Combinatorial Designs
Man versus Machine

Anamari Nakić

Department of Energy and Power Systems
Faculty of Electrical Engineering and Computing
University of Zagreb

Zagreb 2015

- 1850
- Thomas Kirkman
- Schoolgirls problem

Statistical experiments

- Balanced incomplete block designs

Electrical engineering

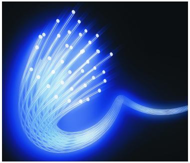
- Generalized balanced tournament designs

Fiber-optic communication

- Optical orthogonal codes

Software testing

- Covering arrays



Interconnection computer networks

- Cyclic projective planes

Cryptographic communication

- Orthogonal arrays

Theory of error-correcting codes

- Steiner systems

Agricultural engineering

- Latin squares

- Algebra
- Number theory
- Geometry

Binary Golay code

- $(24, 12, 8)$ error-correcting code

Application

- NASA deep space missions
- Radio communications

$$
\begin{bmatrix}
100000000000110101010101 \\
010000000000111010101010 \\
001000000000011101101001 \\
000100000000101110010110 \\
000010000000010111011010 \\
000001000000101011100101 \\
000000100000011001110110 \\
000000010000100110111001 \\
000000001000011010011101 \\
000000000100100101101110 \\
000000000010010110100111 \\
000000000001101001011011
\end{bmatrix}
$$

Binary Golay code can be constructed from Steiner system $5\text{-}(24, 8, 1)$.

- 1850
- Thomas Kirkman
- Schoolgirls problem

Statistical experiments

- Balanced incomplete block designs

Electrical engineering

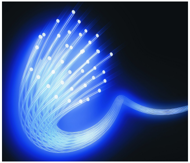
- Generalized balanced tournament designs

Fiber-optic communication

- Optical orthogonal codes

Software testing

- Covering arrays



Interconnection computer networks

- Cyclic projective planes

Cryptographic communication

- Orthogonal arrays

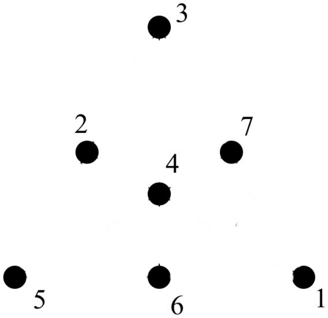
Theory of error-correcting codes

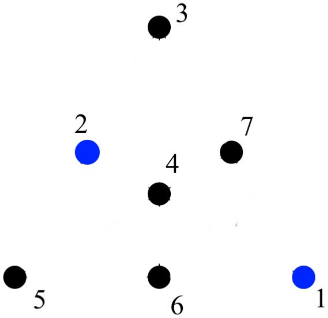
- Steiner systems

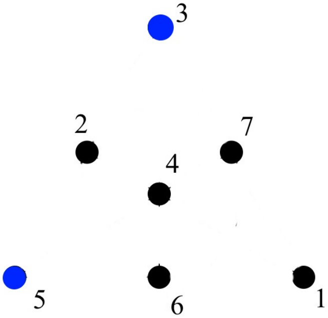
Agricultural engineering

- Latin squares

- Algebra
- Number theory
- Geometry


3
2
7
4
5
6
1


3
2
7
4
5
6
1


3
2
7
4
5
6
1

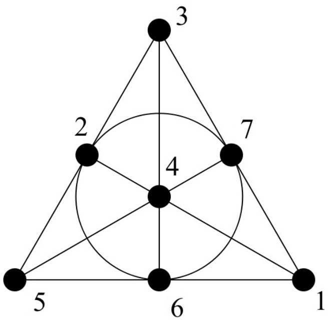
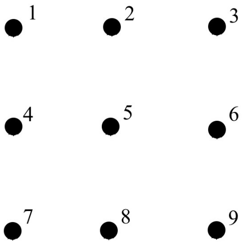
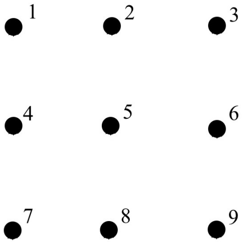


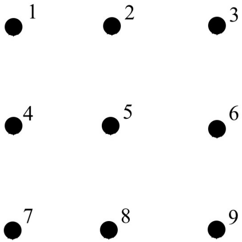
Figure: Steiner system $2\text{-}(7, 3, 1)$


1
2
3
4
5
6
7
8
9



1	2	3	1	5	9
4	5	6	2	6	7
7	8	9	3	4	8
1	4	7	1	6	8
2	5	8	2	4	9
3	6	9	3	5	7

$\mathcal{V}\ldots$



$\mathcal{B}\ldots$

1	2	3	1	5	9
4	5	6	2	6	7
7	8	9	3	4	8
1	4	7	1	6	8
2	5	8	2	4	9
3	6	9	3	5	7

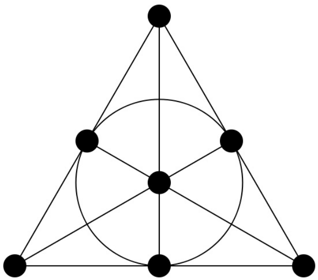


Figure: Steiner system $2\text{-}(7, 3, 1)$

Definition

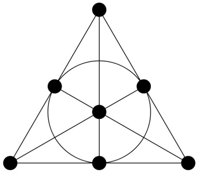
A Steiner system $2\text{-}(v, 3, 1)$ is a finite incidence structure $(\mathcal{V}, \mathcal{B})$, where

- $\mathcal{V}$ is a set of v elements called *points*,
- $\mathcal{B}$ is a set of 3-subsets of $\mathcal{V}$ called *blocks*,
- every set of 2 points is contained in precisely 1 block.

- Necessary conditions

$$\frac{v-1}{2} \text{ is integer}$$

$$\frac{v(v-1)}{6} \text{ is integer}$$



Theorem (Kirkman)

A 2-$(v,3,1)$ *Steiner triple system exists if and only if* $v \equiv 1,3 \pmod 6$.

Steiner triple systems - existence and enumeration

v	$No.$
7	1
9	1
13	13
15	80
19	11084874829
21	≥ 2160980
25	≥ 163929929318400
$\vdots$	$\vdots$

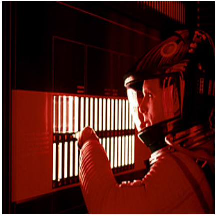
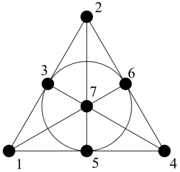
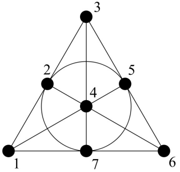


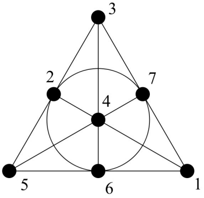
Figure: Dave vs. HAL in 2001: A Space Odyssey

- Designs $(\mathcal{V}, \mathcal{B})$ and $(\mathcal{V}, \mathcal{B}')$ are isomorphic if there exists a bijection $\alpha : \mathcal{V} \to \mathcal{V}$ such that $\alpha\mathcal{B} = \mathcal{B}'$.

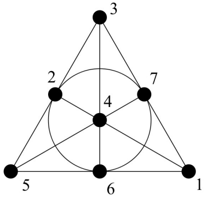


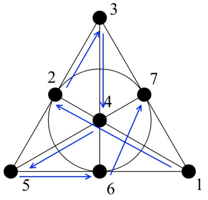


- *Automorphism* of $(\mathcal{V}, \mathcal{B})$ is a permutation $\pi : \mathcal{V} \to \mathcal{V}$ such that $\pi(\mathcal{B}) = \mathcal{B}$.
- Set of all automorphisms of a design $(\mathcal{V}, \mathcal{B})$ is a group.

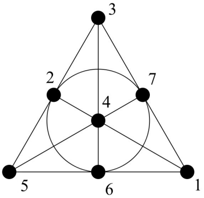


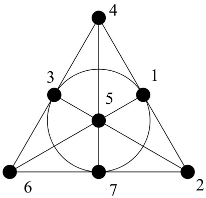
- *Automorphism* of $(\mathcal{V}, \mathcal{B})$ is a permutation $\pi : \mathcal{V} \to \mathcal{V}$ such that $\pi(\mathcal{B}) = \mathcal{B}$.
- Set of all automorphisms of a design $(\mathcal{V}, \mathcal{B})$ is a group.

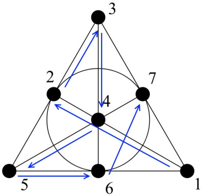




- *Automorphism* of $(\mathcal{V}, \mathcal{B})$ is a permutation $\pi : \mathcal{V} \to \mathcal{V}$ such that $\pi(\mathcal{B}) = \mathcal{B}$.
- Set of all automorphisms of a design $(\mathcal{V}, \mathcal{B})$ is a group.



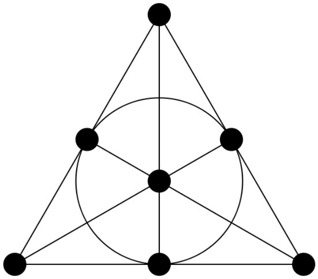




$$\pi = (1\,2\,3\,4\,5\,6\,7)$$

$$+$$

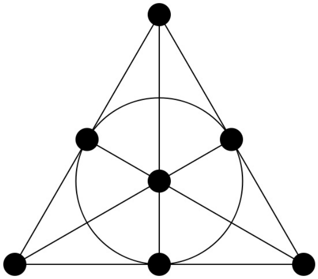
$$1 \quad 2 \quad 4$$



Definition

A Steiner system $2\text{-}(v, 3, 1)$ is a finite incidence structure $(\mathcal{V}, \mathcal{B})$, where

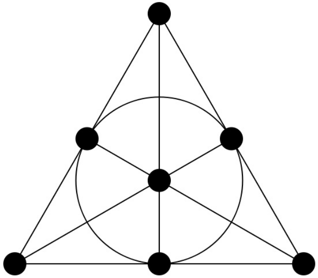
- $\mathcal{V}$ is a set of v elements called *points*,
- $\mathcal{B}$ is a set of 3-subsets of $\mathcal{V}$ called *blocks*,
- every set of 2 points is contained in precisely 1 block.



Definition

A Steiner system $2\text{-}(v, k, 1)$ is a finite incidence structure $(\mathcal{V}, \mathcal{B})$, where

- $\mathcal{V}$ is a set of v elements called *points*,
- $\mathcal{B}$ is a set of k-subsets of $\mathcal{V}$ called *blocks*,
- every set of 2 points is contained in precisely 1 block.

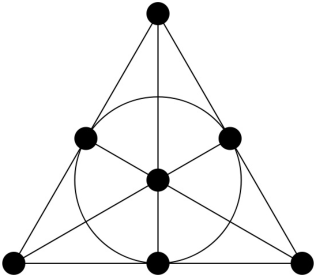


Definition

A Steiner system t-$(v, k, 1)$ is a finite incidence structure $(\mathcal{V}, \mathcal{B})$, where

- $\mathcal{V}$ is a set of v elements called *points*,
- $\mathcal{B}$ is a set of k-subsets of $\mathcal{V}$ called *blocks*,
- every set of t points is contained in precisely 1 block.

$(24, 12, 2)$ binary Golay code $\Leftrightarrow$ Steiner system 5-$(24, 8, 1)$



Definition

A Steiner system $t\text{-}(v,k,1)_q$ is a finite incidence structure $(\mathcal{V},\mathcal{B})$, where

- $\mathcal{V}$ is a vector space of dimension v over finite field $\mathbb{F}_q$,
- $\mathcal{B}$ is a set of k-dimensional subspaces of $\mathcal{V}$ called *blocks*,
- every t-dimensional subspace of $\mathcal{V}$ is contained in precisely 1 block.

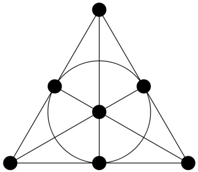
- Peter Cameron's Blog (2014)

I think that this is the most important area to attack next.

Examples.

- 1-$(v,k,1)_q$ designs
- 2-$(13,3,1)_2$ designs
- ???

- M. Braun, T. Etzion, P. Ostergard, A. Vardy, A. Wassermann
Existence of q-analogs of Steiner systems.
arXiv:1304.1462 (2013).

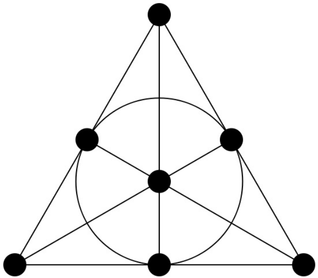


Question: does $2\text{-}(7,3,1)_q$ exist?

Theorem (Braun, Kiermaier, Nakić, 2015)

If a $2\text{-}(7,3,1)_2$ *designs exists, it is either rigid or its automorphism group is cyclic of order* 2, 3 *or* 4.

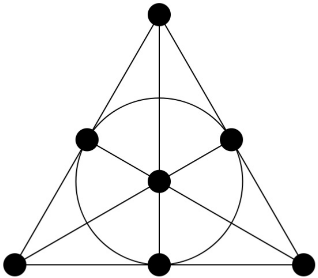
- M. Braun, M. Kiermaier, A. Nakić.
  On the automorphism group of a binary q*-analog of the Fano plane.*
  European Journal of Combinatorics, to appear (2015).



Definition

A Steiner system t-$(v, k, 1)$ is a finite incidence structure $(\mathcal{V}, \mathcal{B})$, where

- $\mathcal{V}$ is a set of v elements called *points*,
- $\mathcal{B}$ is a set of k-subsets of $\mathcal{V}$ called *blocks*,
- every set of t points is contained in precisely 1 block.



Definition

A t-(v, k, λ) design is a finite incidence structure $(\mathcal{V}, \mathcal{B})$, where

- $\mathcal{V}$ is a set of v elements called *points*,
- $\mathcal{B}$ is a set of k-subsets of $\mathcal{V}$ called *blocks*,
- every set of t points is contained in precisely λ blocks.

- Necessary conditions (integrality)

$$\lambda \frac{v-1}{k-1} \text{ is integer}$$

$$\lambda \frac{v(v-1)}{k(k-1)} \text{ is integer}$$

Figure: Gary Kasparov vs. Deep Blue

Theorem (Wilson, 1975)

For every fixed k and λ, there is a constant $C(k, \lambda)$, so that if $v > C(k, \lambda)$ and integrality conditions are satisfied, there exists a 2-(v, k, λ) design.

- R. Wilson. *An existence theory for pairwise balanced designs, III: Proof of the existence conjectures*. J. Comb. Theory A 18(1), 71–79 (1975).
- P. Keevash. *The existence of designs*. arXiv:1401.3665 (2014).

- *Handbook of Combinatorial Designs*, eds. C. Colbourn, J. Dinitz, 2007.

$t-(v,k,\lambda)$	$No.$
$2-(7,3,1)$	1
$2-(7,3,2)$	4
$2-(7,3,3)$	10
$2-(7,3,9)$	17785
$2-(8,3,6)$	3077244
$2-(8,4,3)$	4
$2-(8,4,12)$	> 2310
$2-(15,5,2)$	0
$2-(39,13,6)$	?
$2-(40,10,3)$	?
$2-(57,15,10)$	?
$2-(55,10,4)$	?
$2-(133,7,1)$	?
$2-(175,30,6)$	?
$2-(211,7,1)$	?
$2-(400,20,1)$	?
$2-(421,21,1)$	?
$\vdots$	$\vdots$

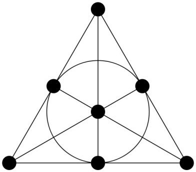
$t-(v,k,\lambda)$	$No.$
$3-(8,4,1)$	1
$3-(10,4,1)$	1
$3-(14,4,1)$	4
$3-(16,7,5)$	?
$3-(17,7,7)$	?
$3-(19,9,140)$	?
$3-(19,9,644)$	?
$3-(20,5,8)$	> 1
$4-(17,5,1)$	?
$4-(23,7,1)$	> 1
$4-(32,5,5)$	> 1
$5-(12,6,1)$	> 1
$5-(18,6,1)$	?
$5-(30,12,220)$	> 1
$5-(60,18,3060)$	> 1
$6-(19,7,1)$	?
$7-(33,8,10)$	> 1
$\vdots$	$\vdots$

- Designs $(\mathcal{V},\mathcal{B})$ and $(\mathcal{V}',\mathcal{B}')$ are isomorphic if there exists a bijection $\alpha:\mathcal{V}\to\mathcal{V}'$ such that $\alpha\mathcal{B}=\mathcal{B}'$.

Computational construction of designs

Exhaustive search

- The incidence matrix of $(\mathcal{V}, \mathcal{B})$

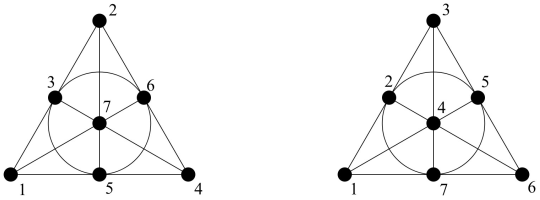


$$\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Design	Number of matrices	
$2-(7,3,1)$	$2^{7\cdot 7}$	$\approx 10^{16}$
$2-(15,3,1)$	$2^{15\cdot 35}$	$\approx 10^{175}$
$3-(16,7,5)$	$2^{16\cdot 80}$	$\approx 10^{426}$
$2-(175,30,6)$	$2^{175\cdot 210}$	$\approx 10^{12250}$

Nonexhaustive search

- *Automorphism* of a design $(\mathcal{V}, \mathcal{B})$ is a mapping $\pi : \mathcal{V} \to \mathcal{V}$ such that $\pi(\mathcal{B}) = \mathcal{B}$.
- Set of all automorphisms of a design $(\mathcal{V}, \mathcal{B})$ is a group.



Construction of designs with prescribed automorphism group:

- The Kramer-Mesner method
  E.S. Kramer, D.M. Mesner.
  t-designs on hypergraphs.
  Discret. Math. 15, 263–296 (1976).
- The method of tactical decomposition
  Z. Janko, T. van Trung.
  Construction of a new symmetric block design for (78, 22, 6) with the help of tactical decompositions.
  J. Comb. Theory A 40, 451–455 (1985).

Open problem: the existence of a 3-$(16, 7, 5)$ design

Theorem (Nakić, 2015)

If a 3-$(16, 7, 5)$ design exists, then it is either rigid or its full automorphism group is a 2-group.

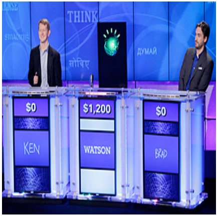
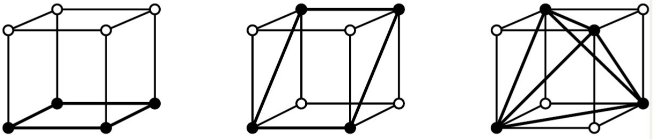


Figure: Jeopardy! Pros vs. Watson

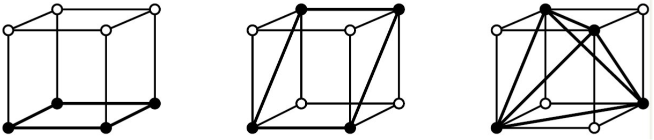
- Z. Eslami.
  On the possible automorphisms of a 3-$(16, 7, 5)$ design.
  Ars Combinatoria 95, 217-224 (2010).

- A. Nakić.
  Non-existence of a simple 3-$(16, 7, 5)$ design with an automorphism of order 3.
  Discrete Mathematics 338(4), 555-565 (2015).



- Incidence matrix

	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}	B_{12}	B_{13}	B_{14}
p_1	1	0	1	0	0	1	1	0	0	0	1	1	0	1
p_2	0	1	1	0	1	0	0	0	1	0	1	0	1	1
p_3	1	0	0	1	1	0	0	1	0	0	1	1	1	0
p_4	0	1	0	1	0	1	0	0	0	1	0	1	1	1
p_5	1	0	1	0	0	1	0	1	1	1	0	0	1	0
p_6	0	1	1	0	1	0	1	1	0	1	0	1	0	0
p_7	1	0	0	1	1	0	1	0	1	1	0	0	0	1
p_8	0	1	0	1	0	1	1	1	1	0	1	0	0	0



- Incidence matrix

	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}	B_{12}	B_{13}	B_{14}
p_1	1	0	1	0	0	1	1	0	0	0	1	1	0	1
p_2	0	1	1	0	1	0	0	0	1	0	1	0	1	1
p_3	1	0	0	1	1	0	0	1	0	0	1	1	1	0
p_4	0	1	0	1	0	1	0	0	0	1	0	1	1	1
p_5	1	0	1	0	0	1	0	1	1	1	0	0	1	0
p_6	0	1	1	0	1	0	1	1	0	1	0	1	0	0
p_7	1	0	0	1	1	0	1	0	1	1	0	0	0	1
p_8	0	1	0	1	0	1	1	1	1	0	1	0	0	0

$$[\rho_{ij}] = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 1 & 2 & 3 & 1 \end{bmatrix} \qquad [\kappa_{ij}] = \begin{bmatrix} 2 & 2 & 1 & 3 \\ 2 & 2 & 3 & 1 \end{bmatrix}$$

Tactical decomposition of designs

Definition

A *tactical decomposition* of a design $(\mathcal{V}, \mathcal{B})$ is any partition

$$\mathcal{V} = \mathcal{V}_1 \sqcup \cdots \sqcup \mathcal{V}_m, \;\; \mathcal{B} = \mathcal{B}_1 \sqcup \cdots \sqcup \mathcal{B}_n$$

with the property that there exist nonnegative integers ρ_{ij} and κ_{ij} such that

- each point of $\mathcal{V}_i$ lies in precisely ρ_{ij} blocks of $\mathcal{B}_j$,
- and each block of $\mathcal{B}_j$ contains precisely κ_{ij} points from $\mathcal{V}_i$.

Matrices $\mathcal{R} = [\rho_{ij}]$ and $\mathcal{K} = [\kappa_{ij}]$ are called *tactical decomposition matrices*.

Orbits of $\mathcal{V}$ and orbits of $\mathcal{B}$ under an action of G form a tactical decomposition of $(\mathcal{V}, \mathcal{B})$.

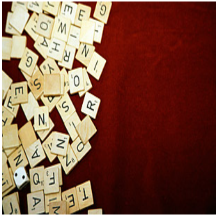


Figure: Scrabble Showdown: Quackle vs. David Boys

$$[\rho_{ij}] = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 1 & 2 & 3 & 1 \end{bmatrix} \qquad [\kappa_{ij}] = \begin{bmatrix} 2 & 2 & 1 & 3 \\ 2 & 2 & 3 & 1 \end{bmatrix}$$

$$\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow$$

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

Tactical decomposition of 2-(v, k, λ) designs

$(\mathcal{V}, \mathcal{B})$ is a 2-(v, k, λ_2) design with tactical decomposition

$$\mathcal{V} = \mathcal{V}_1 \sqcup \cdots \sqcup \mathcal{V}_m,$$

$$\mathcal{B} = \mathcal{B}_1 \sqcup \cdots \sqcup \mathcal{B}_n.$$

Figure: Terminator

$$\sum_{j=1}^{n} \rho_{lj}\kappa_{rj} = \begin{cases} \lambda_1 + (|\mathcal{V}_r| - 1)\cdot\lambda_2, & l = r, \\ |\mathcal{V}_r|\cdot\lambda_2, & l \neq r. \end{cases}$$

$$[\rho_{ij}] = \begin{bmatrix} \vdots & & \vdots \\ \rho_{l1} & \cdots & \rho_{ln} \\ \vdots & & \vdots \\ \vdots & & \vdots \end{bmatrix} \qquad [\kappa_{ij}] = \begin{bmatrix} \vdots & & \vdots \\ \vdots & & \vdots \\ \kappa_{r1} & \cdots & \kappa_{rn} \\ \vdots & & \vdots \end{bmatrix}$$

$$\sum_{j=1}^{14} \rho_{lj} \kappa_{rj} = \begin{cases} 7 + (4-1) \cdot 3, & l = r, \\ 4 \cdot 3, & l \neq r. \end{cases}$$

$$\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow$$

$$[\rho_{ij}] = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 1 & 2 & 3 & 1 \end{bmatrix} \qquad [\kappa_{ij}] = \begin{bmatrix} 2 & 2 & 1 & 3 \\ 2 & 2 & 3 & 1 \end{bmatrix}$$

$$\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow$$

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

Theorem (Krčadinac, Nakić, Pavčević, 2014)

Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ *be a* t-(v, k, λ_t) *design with tactical decomposition*

$$\mathcal{V} = \mathcal{V}_1 \sqcup \cdots \sqcup \mathcal{V}_m, \;\; \mathcal{B} = \mathcal{B}_1 \sqcup \cdots \sqcup \mathcal{B}_n.$$

Then the coefficients of $\mathcal{R} = [\rho_{ij}]$ *and* $\mathcal{K} = [\kappa_{ij}]$ *satisfy*

$$\sum_{j=1}^{n} \rho_{i_1 j} \kappa_{i_1 j}^{m_1 - 1} \kappa_{i_2 j}^{m_2} \cdots \kappa_{i_s j}^{m_s} =$$

$$\sum_{\omega_1=1}^{m_1} \sum_{\omega_2=1}^{m_2} \cdots \sum_{\omega_s=1}^{m_s} \lambda_{\omega_1+\cdots+\omega_s} \left\{ {m_1 \atop \omega_1} \right\} (|\mathcal{V}_{i_1}| - 1)_{\omega_1 - 1} \prod_{j=2}^{s} \left\{ {m_j \atop \omega_j} \right\} (|\mathcal{V}_{i_j}|)_{\omega_j}.$$

- V. Krčadinac , A. Nakić, M. O. Pavčević.
  Equations for coefficients of tactical decomposition matrices for t-designs.
  Des. Codes Cryptogr. 72(2), 465–469 (2014).

Theorem (Krčadinac, Nakić, Pavčević, 2011)

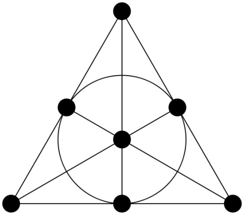
$$\sum_{j=1}^{n} \rho_{lj}\kappa_{rj} = \begin{cases} \lambda_1 + (|\mathcal{V}_r| - 1)\cdot\lambda_2, & l = r, \\ |\mathcal{V}_r|\cdot\lambda_2, & l \neq r. \end{cases}$$

$$\sum_{j=1}^{n} \rho_{lj}\kappa_{rj}\kappa_{sj} =$$

$$= \begin{cases} \lambda_1 + 3\,(|\mathcal{V}_l| - 1)\cdot\lambda_2 + (|\mathcal{V}_l| - 1)\cdot(|\mathcal{V}_l| - 2)\cdot\lambda_3, & \text{for } l = r = s, \\ |\mathcal{V}_r|\cdot|\mathcal{V}_s|\cdot\lambda_3, & \text{for } l \neq r \neq s \neq l, \\ |\mathcal{V}_s|\cdot\lambda_2 + (|\mathcal{V}_r| - 1)\cdot|\mathcal{V}_s|\cdot\lambda_3, & \text{otherwise.} \end{cases}$$

Theorem (Nakić, 2015)

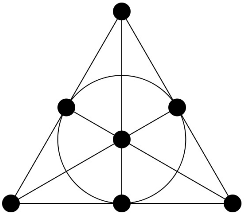
If a 3-$(16,7,5)$ design exists, then it is either rigid or its full automorphism group is a 2-group.



Definition

A t-(v, k, λ) design is a finite incidence structure $(\mathcal{V}, \mathcal{B})$, where

- $\mathcal{V}$ is a set of v elements called *points*,
- $\mathcal{B}$ is a set of k-subsets of $\mathcal{V}$ called *blocks*,
- every set of t points is contained in precisely λ blocks.



Definition

A t-(v, k, λ_t) *design over a finite field* is a pair $(\mathcal{V}, \mathcal{B})$, where

- $\mathcal{V}$ is a v-dimensional vector space over the finite field $\mathbb{F}_q$
- $\mathcal{B}$ is a set of k-dimensional subspaces of $\mathcal{V}$ called *blocks*,
- every t-dimensional subspace of $\mathcal{V}$ is contained in precisely λ blocks.

- P. Cameron. *Locally symmetric designs*. Geom. Dedicata 3, 56–76, (1974).
- P. Delsarte. *Association schemes and t-designs in regular semilattices*. J. Combin. Theory Ser. A 20(2), 230–243 (1976).

Theorem (Nakić, Pavčević, 2014)

If $(\mathcal{V}, \mathcal{B})$ *is a* 2-$(v, k, \lambda)_q$ *design with tactical decomposition*

$$\mathcal{V} = \mathcal{V}_1 \sqcup \cdots \sqcup \mathcal{V}_m, \;\; \mathcal{B} = \mathcal{B}_1 \sqcup \cdots \sqcup_n,$$

then

$$\sum_{j=1}^{n} \rho_{lj} \kappa_{rj} = \begin{cases} \lambda_1 + (|\mathcal{V}_r| - 1) \cdot \lambda_2, & l = r, \\ |\mathcal{V}_r| \cdot \lambda_2, & l \neq r. \end{cases}$$

A. Nakić, M.O. Pavčević. *Tactical decompositions of designs over finite fields*. Des Codes Crypto, DOI 10.1007/s10623-014-9988-7 (2014).

Figure: The Duel: Timo Boll vs. KUKA Robot

Tactical decomposition of 3-$(v,k,\lambda)_q$ designs

Theorem (De Boeck, Nakić, 2015)

If $(\mathcal{V},\mathcal{B})$ *is a* 3-$(v,k,\lambda)_q$ *design with tactical decomposition*

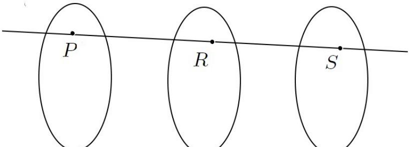
$$\mathcal{V} = \mathcal{V}_1 \sqcup \cdots \sqcup \mathcal{V}_m, \;\; \mathcal{B} = \mathcal{B}_1 \sqcup \cdots \sqcup_n,$$

then

$$\sum_{j=1}^{n} \rho_{lj}\kappa_{rj}\kappa_{sj} =$$

$$= \begin{cases} \lambda_1 + \quad \Lambda_{lrs}\cdot\lambda_2 + \quad (|\mathcal{V}_r|\cdot|\mathcal{V}_s| - \Lambda_{lrs} - 1)\cdot\lambda_3, & \text{for } l = r = s, \\ \qquad\quad \Lambda_{lrs}\cdot\lambda_2 + \quad (|\mathcal{V}_r|\cdot|\mathcal{V}_s| - \Lambda_{lrs})\cdot\lambda_3, & \text{otherwise.} \end{cases}$$

- De Boeck, Nakić: *Necessary conditions for the existence of 3-designs over finite fields with non-trivial automorphism groups.*
  Finished! (2015).



Theorem (De Boeck, Nakić, 2015)

If $(\mathcal{V},\mathcal{B})$ *is a* 3-$(v,k,\lambda)_q$ *design with tactical decomposition*

$$\mathcal{V}=\mathcal{V}_1\sqcup\cdots\sqcup\mathcal{V}_m,\ \ \mathcal{B}=\mathcal{B}_1\sqcup\cdots\sqcup_n,$$

then

$$\sum_{j=1}^{n}\rho_{lj}\kappa_{rj}\kappa_{sj}=$$

$$=\begin{cases}\lambda_1+\quad\Lambda_{lrs}\cdot\lambda_2+\quad(|\mathcal{V}_r|\cdot|\mathcal{V}_s|-\Lambda_{lrs}-1)\cdot\lambda_3, & \text{for } l=r=s,\\ \qquad\quad\Lambda_{lrs}\cdot\lambda_2+\quad(|\mathcal{V}_r|\cdot|\mathcal{V}_s|-\Lambda_{lrs})\cdot\lambda_3, & \text{otherwise.}\end{cases}$$

- De Boeck, Nakić: *Necessary conditions for the existence of 3-designs over finite fields with non-trivial automorphism groups*.
  Finished! (2015).

Open problem

Do Steiner systems 3-$(v,k,1)_q$ exist?

Some results regarding parameter Λ_{lrs}

1. $\Lambda_{lrs} = \Lambda_{lsr}$

2. $|\mathcal{V}_l| \cdot \Lambda_{lrs} = |\mathcal{V}_r| \cdot \Lambda_{rls}$

3. $$\sum_{s=1}^{m} \Lambda_{lrs} = \begin{cases} |\mathcal{V}_r| \cdot (q+1) + \frac{q^v - q^2}{q-1} - 1, & l = r, \\ |\mathcal{V}_r| \cdot (q+1), & l \neq r. \end{cases}$$

Figure: Bladerunner

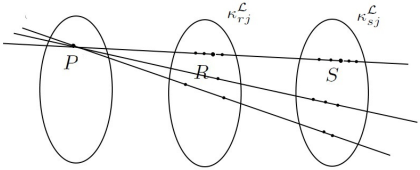
Lemma

The set of 2*-subspaces of* $\mathbb{F}_q^v$ *is a* $2-(v,2,1)_q$ *design* $(\mathcal{V},\mathcal{L})$*. Group* $G \leq P\Gamma L(\mathbb{F}_q^v)$ *acts on* $(\mathcal{V},\mathcal{L})$ *inducing tactical decomposition*

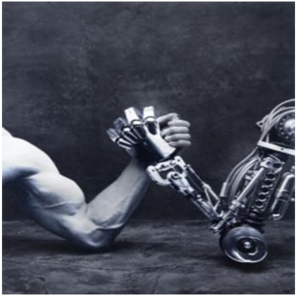
$$\mathcal{V} = \mathcal{V}_1 \sqcup \cdots \sqcup \mathcal{V}_m, \qquad \mathcal{L} = \mathcal{L}_1 \sqcup \cdots \sqcup \mathcal{L}_\omega$$

with tactical decomposition matrices $[\rho_{ij}^{\mathcal{L}}]$ *and* $[\kappa_{ij}^{\mathcal{L}}]$*. Then*

$$\Lambda_{lrs} = \begin{cases} \sum_{j=1}^{\omega} \rho_{lj}^{\mathcal{L}} \kappa_{rj}^{\mathcal{L}} \kappa_{sj}^{\mathcal{L}} - \lambda_1^{\mathcal{L}}, & \text{for } l = r = s, \\ \sum_{j=1}^{\omega} \rho_{lj}^{\mathcal{L}} \kappa_{rj}^{\mathcal{L}} \kappa_{sj}^{\mathcal{L}}, & \text{otherwise.} \end{cases}$$



Thank you for your attention!



But they are useless. They can only give you answers.
Pablo Picasso