Aalto University
School of Science
and Technology

Coding Theory on Non-Standard Alphabets

Random network codes in projective geometries

Marcus Greferath

Department of Mathematics and Systems Analysis
Aalto University School of Sciences
marcus.greferath@aalto.fi

May 2023

What is the connection to coding?

Definition: For a vector space ${}_F V$ define a metric δ on the lattice of subspaces $L({}_F V)$ by:

$$\delta : L({}_F V) \times L({}_F V) \longrightarrow \mathbb{R}, \quad (X, Y) \mapsto \dim(X + Y) - \dim(X \cap Y)$$

- It is not difficult to verify the metric properties (strictly positive, symmetric, triangle inequality).
- Using the dimension formula, we can rewrite

$$\delta(X, Y) \;=\; \dim(X) + \dim(Y) - 2\dim(X \cap Y).$$

- Restricting δ to the Grassmannian $\left[{V \atop k}\right]_q$ we finally see

$$\delta(X, Y) \;=\; 2\,k - 2\dim(X \cap Y).$$

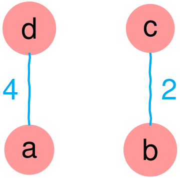
What is the connection to coding?

Definition: Let V be a v-dimensional vector space over the q-element field F. A subset $C \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is called a subspace code with parameters $(v, d; k)_q$, if d is the minimum distance of C.

- If $C \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is a $t-(v, k, 1)_q$ design (q-analog of Steiner system), then two distinct blocks of C can intersect in a subspace of dimension at most $t-1$.
- This comes from the fact that the two blocks would be forced to be identical, if the intersection were t-dimensional.
- For this reason, if every $T \in \begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in at most one block of C, then C becomes a $(v, 2(k-t+1); k)_q$ subspace code.

Automorphisms

Designs over sets:

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

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

Subspace designs:

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

Brute force approach for construction

Step 1: Build matrix

- Designs over sets: incidence matrix between t-subset T_i and k-subsets K_j:

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

- Subspace designs: incidence matrix between t-subspaces T_i and k-subspaces K_j:

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

- $|M_{t,k}| = \begin{bmatrix} v \\ t \end{bmatrix}_q \times \begin{bmatrix} v \\ k \end{bmatrix}_q$

Brute force approach for construction

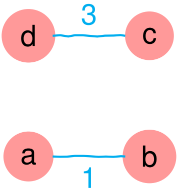
Step 2: Solve system of Diophantine linear equations

- Solve

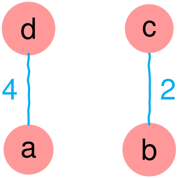
$$M_{t,k} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \lambda \\ \lambda \\ \vdots \\ \lambda \end{bmatrix}$$

Here $x = [x_1, \ldots, x_n]^T$ is a binary vector.

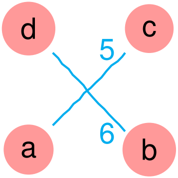
Example



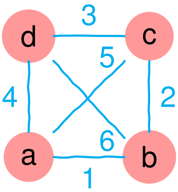
design 1



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

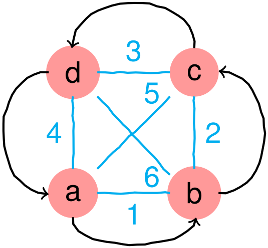
Construction of designs with prescribed automorphism group:

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

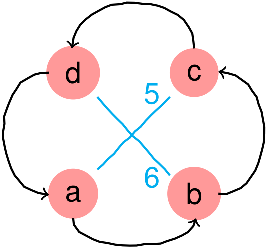
$$\text{for all } g \in G \text{ and } K \in \mathcal{B} \Longrightarrow K^g \in \mathcal{B}$$

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

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

	{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

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

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*

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

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

Expected gain

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

Applications of Kramer-Mesner

mostly by Betten, Braun, Kerber, Kiermaier, Kohnert, Kurz, Laue, Vogel, Wassermann, Zwanzger at Bayreuth University

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

Solving algorithms

t-designs with $\lambda = 1$:

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

t-designs with $\lambda > 1$:

- integer programming (CPLEX, Gurobi)
- heuristic algorithms
- Logic programming
- Gröbner bases
- lattice basis reduction $+$ exhaustive enumeration (Wassermann 1998, 2002)

Subspace designs by computer construction ($q = 2, t \geq 2$)

Braun, Kerber, Laue (2005), S. Braun (2010), Braun, Etzion, Östergård, Vardy, Wassermann (2013), M. Braun (2015)

t-$(v, k, \lambda; q)$	$\lvert M_{t,k}^G \rvert$	λ
3-$(8, 4, \lambda; 2)$	105×217	11, 15
2-$(13, 3, \lambda; 2)$	105×30705	1, . . . , 2047
2-$(11, 3, \lambda; 2)$	31×2263	245, 252
2-$(10, 3, \lambda; 2)$	20×633	15, 30, 45, 60, 75, 90, 105, 120
2-$(9, 4, \lambda; 2)$	11×725	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-$(9, 3, \lambda; 2)$	31×529	21, 22, 42, 43, 63
	28×408	7, 12, 19, 24, 31, 36, 43, 48, 55, 60
	40×460	49
2-$(8, 4, \lambda; 2)$	15×217	21, 35, 56, 70, 91, 105, 126, 140, 161, 175, 196, 210, 231, 245, 266, 280, 301, 315
	13×231	7, 14, 49, 56, 63, 98, 105, 112, 147, 154, 161 196, 203, 210, 245, 252, 259, 294, 301, 308
2-$(8, 3, \lambda; 2)$	43×381	21
2-$(7, 3, \lambda; 2)$	21×93	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
2-$(6, 3, \lambda; 2)$	77×155	3, 6

All beside $2\text{-}(13, 3, \lambda; 2)$ were found by `solvediophant`

Back to the (binary) Fano plane

Does a $2\text{-}(7, 3, 1; q)$ design exist for $q \geq 2$?

Theorem (Braun, Kiermaier, Nakić (2016))

A binary Fano plane can have four non-trivial automorphism groups: One group of order 2, two groups of order 3, one group of order 4.

Theorem (Kiermaier, Kurz, Wassermann (2016))

The order of the automorphism group of a binary q-analog of the Fano plane is at most two.

Thanks to M. Kiermaier and A. Wassermann for their material and kind assistance in composing this tutorial