftrightarrow B = \begin{bmatrix} 0 & & b_{ij} \\ & \ddots & \\ b_{ji} & & 0 \end{bmatrix}$$

The rank of B is even: $rk(B) = 2r$

The minimum weight of the coset $B + RM(1, 2)$ is $2^{m-1} - 2^{m-1-r}$

Kerdock sets

Quadratic forms over $GF(2)$:

$$B(x_1, \dots, x_m) = \sum_{1 \leq i < j \leq m} b_{ij} x_i x_j \longleftrightarrow B = \begin{bmatrix} 0 & & b_{1j} \\ & \ddots & \\ b_{ji} & & 0 \end{bmatrix}$$

The rank of B is even: $rk(B) = 2r$

The minimum weight of the coset $B + RM(1, 2)$ is $2^{m-1} - 2^{m-1-r}$

To get a good code, we want r as large as possible: $m = 2r$ (**even!**)

Kerdock sets

Quadratic forms over $GF(2)$:

$$B(x_1, \dots, x_m) = \sum_{1 \leq i < j \leq m} b_{ij} x_i x_j \longleftrightarrow B = \begin{bmatrix} 0 & & b_{ij} \\ & \ddots & \\ b_{ji} & & 0 \end{bmatrix}$$

The rank of B is even: $rk(B) = 2r$

The minimum weight of the coset $B + RM(1, 2)$ is $2^{m-1} - 2^{m-1-r}$

To get a good code, we want r as large as possible: $m = 2r$ (**even!**)

To get many codewords, we want as many symplectic matrices B_1, \dots, B_ℓ as possible such that $rk(B_i - B_j) = m$.

Kerdock sets

Quadratic forms over $GF(2)$:

$$B(x_1, \dots, x_m) = \sum_{1 \leq i < j \leq m} b_{ij} x_i x_j \longleftrightarrow B = \begin{bmatrix} 0 & & b_{1j} \\ & \ddots & \\ b_{ji} & & 0 \end{bmatrix}$$

The rank of B is even: $rk(B) = 2r$

The minimum weight of the coset $B + RM(1, 2)$ is $2^{m-1} - 2^{m-1-r}$

To get a good code, we want r as large as possible: $m = 2r$ (**even!**)

To get many codewords, we want as many symplectic matrices B_1, \dots, B_ℓ as possible such that $rk(B_i - B_j) = m$. **Upper bound:** $\ell \leq 2^{m-1} - 1$

Kerdock sets

Quadratic forms over $GF(2)$:

$$B(x_1, \dots, x_m) = \sum_{1 \leq i < j \leq m} b_{ij} x_i x_j \longleftrightarrow B = \begin{bmatrix} 0 & & b_{1j} \\ & \ddots & \\ b_{ji} & & 0 \end{bmatrix}$$

The rank of B is even: $rk(B) = 2r$

The minimum weight of the coset $B + RM(1, 2)$ is $2^{m-1} - 2^{m-1-r}$

To get a good code, we want r as large as possible: $m = 2r$ (**even!**)

To get many codewords, we want as many symplectic matrices B_1, \dots, B_ℓ as possible such that $rk(B_i - B_j) = m$. **Upper bound:** $\ell \leq 2^{m-1} - 1$

A set of $\ell = 2^{m-1} - 1$ matrices is called a **Kerdock set** and gives rise to the Kerdock code.

Kerdock sets

Quadratic forms over $GF(2)$:

$$B(x_1, \dots, x_m) = \sum_{1 \leq i < j \leq m} b_{ij} x_i x_j \longleftrightarrow B = \begin{bmatrix} 0 & & b_{1j} \\ & \ddots & \\ b_{ji} & & 0 \end{bmatrix}$$

The rank of B is even: $rk(B) = 2r$

The minimum weight of the coset $B + RM(1, 2)$ is $2^{m-1} - 2^{m-1-r}$

To get a good code, we want r as large as possible: $m = 2r$ (**even!**)

To get many codewords, we want as many symplectic matrices B_1, \dots, B_ℓ as possible such that $rk(B_i - B_j) = m$. **Upper bound:** $\ell \leq 2^{m-1} - 1$

A set of $\ell = 2^{m-1} - 1$ matrices is called a **Kerdock set** and gives rise to the Kerdock code. **How to construct Kerdock sets?**

Kerdock sets

Quadratic forms over $GF(2)$:

$$B(x_1, \dots, x_m) = \sum_{1 \leq i < j \leq m} b_{ij} x_i x_j \longleftrightarrow B = \begin{bmatrix} 0 & & b_{1j} \\ & \ddots & \\ b_{ji} & & 0 \end{bmatrix}$$

The rank of B is even: $rk(B) = 2r$

The minimum weight of the coset $B + RM(1, 2)$ is $2^{m-1} - 2^{m-1-r}$

To get a good code, we want r as large as possible: $m = 2r$ (**even!**)

To get many codewords, we want as many symplectic matrices B_1, \dots, B_ℓ as possible such that $rk(B_i - B_j) = m$. **Upper bound:** $\ell \leq 2^{m-1} - 1$

A set of $\ell = 2^{m-1} - 1$ matrices is called a **Kerdock set** and gives rise to the Kerdock code. **How to construct Kerdock sets?**

W. M. Kantor, *Codes, quadratic forms and finite geometries*, Proc. Sympos. Appl. Math. **50** (1995), Amer. Math. Soc., 153–177.

Kerdock sets

Trace map $T : GF(2^{m-1}) \rightarrow GF(2)$, $T(x) = \sum_{i=0}^{m-2} x^{2^i}$

Kerdock sets

Trace map $T : GF(2^{m-1}) \rightarrow GF(2)$, $T(x) = \sum_{i=0}^{m-2} x^{2^i}$

Linear operator $B_s : GF(2^{m-1}) \oplus GF(2) \rightarrow GF(2^{m-1}) \oplus GF(2)$,

$$B_s(x, a) = (xs^2 + sT(sx) + as, T(sx))$$

Kerdock sets

Trace map $T : GF(2^{m-1}) \rightarrow GF(2)$, $T(x) = \sum_{i=0}^{m-2} x^{2^i}$

Linear operator $B_s : GF(2^{m-1}) \oplus GF(2) \rightarrow GF(2^{m-1}) \oplus GF(2)$,

$$B_s(x, a) = (xs^2 + sT(sx) + as, T(sx))$$

The set of matrices $\{B_s \mid s \in GF(2^{m-1}) \setminus \{0\}\}$ is a Kerdock set!

Kerdock sets

Trace map $T : GF(2^{m-1}) \rightarrow GF(2)$, $T(x) = \sum_{i=0}^{m-2} x^{2^i}$

Linear operator $B_s : GF(2^{m-1}) \oplus GF(2) \rightarrow GF(2^{m-1}) \oplus GF(2)$,

$$B_s(x, a) = (xs^2 + sT(sx) + as, T(sx))$$

The set of matrices $\{B_s \mid s \in GF(2^{m-1}) \setminus \{0\}\}$ is a Kerdock set!

A variation of this construction gives many inequivalent examples:

W. M. Kantor, *An exponential number of generalized Kerdock codes*,
Inform. and Control **53** (1982), no. 1-2, 74–80.

Kerdock sets

Trace map $T : GF(2^{m-1}) \rightarrow GF(2)$, $T(x) = \sum_{i=0}^{m-2} x^{2^i}$

Linear operator $B_s : GF(2^{m-1}) \oplus GF(2) \rightarrow GF(2^{m-1}) \oplus GF(2)$,

$$B_s(x, a) = (xs^2 + sT(sx) + as, T(sx))$$

The set of matrices $\{B_s \mid s \in GF(2^{m-1}) \setminus \{0\}\}$ is a Kerdock set!

A variation of this construction gives many inequivalent examples:

W. M. Kantor, *An exponential number of generalized Kerdock codes*,
Inform. and Control **53** (1982), no. 1-2, 74–80.

If m is **odd**, alternating matrices cannot be nonsingular (because their rank is even). Next best thing: take matrices B of rank $m - 1$, i.e. $m = 2r + 1$.

Kerdock sets in odd dimensions

For $rk(B) = m - 1$, the minimum weight of the coset $B + RM(1, 2)$ is

$$2^{m-1} - 2^{(m-1)/2} = k$$

Kerdock sets in odd dimensions

For $rk(B) = m - 1$, the minimum weight of the coset $B + RM(1, 2)$ is

$$2^{m-1} - 2^{(m-1)/2} = k$$

We want as many matrices B_1, \dots, B_ℓ as possible such that $rk(B_i - B_j) = m - 1$.

Kerdock sets in odd dimensions

For $rk(B) = m - 1$, the minimum weight of the coset $B + RM(1, 2)$ is

$$2^{m-1} - 2^{(m-1)/2} = k$$

We want as many matrices B_1, \dots, B_ℓ as possible such that $rk(B_i - B_j) = m - 1$. **Upper bound:** $\ell \leq 2^m - 1$

Kerdock sets in odd dimensions

For $rk(B) = m - 1$, the minimum weight of the coset $B + RM(1, 2)$ is

$$2^{m-1} - 2^{(m-1)/2} = k$$

We want as many matrices B_1, \dots, B_ℓ as possible such that $rk(B_i - B_j) = m - 1$. **Upper bound:** $\ell \leq 2^m - 1$

A maximal set of matrices can be obtained by a modification of Kantor's construction:

Trace map $T : GF(2^m) \rightarrow GF(2)$, $T(x) = \sum_{i=0}^{m-1} x^{2^i}$

Linear operator $B_s : GF(2^m) \rightarrow GF(2^m)$, $B_s(x) = xs^2 + sT(sx)$

The set of matrices $\{B_s \mid s \in GF(2^m) \setminus \{0\}\}$ defines the code.

Kerdock sets in odd dimensions

For $rk(B) = m - 1$, the minimum weight of the coset $B + RM(1, 2)$ is

$$2^{m-1} - 2^{(m-1)/2} = k$$

We want as many matrices B_1, \dots, B_ℓ as possible such that $rk(B_i - B_j) = m - 1$. **Upper bound:** $\ell \leq 2^m - 1$

A maximal set of matrices can be obtained by a modification of Kantor's construction:

Trace map $T : GF(2^m) \rightarrow GF(2)$, $T(x) = \sum_{i=0}^{m-1} x^{2^i}$

Linear operator $B_s : GF(2^m) \rightarrow GF(2^m)$, $B_s(x) = xs^2 + sT(sx)$

The set of matrices $\{B_s \mid s \in GF(2^m) \setminus \{0\}\}$ defines the code.

The code is nonlinear over $GF(2)$ and supports 3-designs of degree 3.

Kerdock sets in odd dimensions

For $rk(B) = m - 1$, the minimum weight of the coset $B + RM(1, 2)$ is

$$2^{m-1} - 2^{(m-1)/2} = k$$

We want as many matrices B_1, \dots, B_ℓ as possible such that $rk(B_i - B_j) = m - 1$. **Upper bound:** $\ell \leq 2^m - 1$

A maximal set of matrices can be obtained by a modification of Kantor's construction:

Trace map $T : GF(2^m) \rightarrow GF(2)$, $T(x) = \sum_{i=0}^{m-1} x^{2^i}$

Linear operator $B_s : GF(2^m) \rightarrow GF(2^m)$, $B_s(x) = xs^2 + sT(sx)$

The set of matrices $\{B_s \mid s \in GF(2^m) \setminus \{0\}\}$ defines the code.

The code is nonlinear over $GF(2)$ and supports 3-designs of degree 3.

There are also $GF(2)$ -linear codes with the same weight distribution (extended BCH codes) supporting non-isomorphic designs!

Kerdock sets in odd dimensions

J.-M. Goethals, *Nonlinear codes defined by quadratic forms over $GF(2)$* ,
Information and Control **31** (1976), no. 1, 43–74.

Kerdock sets in odd dimensions

J.-M. Goethals, *Nonlinear codes defined by quadratic forms over $GF(2)$* , *Information and Control* **31** (1976), no. 1, 43–74.

An (m, r) -set is a set $\{B_1, \dots, B_\ell\}$ of $m \times m$ alternating matrices over $GF(2)$ such that $rk(B_i - B_j) \geq 2r$.

J.-M. Goethals, *Nonlinear codes defined by quadratic forms over $GF(2)$* , Information and Control **31** (1976), no. 1, 43–74.

An (m, r) -set is a set $\{B_1, \dots, B_\ell\}$ of $m \times m$ alternating matrices over $GF(2)$ such that $rk(B_i - B_j) \geq 2r$.

E. R. Berlekamp, *The weight enumerators for certain subcodes of the second order binary Reed-Muller codes*, Information and Control **17** (1970), 485–500.

Kerdock sets in odd dimensions

J.-M. Goethals, *Nonlinear codes defined by quadratic forms over $GF(2)$* , Information and Control **31** (1976), no. 1, 43–74.

An (m, r) -set is a set $\{B_1, \dots, B_\ell\}$ of $m \times m$ alternating matrices over $GF(2)$ such that $rk(B_i - B_j) \geq 2r$.

E. R. Berlekamp, *The weight enumerators for certain subcodes of the second order binary Reed-Muller codes*, Information and Control **17** (1970), 485–500.

For odd m , the Gray maps of these codes are not \mathbb{Z}_4 -linear.

Numbers of non-isomorphic designs

| v | k | λ | x | y | z | Nd | |
|-----|-----|-----------|-----|-----|-----|-----------|--------------|
| 16 | 4 | 1 | 0 | 1 | 2 | ≥ 45 | $AG_2(4, 2)$ |
| 16 | 6 | 4 | 1 | 2 | 3 | $= 1$ | Mathon 1981 |
| 32 | 8 | 7 | 0 | 2 | 4 | ≥ 3 | $AG_3(5, 2)$ |
| 32 | 12 | 22 | 2 | 4 | 6 | ≥ 3 | |
| 64 | 16 | 35 | 0 | 4 | 8 | ≥ 1 | $AG_4(6, 2)$ |
| 64 | 28 | 156 | 10 | 12 | 14 | ≥ 1 | |
| 128 | 32 | 155 | 0 | 8 | 16 | ≥ 1 | $AG_5(7, 2)$ |
| 128 | 56 | 660 | 20 | 24 | 28 | ≥ 4 | |
| 256 | 64 | 651 | 0 | 16 | 32 | ≥ 1 | $AG_6(8, 2)$ |
| 256 | 120 | 3304 | 52 | 56 | 60 | ≥ 1 | |
| 512 | 128 | 2667 | 0 | 32 | 64 | ≥ 1 | $AG_7(9, 2)$ |
| 512 | 240 | 13384 | 104 | 112 | 120 | ≥ 4 | |

Thanks for your attention!