On designs and Steiner systems over finite fields

Alfred Wassermann

Department of Mathematics, Universität Bayreuth, Germany

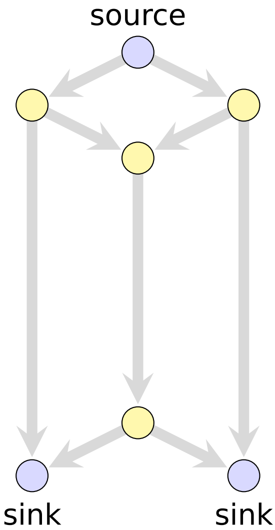
Special Days on
Combinatorial Construction Using Finite Fields,
Linz 2013

Outline

- Network coding
- Design theory
- Symmetry
- Computer construction
- Projective geometry
- New results
  (joint work with M. Braun, T. Etzion, A. Kohnert, P. Östergård, A. Vardy)
- Summary

Network coding

Flow network



- directed graph, with sources and sinks
- each edge e has a capacity c_e
- each edge receives a non-negative flow $f_e \leq c_e$
- the net flow into any non-source non-sink vertex is zero

In the following:

- $c_e = 1$
- $f_e \in \{0, 1\}$

Flow networks

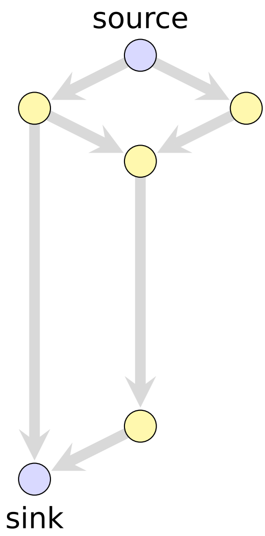
Theorem (Ford, Fulkerson 1956, Elias, Feinstein, Shannon 1956)

In a flow network, the maximum amount of flow passing from a source s to a sink t is equal to the minimum capacity, which when removed, separates s from t.

Theorem (Menger 1927)

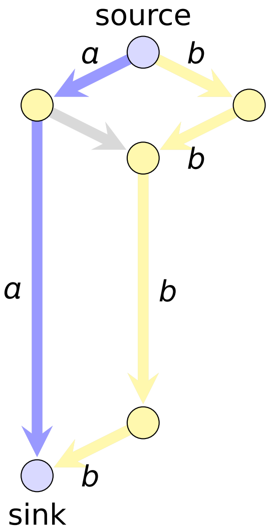
Maximum number of edge-disjoint paths from s to t in a directed graph is equal to the minimum s-t cut.

Example: 1 source, 1 sink



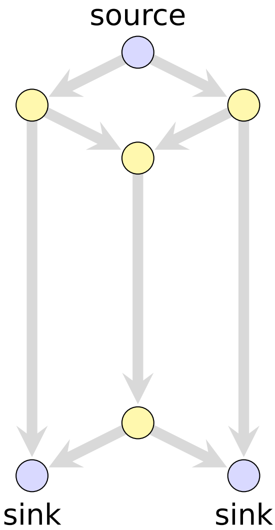
- cut-capacity $= 2$
- min-cut $= 2 =$ max-flow
- Menger's theorem: two edge-disjoint paths
- route packets a and b along these paths

Example: 1 source, 1 sink



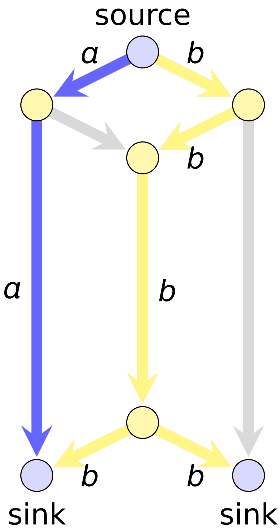
- cut-capacity $= 2$
- min-cut $= 2 =$ max-flow
- Menger's theorem: two edge-disjoint paths
- route packets a and b along these paths

Example: 1 source, 2 sinks



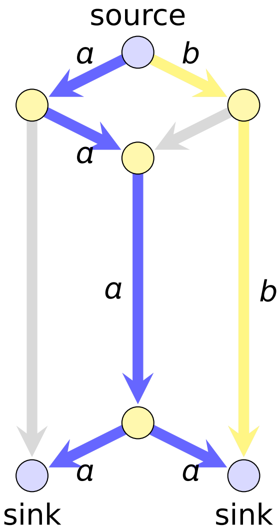
- cut-capacity $= 2$
- can route 2 packets to one sink, 1 packet to the other
- and vice-versa
- Time-sharing between these two strategies can achieve a multicast rate of 1.5 packets per use of the network.

Example: 1 source, 2 sinks



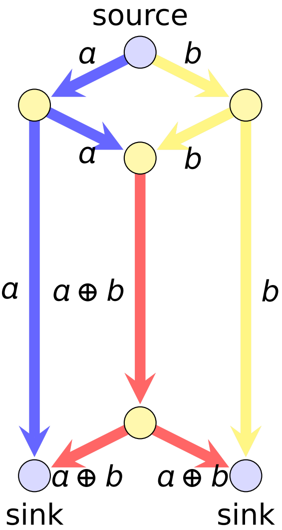
- cut-capacity $= 2$
- can route 2 packets to one sink, 1 packet to the other
- and vice-versa
- Time-sharing between these two strategies can achieve a multicast rate of 1.5 packets per use of the network.

Example: 1 source, 2 sinks



- cut-capacity $= 2$
- can route 2 packets to one sink, 1 packet to the other
- and vice-versa
- Time-sharing between these two strategies can achieve a multicast rate of 1.5 packets per use of the network.

Example: 1 source, 2 sinks



- perform coding at the bottle-neck
- a and b are packets of bits
- $a \oplus b = a + b$ over $\mathbb{F}_2$
- $a \oplus (a \oplus b) = b$
  $b \oplus (a \oplus b) = a$
- both sinks can recover both messages
- Network coding achieves a multicast rate of 2 packets per use of the network
- best possible

Network coding – essence

- R. Ahlswede, N. Cai, S.-Y. R. Li, R. W. Yeung 2000
- packets can be mixed with each other – rather than just routed or replicated
- a higher throughput can be achieved

Error correction in noncoherent network coding

R. Kötter

F. Kschischang

- Kötter, Kschischang (2008)
- Silva, Kötter, Kschischang (2008)

Error correction in noncoherent network coding

Possible error sources:

- Random errors that could not be detected at the physical layer
- Corrupt packets injected at the application level by a malicious user

Error correction in noncoherent network coding

Possible error sources:

- Random errors that could not be detected at the physical layer
- Corrupt packets injected at the application level by a malicious user

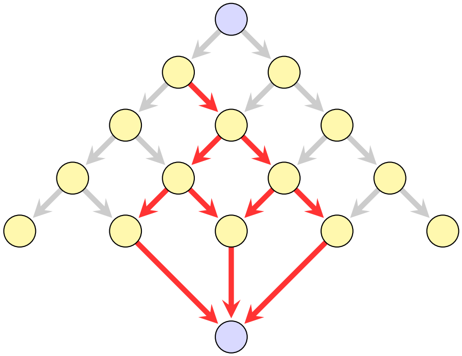
Local view at routing node:

- Randomly combine incoming packets linearly
- A corrupt packet is modeled as the addition of an error packet to a genuine packet

$$P_i^{(\text{out})} = \sum_{j=1}^{m} a_{ij} P_j^{(\text{in})} + E_i$$

Error propagation

- Packet mixing makes network coding highly prone to error propagation. This essentially rules out classical error correction.



Error correction in noncoherent network coding

Global view:

- The overall network can be viewed as a point-to-point channel
- Source: $X = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_k \end{pmatrix}$ sink: $Y = \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_{k'} \end{pmatrix}$
- $X_i, Y_j \in \mathbb{F}_q^v$
- Transmission:

$$X \quad \mapsto \quad Y = A \cdot X + B \cdot E,$$

where A, B, E are unknown

Key observation

$$X \quad \longmapsto \quad Y = A \cdot X + B \cdot E$$

In case $E = 0$:

$$X \quad \longmapsto \quad Y = A \cdot X$$

rows of $A \cdot X \quad \in \quad \langle X_1, X_2, \ldots, X_k \rangle \quad (=$ row space of $X)$

Random linear network coding

- Randomly combine information vectors at intermediate nodes
- Codewords are subspaces of a finite vector space
- Convenient: all codewords have same dimension k

Network codes

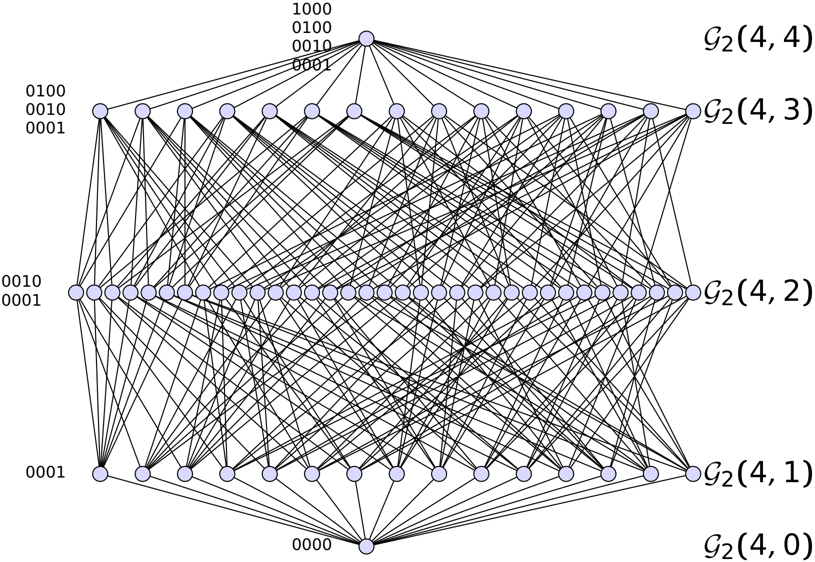
- ambient space $\mathcal{V} = \mathbb{F}_q^v$
- constant dimension (network) code:

$$\mathcal{C} \subseteq \{U \le \mathbb{F}_q^v : \dim U = k\}$$

- Grassmannian: $\mathcal{G}_q(v,k) := \{U \le \mathbb{F}_q^v : \dim U = k\}$

H. Graßmann

Subspace lattice of $\mathbb{F}_2^4$



Subspace lattice

- $|\mathcal{G}_q(v,k)| = \begin{bmatrix} v \\ k \end{bmatrix}_q$
- Gaussian coefficient:

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

- $\lim_{q\to 1} \begin{bmatrix} v \\ k \end{bmatrix}_q = \binom{v}{k}$

Subspace distance

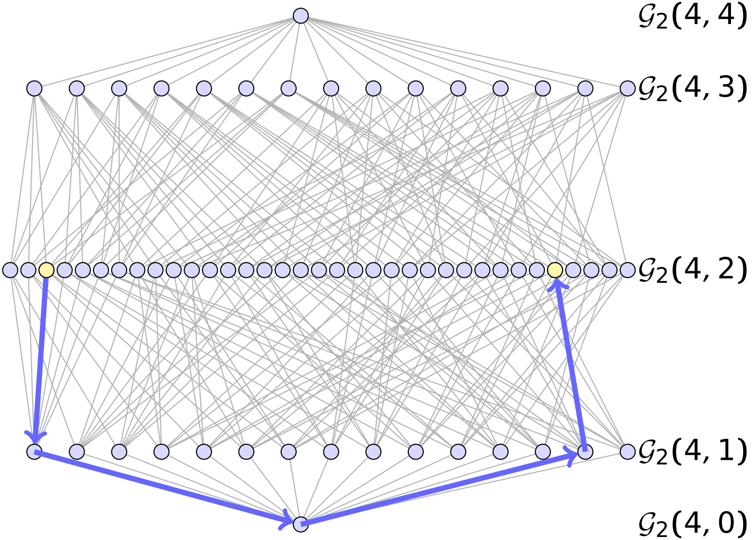
- subspace distance for $U, V \in \mathcal{G}_q(v,k)$

$$\begin{aligned} d(U,V) &= \dim U + \dim V - 2\dim U \cap V \\ &= 2k - 2\dim U \cap V \\ &=: 2\delta \end{aligned}$$

- minimum distance

$$d(\mathcal{C}) := \min\{d(U,V) : U, V \in \mathcal{C}, U \neq V\}$$

Subspace distance in $\mathbb{F}_2^4$



Problems

- maximize $|\mathcal{C}|$ for given v, k, d
- determine upper and lower bounds for

$$A_q(v,k,d) := \max\{|\mathcal{C}| : \mathcal{C} \subseteq \mathcal{G}_q(v,k), d(\mathcal{C}) \ge d\}$$

Upper bounds

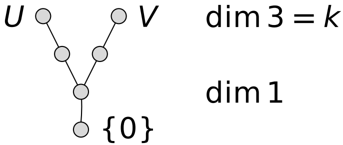
- Sphere packing bound: $A_q(v,k,2\delta) \le \dfrac{|\mathcal{G}_q(v,k)|}{|B_k(\delta-1)|}$
- Singleton bound: $A_q(v,k,2\delta) \le \begin{bmatrix} v-\delta+1 \\ k-\delta+1 \end{bmatrix}_q$
- Anticode bound:
  - Anticode of diameter e: set of subspaces $U \in \mathcal{G}_q(v,k)$ such that all pairwise distances are $\le e$
  - $A_q(v,k,2\delta) \le \dfrac{\begin{bmatrix} v \\ k \end{bmatrix}_q}{\begin{bmatrix} v-k+\delta-1 \\ \delta-1 \end{bmatrix}_q} = \dfrac{\begin{bmatrix} v \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q}$
- Johnson type bounds:

$$A_q(v,k,2\delta) \le \left\lfloor \frac{q^v-1}{q^k-1} \cdot A_q(v-1,k-1,2\delta) \right\rfloor$$

Previous bounds for $A_2(v, 3, 4)$

v	$\geq$	$\leq$	Ref
6	77	81	[K]
7	329	381	[B]
8	1312	1493	[B]
9	5694	6205	[E]
10	21483	24698	[K]
11	92411	99718	[B]
12	385515	398385	[B]
13	1490762	1597245	
14	5996178	6387029	[B]

- [K] Kohnert, Kurz (2008)
- [E] Etzion, Vardy (2008)
- [B] Braun, Reichelt (2013)

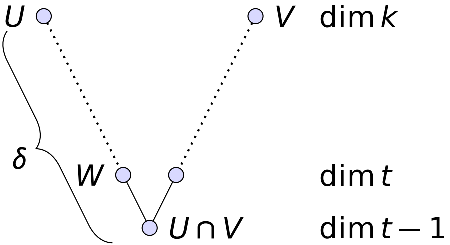


Constant dimension codes

- $U, V \in \mathcal{G}_q(v, k)$:

$$d(U, V) = 2k - 2\dim U \cap V = 2\delta$$

- Let $t - 1 := k - \delta$



- $d(\mathcal{C}) = 2\delta$:

$$\dim U \cap V \leq t - 1 \quad \text{for all } U, V \in \mathcal{C}, U \neq V$$

- For all $W \in \mathcal{G}_q(v, t)$:

$$|\{U \in \mathcal{C} : W \leq U\}| \leq 1$$

Extremal case

- $\mathcal{C} \subseteq \mathcal{G}_q(v,k)$
- For all $W \in \mathcal{G}_q(v,t)$:

$$|\{U \in \mathcal{C} : W \leq U\}| \leq 1$$

Extremal case

- $\mathcal{C} \subseteq \mathcal{G}_q(v,k)$
- For all $W \in \mathcal{G}_q(v,t)$:

$$|\{U \in \mathcal{C} : W \leq U\}| \leq 1$$

- Extremal case: for all $W \in \mathcal{G}_q(v,t)$

$$|\{U \in \mathcal{C} : W \leq U\}| = 1$$

Extremal case

- $\mathcal{C} \subseteq \mathcal{G}_q(v,k)$
- For all $W \in \mathcal{G}_q(v,t)$:

$$|\{U \in \mathcal{C} : W \leq U\}| \leq 1$$

- Extremal case: for all $W \in \mathcal{G}_q(v,t)$

$$|\{U \in \mathcal{C} : W \leq U\}| = 1$$

- In this case, $|\mathcal{C}|$ meets anticode bound and Johnson bound:

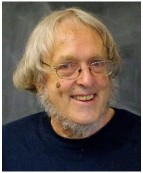
$$|\mathcal{C}| = \frac{\begin{bmatrix} v \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q} = \frac{\begin{bmatrix} v \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q}$$

- $\mathcal{C}$: perfect diameter code

Design theory

Design theory

- Cameron (1974), Delsarte (1976)

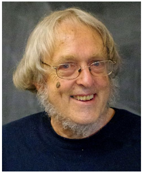


P. Cameron

- $\mathcal{B} \subseteq \mathcal{G}_q(v, k)$: set of k-subspaces (blocks)
- $(\mathbb{F}_q^v, \mathcal{B})$: q-Steiner system $S_q[t, k, v]$

  each t-subspace of $\mathbb{F}_q^v$ is contained in exactly one block of $\mathcal{B}$

Design theory



P. Cameron

- Cameron (1974), Delsarte (1976)

- $\mathcal{B} \subseteq \mathcal{G}_q(v, k)$: set of k-subspaces (blocks)
- $(\mathbb{F}_q^v, \mathcal{B})$: q-Steiner system $S_q[t, k, v]$

  each t-subspace of $\mathbb{F}_q^v$ is contained in exactly one block of $\mathcal{B}$

More general:

- $\mathcal{B} \subseteq \mathcal{G}_q(v, k)$: set of k-subspaces (blocks)
- $(\mathbb{F}_q^v, \mathcal{B})$: t-$(v, k, \lambda; q)$ design over $\mathbb{F}_q$

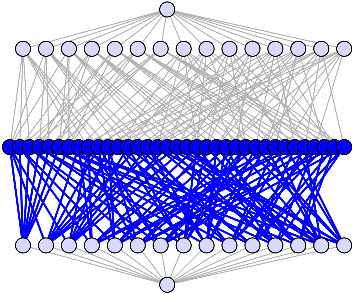
  each t-subspace of $\mathbb{F}_q^v$ is contained in exactly λ blocks of $\mathcal{B}$

Design theory

- $\mathcal{B}$ set: simple design
- $\mathcal{B}$ multiset: non-simple design

Design theory

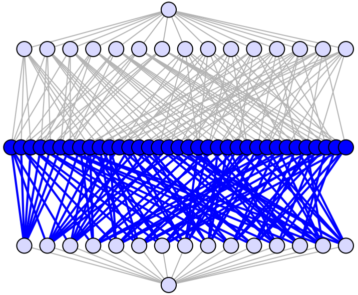
- $\mathcal{B}$ set: simple design
- $\mathcal{B}$ multiset: non-simple design
- $\mathcal{B} = \mathcal{G}_q(v, k)$ is a t-$(v, k, \begin{bmatrix} v-t \\ k-t \end{bmatrix}_q; q)$ design: trivial design



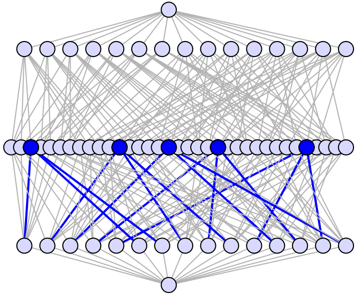
trivial 1-$(4, 2, 7; 2)$ design

Design theory

- $\mathcal{B}$ set: simple design
- $\mathcal{B}$ multiset: non-simple design
- $\mathcal{B} = \mathcal{G}_q(v,k)$ is a t-$(v,k,\begin{bmatrix} v-t \\ k-t \end{bmatrix}_q;q)$ design: trivial design



trivial 1-$(4,2,7;2)$ design



1-$(4,2,1;2)$ design

t-$(v, k, \lambda; q)$ designs

- $|\mathcal{B}| = \lambda \frac{\begin{bmatrix} v \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$
- Necessary conditions:

$$\lambda_i = \lambda \frac{\begin{bmatrix} v-i \\ t-i \end{bmatrix}_q}{\begin{bmatrix} k-i \\ t-i \end{bmatrix}_q} \in \mathbb{Z} \qquad \text{for } i = 0, \ldots, t$$

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

Related design parameters

t-$(v, k, \lambda; q)$ design $\rightarrow$

- supplemented design: t-$\left(v, k, \begin{bmatrix} v-t \\ k-t \end{bmatrix}_q - \lambda; q\right)$
- complementary design: t-$\left(v, v-k, \lambda \begin{bmatrix} v-t \\ k \end{bmatrix}_q / \begin{bmatrix} v-t \\ k-t \end{bmatrix}_q; q\right)$
- reduced design: $(t-1)$-$\left(v, k, \lambda \begin{bmatrix} v-t+1 \\ 1 \end{bmatrix}_q / \begin{bmatrix} k-t+1 \\ 1 \end{bmatrix}_q; q\right)$
- derived design: $(t-1)$-$(v-1, k-1, \lambda; q)$
- residual design: $(t-1)$-$\left(v-1, k, \lambda \frac{q^{v-k}-1}{q^{v-t+1}-1}; q\right)$
  Kiermaier, Laue (2013)
- Open problem: $t \rightarrow (t+1)$?

t-designs (over sets)

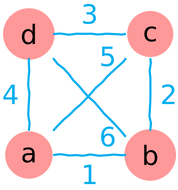
- $\mathcal{V}$: set of points, $|\mathcal{V}| = v$.
- $\mathcal{B}$: set of k-subsets K (blocks) $\quad K \subseteq \mathcal{V}$ and $|K| = k$
- $(\mathcal{V}, \mathcal{B})$: t-(v, k, λ) design

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

- t-$(v, k, 1)$ design: Steiner system $S(t, k, v)$
-    

J. Plücker	T. Kirkman	J. Steiner	R. Fisher
1835	1844	1853	1926

Example

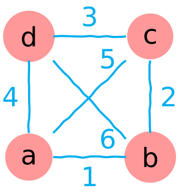


Task:

Cover every vertex (1-subset) by exactly one edge (2-subset):

1-$(4, 2, 1)$ *design*

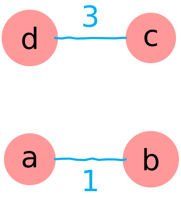
Example



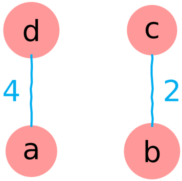
Task:

Cover every vertex (1-subset) by exactly one edge (2-subset):

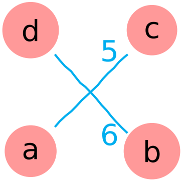
$1\text{-}(4, 2, 1)$ *design*



design 1



design 2



design 3

t-designs (over sets)

- designs over finite fields are also called q-analogs
- related design parameters
- $t \rightarrow (t+1)$ Ajoodani-Namini (1996)

“Large sets” of designs (over sets)

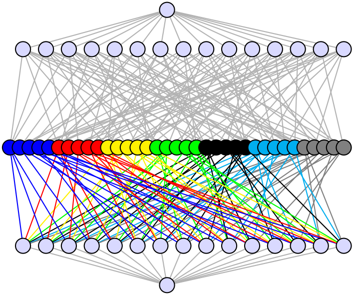
- the set of all k-subsets is a t-$(v, k, \binom{v-t}{k-t})$ design: trivial design
- a partition of the trivial design into N disjoint t-(v, k, λ) designs is called large set

$$LS[N](t, k, v)$$

- $N \cdot \lambda = \binom{v-t}{k-t}$
- Sylvester (1860): “packing”
- “large set of disjoint designs”, Lindner, Rosa (1975)

Large sets of designs over finite fields

- $\mathcal{G}_q(v,k)$ is a t-$(v,k,\begin{bmatrix}n-t\\k-t\end{bmatrix}_q;q)$ design
- Large set $LS_q[N](t,k,v)$: partition of $\mathcal{G}_q(v,k)$ into N disjoint t-$(v,k,\lambda;q)$ designs



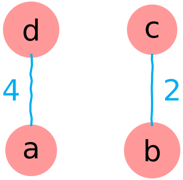
$LS_2[7](1,2,4)$

- Necessary: $N\cdot\lambda=\begin{bmatrix}v-t\\k-t\end{bmatrix}_q$

Symmetry

Automorphisms

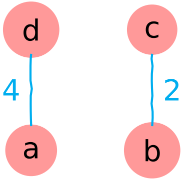
Designs over sets:

- S_v: symmetric group
- $\sigma \in S_v$ is automorphism: $\mathcal{B}^\sigma = \mathcal{B}$
- Example: 

$\sigma = (ad)(bc)$
- Set of automorphisms: automorphism group

Automorphisms

Designs over sets:

- S_v: symmetric group
- $\sigma \in S_v$ is automorphism: $\mathcal{B}^\sigma = \mathcal{B}$
- Example:  $\sigma = (ad)(bc)$

- Set of automorphisms: automorphism group

Designs over finite fields:

- $\mathrm{P\Gamma L}(v, q)$ projective semilinear group
- $GL(v, q) = \{M \in \mathbb{F}_q^{v \times v} : M \text{ invertible}\}$
- $\sigma \in \mathrm{P\Gamma L}(v, q)$ automorphism: $\mathcal{B}^\sigma = \mathcal{B}$

Automorphisms of designs over finite fields

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

  (Kantor 1980, Dye 1989)

Computer construction

Brute force approach for construction

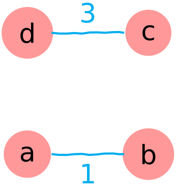
- incidence matrix between t-subset and k-subsets:

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

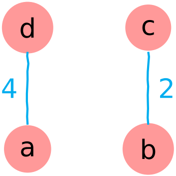
- solve

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

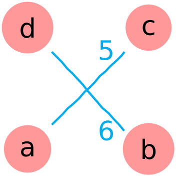
Example



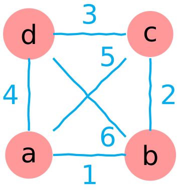
design 1



design 2



design 3



$M_{1,2}$	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

Designs with prescribed automorphism group

Construction of designs with prescribed automorphism group

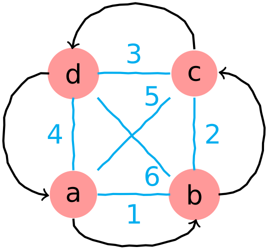
- choose group G acting on $\mathcal{V}$, i.e. $G \leq S_v$
- search for t-designs $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ having G as a group of automorphisms,
  i.e. for all

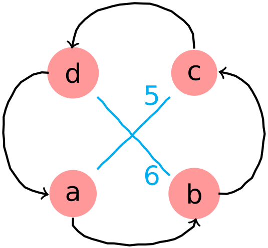
$$g \in G \text{ and } K \in \mathcal{B} \Longrightarrow K^g \in \mathcal{B}.$$

- construct $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ as

  union of orbits of G on k-subsets.

Example: cyclic symmetry





design 3

	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

The method of Kramer and Mesner

Definition

- $K \subset \mathcal{V}$ and $|K| = k$: $K^G := \{K^g \mid g \in G\}$
- $T \subset \mathcal{V}$ and $|T| = t$: $T^G := \{T^g \mid g \in G\}$
- Let
$$K_1^G \cup K_2^G \cup \ldots \cup K_n^G \subseteq \binom{\mathcal{V}}{k}$$
and
$$T_1^G \cup T_2^G \cup \ldots \cup T_m^G = \binom{\mathcal{V}}{t}$$
- $$M_{t,k}^G = (m_{i,j}) \text{ where } m_{i,j} := |\{K \in K_j^G \mid T_i \subset K\}|$$

The method of Kramer and Mesner

Theorem (Kramer and Mesner, 1976)

The union of orbits corresponding to the $1s$ *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,λ) *design having* G *as an automorphism group.*

Expected gain

- Brute force approach: $|M_{t,k}| = \binom{v}{t} \times \binom{v}{k}$
- Kramer-Mesner: $|M_{t,k}^G| \approx \frac{\binom{v}{t}}{|G|} \times \frac{\binom{v}{k}}{|G|}$

Solving algorithms

t-designs with $\lambda > 1$:

- integer programming (CPLEX, Gurobi)
- lattice basis reduction + exhaustive enumeration (W. 1998, 2002)
- heuristic algorithms

t-designs with $\lambda = 1$:

- maximum clique algorithms (Östergård: cliquer)
- exact cover (Knuth: dancing links)

Applications of Kramer-Mesner in Bayreuth

(Betten, Braun, Kerber, Kiermaier, Kohnert, Kurz, Laue, W., Vogel, Zwanzger)

- designs over sets
- designs over finite fields
- large sets of designs
- linear codes
- self-orthogonal codes
- ring-linear codes
- two-weight codes
- arcs, blocking sets in projective geometry

Known designs over finite fields

Families of designs

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

Designs over $\mathbb{F}_2$ by computer construction

Braun, Kerber, Laue (2005), S. Braun (2010)

t-$(v,k,\lambda;q)$	G	$\lvert M_{t,k}^G \rvert$	$\lambda_{\max}$	λ
3-$(8,4,\lambda;2)$	$\langle\sigma,\phi^2\rangle$	105×217	31	11, 15
2-$(10,3,\lambda;2)$	$\langle\sigma,\phi\rangle$	20×633	255	15, 30, 45, 60, 75, 90, 105, 120
2-$(9,4,\lambda;2)$	$\langle\sigma,\phi\rangle$	11×725	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-$(9,3,\lambda;2)$	$\langle\sigma,\phi^3\rangle$	31×529	127	21, 22, 42, 43, 63
2-$(8,4,\lambda;2)$	$\langle\sigma,\phi^2\rangle$	15×217	651	21, 35, 56, 70, 91, 105, 126, 140, 161, 175, 196, 210, 231, 245, 266, 280, 301, 315
2-$(8,3,\lambda;2)$	$\langle\sigma\rangle$	43×381	63	21
2-$(7,3,\lambda;2)$	$\langle\sigma\rangle$	21×93	31	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
2-$(6,3,\lambda;2)$	$\langle\sigma^7\rangle$	77×155	15	3, 6

σ: Singer cycle, ϕ: Frobenius automorphism

Projective geometry

Projective geometry

- projective space $PG(v-1,q)$
- spread in $PG(v-1,q)$: set of lines that partitions the points, i.e. $S_q[1,2,v]$

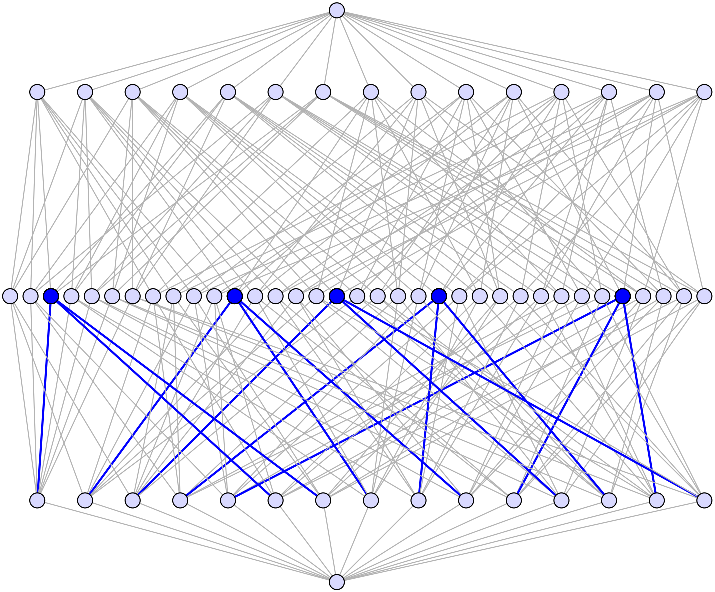
Projective geometry

- projective space $PG(v-1,q)$
- spread in $PG(v-1,q)$: set of lines that partitions the points, i.e. $S_q[1,2,v]$
- $(k-1)$-spread in $PG(v-1,q)$: $S_q[1,k,v]$
- $(k-1)$-spreads exist iff k divides v

Projective geometry

- projective space $PG(v-1,q)$
- spread in $PG(v-1,q)$: set of lines that partitions the points, i.e. $S_q[1,2,v]$
- $(k-1)$-spread in $PG(v-1,q)$: $S_q[1,k,v]$
- $(k-1)$-spreads exist iff k divides v
- $(t-1,k-1)$-spreads in $PG(v-1,q)$: $S_q[t,k,v]$
- also called $(t,k-1)$-systems in $PG(v,q)$,
  Ceccherini (1967), Tallini (1975)

Projective geometry – spreads



Projective geometry – spreads

- Motivation: André, Bose, Bruck construction (1954):
  spreads $\rightarrow$ translation planes
- Spread codes and spread decoding in network codes (Manganiello, Gorla, Rosenthal 2008)
- Large set of spreads: parallelism, packing

Projective geometry – (s, r)-spreads

- Beutelspacher 1978:

  "Es scheint unbekannt zu sein, ob in einem endlichen projektiven Raum der Dimension d eine (s, r)-Faserung existieren kann, wenn $0 < s < r < d$ gilt."

- Conjecture (Metsch 1999):

  "(s, r)-spreads in finite projective spaces do not exist for $s > 0$."

Projective geometry – (s, r)-spreads

“(s, r)-spreads in finite projective spaces do not exist for $s > 0$.”

translates to

“$S_q[t, k, v]$ Steiner systems over finite fields do not exist for $t > 1$.”

New results

$S_2[2,3,13]$ does exist[1]

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

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

[1] Braun, Etzion, Östergård, Vardy, W. (2013) submitted

$S_2[2, 3, 13]$

- $\begin{bmatrix} 13 \\ 3 \end{bmatrix}_2 = 3\,269\,560\,515$
- # blocks: $\begin{bmatrix} 13 \\ 2 \end{bmatrix}_2 / \begin{bmatrix} 3 \\ 2 \end{bmatrix}_2 = 1\,597\,245$
- Kramer-Mesner with group $G = \langle \phi, \sigma \rangle$

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

- $|G| = 13 \cdot (2^{13} - 1) = 106\,483$
- all orbits are of full length $|G|$

$S_2[2,3,13]$

- Kramer-Mesner matrix

$$M^G_{2,3} \cdot x = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

- $|M^G_{2,3}| = 105 \times 30\,705$
- # columns containing $0, 1$ only $= 25\,572$
- use dancing links by Knuth to solve the system
- up to now:
  - ≥ 1030 non-isomorphic solutions
  - ≥ 630 disjoint solutions
  - i.e. 2-$(13, 3, \lambda; 2)$ exist for $\lambda = 1, 2, \ldots, 630$

Why Singer cycle + Frobenius?

Transitive designs:

- A group G acts t-transitively on a vector space V if the set of t-subspaces is a single orbit.

Theorem (Cameron, Kantor 1979)

If $G \leq GL(v, q)$ is t-transitive with $t \geq 2$ then G is also k-transitive for $t < k \leq v$.

Miyakawa, Munemasa, Yoshiara 1995

Theorem (Hering 1974, Liebeck 1987)

If $G \le GL(v, q)$ acts transitively on the 1-subspaces of $\mathbb{F}_q^v$ with $v \ge 6$, then one of the following holds:

- $G \le \langle \sigma, \phi \rangle$
- $SL_a(q^{n/a}) \trianglelefteq G$, *where* $a \mid v$, $a \le 2$
- $Sp_{2a}(q^{v/2a}) \trianglelefteq G$, *where* $2a \mid v$
- $G_2(q^{v/6}) \trianglelefteq G < Sp_6(q^{v/6})$, *where* $q = 2^m$ *and* $6 \mid v$
- *few sporadic cases for* $v = 6$

The first large sets for $t \geq 2$

- $LS_2[3](2, 3, 8)$ does exist[2]
  - Consists of three disjoint 2-$(8, 3, 21; 2)$ designs
  - Group: Singer cycle in $GL(8, 2)$ of order 255
  - $LS_2[3](2, 5, 8)$ does exist (complementary design)
- $LS_3[2](2, 3, 6)$ does exist
  - Consists of two disjoint 2-$(6, 3, 20; 3)$ designs
- $LS_5[2](2, 3, 6)$ does exist
  - Consists of two disjoint 2-$(6, 3, 20; 5)$ designs

---

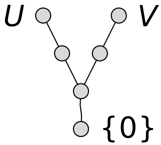
[2] Braun, Kohnert, Östergård, W. (2013) submitted

Summary

Bounds for $A_2(v, 3, 4)$

v	$\geq$	$\leq$	Ref
6	77	~~81~~ 77	[K], [H]
7	329	381	[B]
8	1312	1493	[B]
9	5694	6205	[E]
10	21483	24698	[K]
11	92411	99718	[B]
12	385515	398385	[B]
13	1597245	1597245	
14	5996178	6387029	[B]

- [K] Kohnert, Kurz (2008)
- [E] Etzion, Vardy (2008)
- [B] Braun, Reichelt (2013)
- [H] Honold, Kiermaier, Kurz (2013)



$\dim 3 = k$
$\dim 2 = t$
$\dim 1$

Designs over sets vs. finite fields

designs over sets	designs over finite fields
constructions for $t \leq 9$	constructions for $t = 2, 3$
designs exist for all t (Teirlinck 1986)	designs exist for all t (Fazely, Lovett, Vardy 2013)
t-design $\to$ $(t+1)$-designs	?
Steiner systems are known for $t \leq 5$ $t > 5$?	Steiner systems are known for $t = 1$ (k-spreads) and $S_2[2, 3, 13]$
$S(2, 3, v)$ direct constructions	?
recursive constructions: $S(2, 3, v) \to S(2, 3, 2v + 1)$ $S(2, 3, v) \to S(2, 3, 3v)$ $S(2, 3, v), S(2, 3, w) \to S(2, 3, v \cdot w)$	?

Open problems

- 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 $S_2[2,3,v]$ for other groups?
- $S_2[2,3,7]$?
- Infinite series?
- *Problems on q-Analogs in Coding Theory*, T. Etzion (2013)

Thank you for listening !