# Construction of $q$-analogs of Steiner systems

Alfred Wassermann

Department of Mathematics, Universität Bayreuth, Germany

joint work with M. Braun, T. Etzion, P. Östergård, A. Vardy

CanaDAM 2013, St. John's

# Outline

- $t$-designs of sets
- construction by Kramer-Mesner method
- $q$-analogs of designs
- $q$-Steiner system for $t \geq 2$

# $t$-designs (over sets)

## Definition

- $V$: set of points, $|V| = v$.
- $\mathcal{B}$: set of $k$-subsets $K$ (blocks) $\quad K \subset V$ and $|K| = k$
- $t$-$(v, k, \lambda)$ design $\mathcal{D} = (V, \mathcal{B})$:

  *Every $t$-subset $T \subset V$ is contained in exactly $\lambda$ blocks of $\mathcal{B}$.*

# $t$-designs (over sets)

## Definition

- $V$: set of points, $|V| = v$.
- $\mathcal{B}$: set of $k$-subsets $K$ (blocks) $\quad K \subset V$ and $|K| = k$
- $t$-$(v, k, \lambda)$ design $\mathcal{D} = (V, \mathcal{B})$:

  *Every $t$-subset $T \subset V$ is contained in exactly $\lambda$ blocks of $\mathcal{B}$.*

- $\lambda = 1$: Steiner system $S(t, k, v)$
- $\sigma \in S_v$ is automorphism: $\mathcal{B}^\sigma = \mathcal{B}$.

# Brute force approach for construction

- Incidence matrix between $t$-subset and $k$-subsets:

# Brute force approach for construction

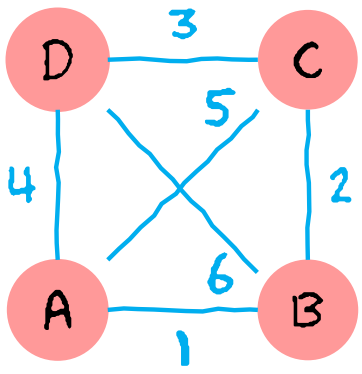
- Incidence matrix between $t$-subset and $k$-subsets:

$$M_{t,k} = (m_{i,j}), \text{ where } m_{i,j} = \begin{cases} 1 & \text{if } T_i \subset K_j \\ 0 & \text{else} \end{cases}$$

- Solve

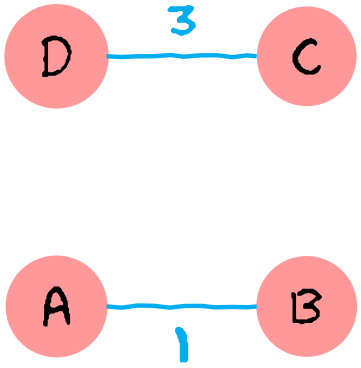
$$M_{t,k} \cdot x = \begin{pmatrix} \lambda \\ \lambda \\ \vdots \\ \lambda \end{pmatrix} \quad \text{for 0/1-vector } x$$

# Toy example

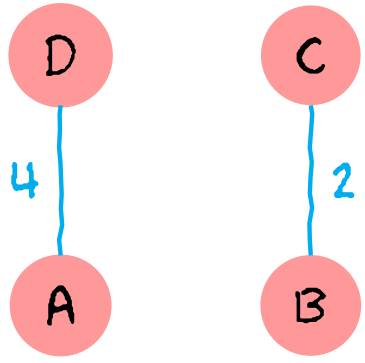



Cover every vertex (1-subset) by exactly one edge (2-subset):
1-$(4, 2, 1)$ design.

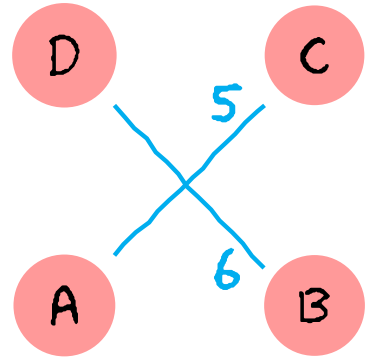
# Toy example




DESIGN 1

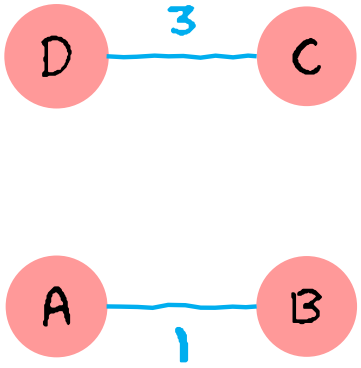



DESIGN 2

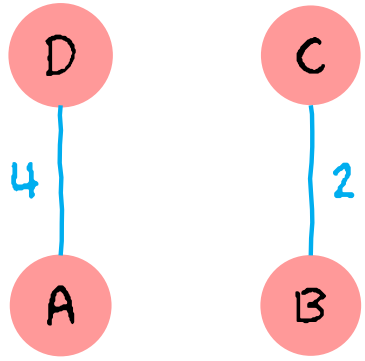



DESIGN 3

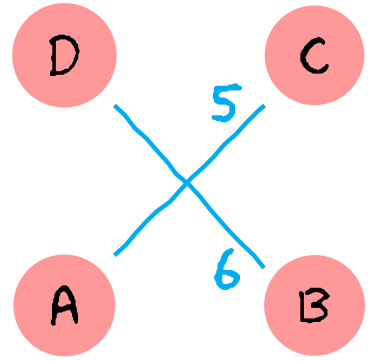
# Toy example



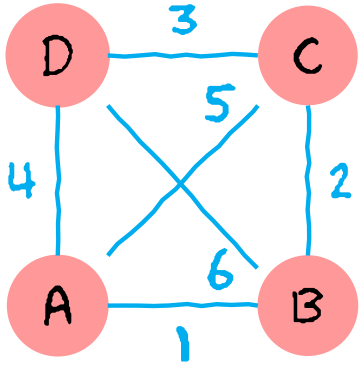

DESIGN 1




DESIGN 2

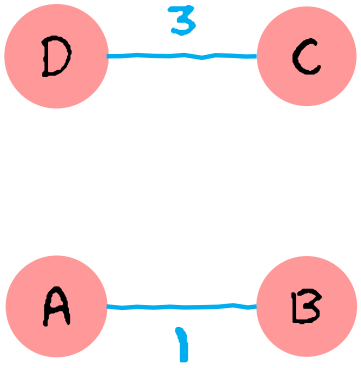



DESIGN 3

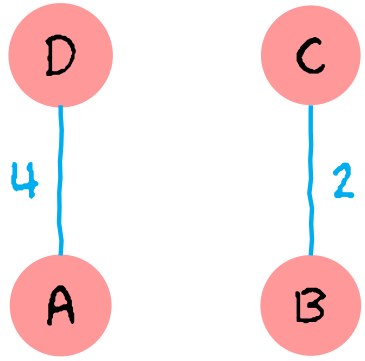



| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| A | 1 | | | 1 | 1 | |
| B | 1 | 1 | | | | 1 |
| C | | 1 | 1 | | 1 | |
| D | | | 1 | 1 | | 1 |

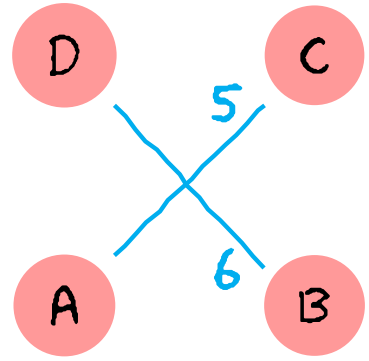
# Toy example



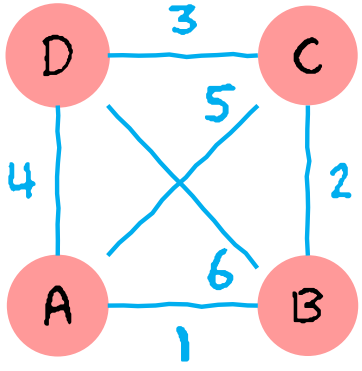

DESIGN 1




DESIGN 2




DESIGN 3




| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| A | 1 | | | 1 | 1 | |
| B | 1 | 1 | | | | 1 |
| C | | 1 | 1 | | 1 | |
| D | | | 1 | 1 | | 1 |
| DESIGN 1 | 1 | | 1 | | | |
| DESIGN 2 | | 1 | | 1 | | |
| DESIGN 3 | | | | | 1 | 1 |

# Brute force approach for construction

- $|M_{t,k}| = \binom{v}{t} \times \binom{v}{k}$

# Designs with prescribed automorphism group

Construction of designs with prescribed automorphism group

- Choose group $G$ acting on $V$, i.e. $G \leq S_v$

# Designs with prescribed automorphism group

Construction of designs with prescribed automorphism group

- Choose group $G$ acting on $V$, i.e. $G \leq S_v$
- Search for $t$-designs $\mathcal{D} = (V, \mathcal{B})$ having $G$ as **a** group of automorphisms,
  i.e. for all

$$g \in G \text{ and } K \in \mathcal{B} \Longrightarrow K^g \in \mathcal{B}.$$

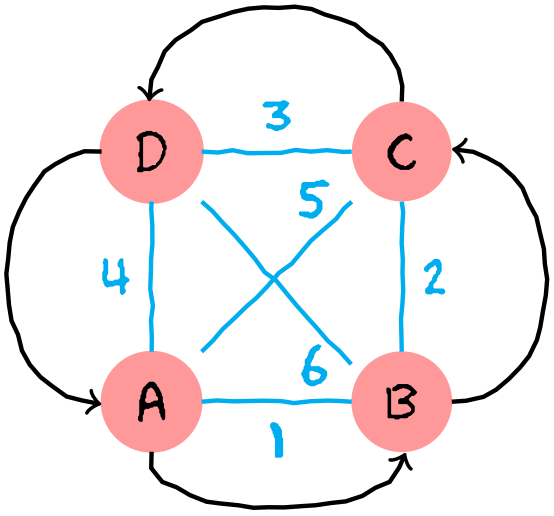
# Designs with prescribed automorphism group

Construction of designs with prescribed automorphism group

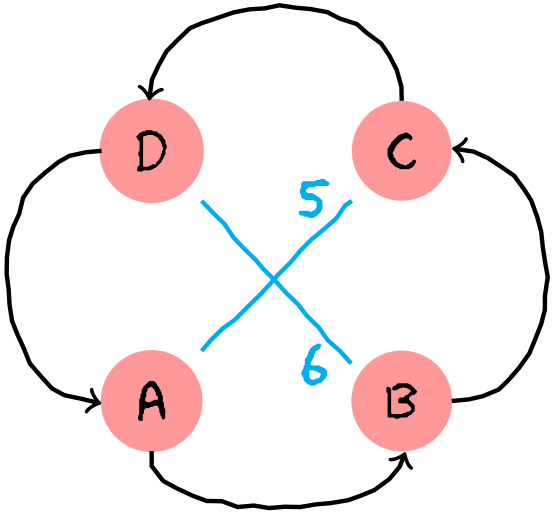
- Choose group $G$ acting on $V$, i.e. $G \leq S_v$
- Search for $t$-designs $\mathcal{D} = (V, \mathcal{B})$ having $G$ as **a** group of automorphisms,
  i.e. for all
  $$g \in G \text{ and } K \in \mathcal{B} \Longrightarrow K^g \in \mathcal{B}.$$

- Construct $\mathcal{D} = (V, \mathcal{B})$ as
  *union of orbits of $G$ on $k$-subsets.*

# Toy example: cyclic symmetry

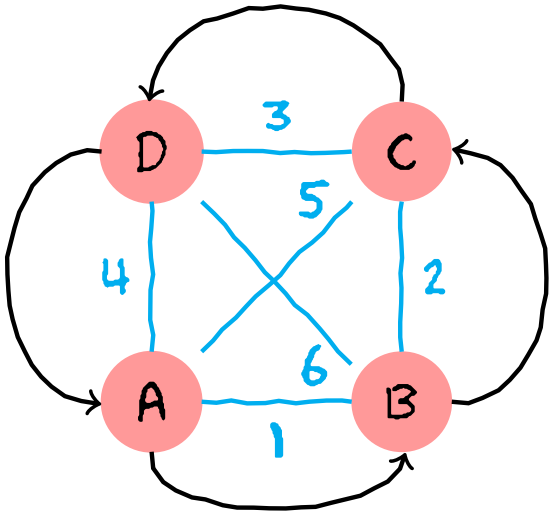



| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| A | 1 | | | 1 | 1 | |
| B | 1 | 1 | | | | 1 |
| C | | 1 | 1 | | 1 | |
| D | | | 1 | 1 | | 1 |

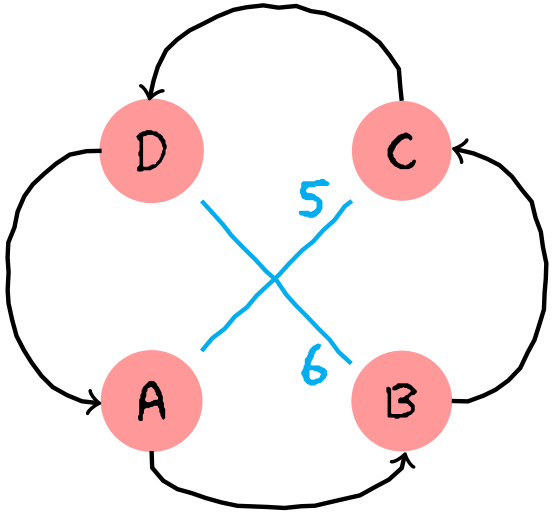



DESIGN 3

# Toy example: cyclic symmetry



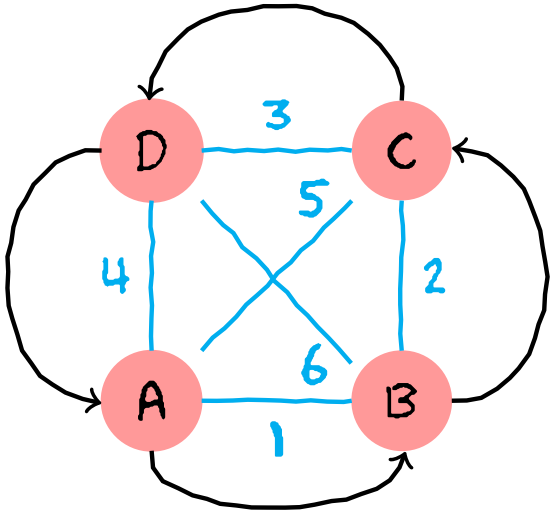

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| A | 1 | | | 1 | 1 | |
| B | 1 | 1 | | | | 1 |
| C | | 1 | 1 | | 1 | |
| D | | | 1 | 1 | | 1 |



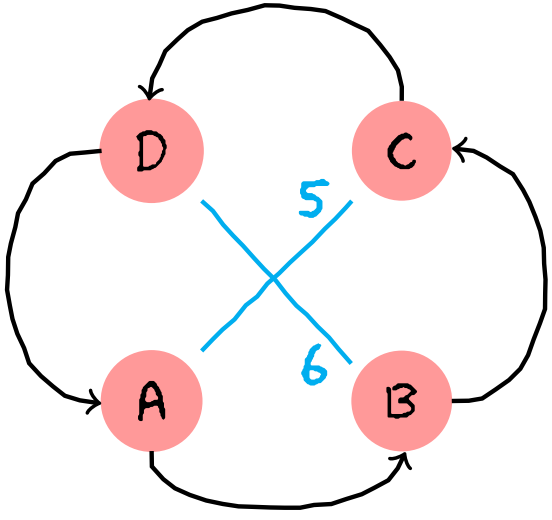

| | {1, 2, 3, 4} | {5, 6} |
|---|---|---|
| A | 2 | 1 |
| B | 2 | 1 |
| C | 2 | 1 |
| D | 2 | 1 |

DESIGN 3

# Toy example: cyclic symmetry




| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| A | 1 | | | 1 | 1 | |
| B | 1 | 1 | | | | 1 |
| C | | 1 | 1 | | 1 | |
| D | | | 1 | 1 | | 1 |




| | {1, 2, 3, 4} | {5, 6} |
|---|---|---|
| A | 2 | 1 |
| B | 2 | 1 |
| C | 2 | 1 |
| D | 2 | 1 |

| | {1, 2, 3, 4} | {5, 6} |
|---|---|---|
| {A, B, C, D} | 2 | 1 |

DESIGN 3

# The method of Kramer and Mesner

## Definition

- $K \subset V$ and $|K| = k$: $K^G := \{K^g \mid g \in G\}$
- $T \subset V$ and $|T| = t$: $T^G := \{T^g \mid g \in G\}$

# The method of Kramer and Mesner

## Definition

- $K \subset V$ and $|K| = k$: $K^G := \{K^g \mid g \in G\}$
- $T \subset V$ and $|T| = t$: $T^G := \{T^g \mid g \in G\}$
- Let

$$K_1^G \cup K_2^G \cup \ldots \cup K_n^G \subseteq \binom{V}{k}$$

and

$$T_1^G \cup T_2^G \cup \ldots \cup T_m^G = \binom{V}{t}$$

# The method of Kramer and Mesner

## Definition

- $K \subset V$ and $|K| = k$: $K^G := \{K^g \mid g \in G\}$
- $T \subset V$ and $|T| = t$: $T^G := \{T^g \mid g \in G\}$
- Let

$$K_1^G \cup K_2^G \cup \ldots \cup K_n^G \subseteq \binom{V}{k}$$

and

$$T_1^G \cup T_2^G \cup \ldots \cup T_m^G = \binom{V}{t}$$

- $$M_{t,k}^G = (m_{i,j}) \text{ where } m_{i,j} := |\{K \in K_j^G \mid T_i \subset K\}|$$

# The method of Kramer and Mesner

**Theorem (Kramer and Mesner, 1976)**

*The union of orbits corresponding to the* 1*s in a* $\{0,1\}$ *vector which solves*

$$M_{t,k}^{G} \cdot x = \begin{pmatrix} \lambda \\ \lambda \\ \vdots \\ \lambda \end{pmatrix}$$

*is a* $t$*-*$(v,k,\lambda)$ *design having* $G$ *as an automorphism group.*

# $q$-analogs of designs

- Cameron (1974), Delsarte (1976)
- Vector space $\mathbb{F}_q^n$
- $\mathcal{B}$: set of $k$-subspaces $K$ (blocks) $\quad K \subseteq \mathbb{F}_q^n$, $\dim K = k$
- $t$-$(n, k, \lambda; q)$ design over $\mathbb{F}_q$ $(\mathbb{F}_q^n, \mathcal{B})$:

  *each $t$-subspace of $\mathbb{F}_q^n$ is contained in exactly $\lambda$ blocks of $\mathcal{B}$*

# $q$-analogs of designs

- Cameron (1974), Delsarte (1976)
- Vector space $\mathbb{F}_q^n$
- $\mathcal{B}$: set of $k$-subspaces $K$ (blocks) $\quad K \subseteq \mathbb{F}_q^n$, $\dim K = k$
- $t$-$(n, k, \lambda; q)$ design over $\mathbb{F}_q$ $(\mathbb{F}_q^n, \mathcal{B})$:

  *each $t$-subspace of $\mathbb{F}_q^n$ is contained in exactly $\lambda$ blocks of $\mathcal{B}$*

- $\lambda = 1$: $q$-Steiner system $S_q[t, k, n]$
- $\sigma \in GL(n, q)$ automorphism: $\mathcal{B}^\sigma = \mathcal{B}$

# $q$-analogs of designs

- Gaussian coefficient:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

- $t$-$(n,k,\lambda;q)$ design: $|\mathcal{B}| = \lambda \frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$
- Necessary conditions:

$$\lambda_s = \lambda \frac{\begin{bmatrix} n-s \\ t-s \end{bmatrix}_q}{\begin{bmatrix} k-s \\ t-s \end{bmatrix}_q} \in \mathbb{Z} \qquad \text{for } s = 0, \ldots, t$$

- $t = 2,\ k = 3, \lambda = 1 \quad \Rightarrow \quad n \equiv 1, 3 \pmod 6$

# Geometry

- $S_q[t, k, n]$ Steiner systems are called
  - $(t, k)$-*spreads* in $\mathbb{F}_q^n$
  - $(t-1, k-1)$-systems in $PG(n, q)$
  - Ceccherini (1967), Tallini (1975)
- $t = 1$: spread in $\mathbb{F}_q^n$
- spreads ($t = 1$) exist iff $k$ divides $n$
- Metsch 1999:

  *Conjecture:* $(t, k)$*-spreads in finite vector spaces do not exist for* $t \geq 2$

# Automorphisms of $q$-analogs of designs

- $\rho$ automorphism of a $q$-analog design: $\rho \in GL(n, q)$

# Automorphisms of $q$-analogs of designs

- $\rho$ automorphism of a $q$-analog design: $\rho \in GL(n, q)$
- Singer cycle:
  - take $v \in \mathbb{F}_q^n$ as an element of $\mathbb{F}_{q^n}$
  - $(\mathbb{F}_{q^n} \setminus \{0\}, \cdot)$ is a cyclic group $G$ of order $q^n - 1$, i.e.
  - $G = \langle \sigma \rangle$
  - $G \leq GL(n, q)$ is called *Singer cycle*

# Automorphisms of $q$-analogs of designs

- $\rho$ automorphism of a $q$-analog design: $\rho \in GL(n, q)$
- Singer cycle:
  - take $v \in \mathbb{F}_q^n$ as an element of $\mathbb{F}_{q^n}$
  - $(\mathbb{F}_{q^n} \setminus \{0\}, \cdot)$ is a cyclic group $G$ of order $q^n - 1$, i.e.
  - $G = \langle \sigma \rangle$
  - $G \leq GL(n, q)$ is called *Singer cycle*
- Frobenius automorphism:
  - $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, $v \mapsto v^q$
  - $|\langle \phi \rangle| = n$

# Automorphisms of $q$-analogs of designs

- $\rho$ automorphism of a $q$-analog design: $\rho \in GL(n, q)$
- Singer cycle:
  - take $v \in \mathbb{F}_q^n$ as an element of $\mathbb{F}_{q^n}$
  - $(\mathbb{F}_{q^n} \setminus \{0\}, \cdot)$ is a cyclic group $G$ of order $q^n - 1$, i.e.
  - $G = \langle \sigma \rangle$
  - $G \leq GL(n, q)$ is called *Singer cycle*
- Frobenius automorphism:
  - $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, $v \mapsto v^q$
  - $|\langle \phi \rangle| = n$
- $|\langle \sigma, \phi \rangle| = n \cdot (q^n - 1)$
- $n$ odd prime: $\langle \sigma, \phi \rangle$ maximal subgroup in $GL(n, q)$ (Kantor, Dye)

# Known families of $q$-analogs of designs

- Thomas (1987):
  2-$(n, 3, 7; 2)$ for $n \geq 7$ and $\pm 1 \equiv n \pmod 6$
- Suzuki (1989):
  2-$(n, 3, q^2 + q + 1; q)$ for $n \geq 7$ and $\pm 1 \equiv n \pmod 6$
- Miyakawa, Munemasa, Yoshiara (1995):
  2-$(7, 3, \lambda; q)$ for $q = 2, 3$
- Itoh (1998):
  From 2-$(n, 3, q^3(q^{n-5} - 1)/(q - 1); q)$ to
  2-$(mn, 3, q^3(q^{n-5} - 1)/(q - 1); q)$

# Known $q$-analogs of designs by computer construction

Braun, Kerber, Laue (2005)

| $t$-$(n,k,\lambda;q)$ | $G$ | $\lvert M_{t,k}^G \rvert$ | $\lambda_{\max}$ | $\lambda$ |
|---|---|---|---|---|
| 3-$(8,4,\lambda;2)$ | $\langle \sigma, \phi^2 \rangle$ | $105 \times 217$ | 31 | 11, 15 |
| 2-$(10,3,\lambda;2)$ | $\langle \sigma, \phi \rangle$ | $20 \times 633$ | 255 | 15, 30, 45, 60, 75, 90, 105, 120 |
| 2-$(9,4,\lambda;2)$ | $\langle \sigma, \phi \rangle$ | $11 \times 725$ | 2667 | 21, 63, 84, 126, 147, 189, 210, 252, 273, 315, 336, 378, 399, 441, 462, 504, 525, 567, 576, 588, 630, 651, 693, 714, 756, 777, 819, 840, 882, 903, 945, 966, 1008, 1029, 1071, 1092, 1134, 1155, 1197, 1218, 1260, 1281, 1323 |
| 2-$(9,3,\lambda;2)$ | $\langle \sigma, \phi^3 \rangle$ | $31 \times 529$ | 127 | 21, 22, 42, 43, 63 |
| 2-$(8,4,\lambda;2)$ | $\langle \sigma, \phi^2 \rangle$ | $15 \times 217$ | 651 | 21, 35, 56, 70, 91, 105, 126, 140, 161, 175, 196, 210, 231, 245, 266, 280, 301, 315 |
| 2-$(8,3,\lambda;2)$ | $\langle \sigma \rangle$ | $43 \times 381$ | 63 | 21 |
| 2-$(7,3,\lambda;2)$ | $\langle \sigma \rangle$ | $21 \times 93$ | 31 | 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 |
| 2-$(6,3,\lambda;2)$ | $\langle \sigma^7 \rangle$ | $77 \times 155$ | 15 | 3, 6 |

$\sigma$: Singer cycle, $\phi$: Frobenius automorphism

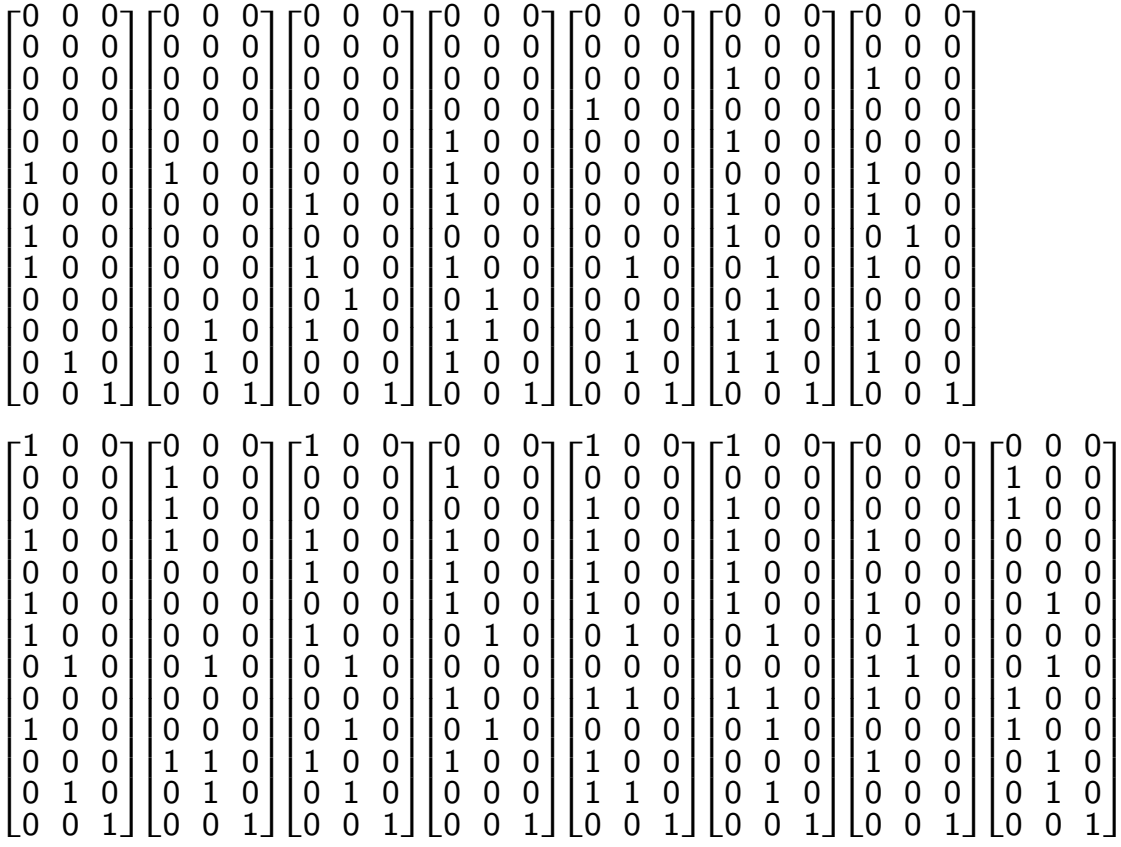
# A $S_2[2,3,13]$ $q$-Steiner system

The normalizer of the Singer cycle $G = \langle \sigma, \phi \rangle \leq GL(13,2)$ is generated by the following two matrices:

$$\phi = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1
\end{bmatrix}$$

$$\sigma = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{bmatrix}$$

# A $S_2[2,3,13]$ $q$-Steiner system



# $S_2[2, 3, 13]$

- $\begin{bmatrix} 13 \\ 3 \end{bmatrix}_2 = 3\,269\,560\,515$
- # blocks: $\begin{bmatrix} 13 \\ 2 \end{bmatrix}_2 / \begin{bmatrix} 3 \\ 2 \end{bmatrix}_2 = 1\,597\,245$
- $|G| = 13 \cdot (2^{13} - 1) = 106\,483$
- all orbits are of full length
- design consists of 15 orbits
- $$M_{2,3}^G \cdot x = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$
- $|M_{2,3}^G| = 105 \times 30\,705$
- # columns containing $0, 1$ only $= 25\,572$
- use *dancing links* by Don Knuth to solve the system

# Open problems for $S_2[2, 3, n]$

- computer free description for $S_2(2, 3, 13)$
- known: $n = 13$ is the smallest possible case having a Singer cycle as automorphism group (Computer search)
  open: Are there $S_2(2, 3, n)$ for other groups?
- $n = 7$: A $S_2(2, 3, 7)$ would consist of 381 3-spaces.
  best packing of 3-spaces: 329 (Braun, next talk)
- infinite series?

Thank you for listening !