Aalto University
School of Science
and Technology

Coding Theory on Non-Standard Alphabets

Random network codes in projective geometries

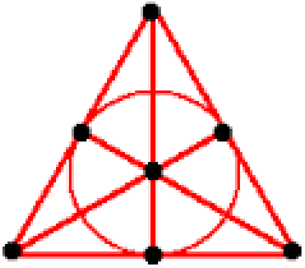
Marcus Greferath

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

May 2023

Subspace Designs for Network Coding

- Have you prviously seen this figure?



- One of the best known images in Discrete Mathematics
- It is an illustration of the so-called Fano plane.

Projective Geometry

The Fano plane is the smallest non-trivial example of what is called a projective space. These geometries are incidence structures (P, G) consisting of points and lines, such that the following 3 axioms are satisfied:

- Any two (distinct) points are contained in a unique line.
- If a line intersects with two sides of a triangle (but not in the vertices), then it will also intersect with the third side.
- There are at least 4 points, no 3 of which are on a common line.

Projective Geometry

A large class of projective spaces comes from vector spaces: Let V be a vector space of dimension at least 3 over the field $\mathbb{F}$. Define (P, G) by

- $P := \{U \leq V \mid \dim(U) = 1\}$
- $G := \{U \leq V \mid \dim(U) = 2\}$

Then the pair (P, G) indeed satisfies the above 3 axioms.

More-over, if $V = \mathbb{F}_2^3$, then the above image of the Fano plane describes the structure of (P, G).

Projective Geometry

Finally, there is a notion of dimension, that arises as follows:

- A subspace is a subset A of P such that with every two points $p, q \in A$ the entire line spanned by p and q will be also contained in A.
- It can be seen that arbitrary intersections of subspaces again form subspaces.
- If B is an arbitrary subset of P, then

  $$[B] := \bigcap \{B \subseteq A \subseteq P \mid A \text{ subspace}\},$$

  i.e. the smallest subspace containing B is called the subspace generated by B.

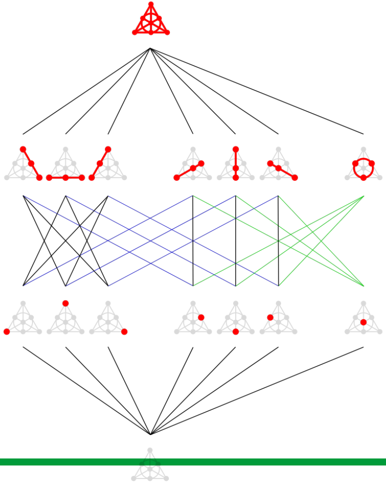
Projective Geometry

The dimension of a subspace A is then the size of the smallest subset generating A, reduced by 1. This way, we have the following further concepts:

- Singletons are the subspaces of dimension 0.
- Lines are subspaces of dimension 1.
- Planes are subspaces of dimension 2.
- $\ldots$
- Hyperplanes are subspaces of dimension $n-1$, provided the given projective space is of dimension n.

Projective Geometry

The set of all subspaces of a projective space (P, G), partially ordered by set inclusion, is called the projective geometry of (P, G).



Subset lattice

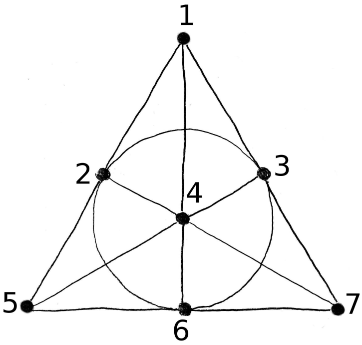
- Let X be a v-element set.
- $\binom{X}{k} :=$ Set of all k-subsets of X.
- $\#\binom{X}{k} = \binom{v}{k}$.
- Subsets of X form a Boolean lattice (wrt. $\subseteq$).

Definition

$D \subseteq \binom{X}{k}$ is a t-(v, k, λ) (block) design if each $T \in \binom{X}{t}$ is contained in exactly λ blocks (elements of D).

- If $\lambda = 1$: D is called a Steiner system
- For $\lambda = 1, t = 2, k = 3$, D is referred to as a Steiner triple system STS(v)

Example



$$X = \{1, 2, 3, 4, 5, 6, 7\}, \quad D = \{\{1, 2, 5\}, \{1, 4, 6\}$$
$$\{1, 3, 7\}, \{2, 3, 6\}, \{2, 4, 7\}, \{3, 4, 5\}, \{5, 6, 7\}\}$$

Fano plane D is a 2-$(7, 3, 1)$ design, i.e an $\mathrm{STS}(7)$.

Lemma

Let D be a t-(v, k, λ) design and $i \in \{0, \ldots, t\}$. Then D is also an i-(v, k, λ_i) design with

$$\lambda_i = \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}} \cdot \lambda. \qquad \text{In particular, } \#D = \lambda_0$$

Example

Fano plane STS(7) ($v = 7$, $k = 3$, $t = 2$, $\lambda = 1$):

$$\lambda_2 = 1, \quad \lambda_1 = 3, \quad \lambda_0 = 7$$

Corollary: Integrality conditions

If a t-(v, k, λ) design exists, then $\lambda_0, \lambda_1, \ldots, \lambda_t \in \mathbb{Z}$, i.e. all these Parameters must be admissible.

Remark

All finite projective spaces are Steiner systems. The underlying 2-designs have parameters $(\frac{q^n-1}{q-1}, q+1, 1)$. Here q is the number of elements in the finite field, and n is the dimension of the vector space.

Lemma

STS(v) admissible $\iff v \equiv 1, 3 \pmod 6$.

STS(v) for small v

- Fano plane STS(7) is smallest (non-trivial) example.
- Next admissible case is STS(9) which exists as affine plane of order 3.

Theorem (Kirkman 1847)

All admissible STS(v) do exist.

Subspace lattice

- Let V be a v-dimensional $\mathbb{F}_q$ vector space.
- Grassmannian $\begin{bmatrix} V \\ k \end{bmatrix}_q :=$ Set of all k-dim. subspaces of V.
- Gaussian Binomial coefficient

$$\#\begin{bmatrix} V \\ k \end{bmatrix}_q = \begin{bmatrix} v \\ k \end{bmatrix}_q = \frac{(q^v-1)(q^{v-1}-1)\cdot\ldots\cdot(q^{v-k+1}-1)}{(q-1)(q^2-1)\cdot\ldots\cdot(q^k-1)}$$

- Subspace lattice of V = projective geometry $\mathrm{PG}(v-1,q)$
  - Elements of $\begin{bmatrix} V \\ 1 \end{bmatrix}_q$ are points.
  - Elements of $\begin{bmatrix} V \\ 2 \end{bmatrix}_q$ are lines.
  - Elements of $\begin{bmatrix} V \\ 3 \end{bmatrix}_q$ are planes.
  - Elements of $\begin{bmatrix} V \\ v-1 \end{bmatrix}_q$ are hyperplanes.

How to obtain q-analogs in combinatorics?

Replace subset lattice by subspace lattice!

traditional	q-analog
v-element set X	v-dim. $\mathbb{F}_q$ vector space V
$\binom{V}{k}$	$\begin{bmatrix} V \\ k \end{bmatrix}_q$
$\binom{v}{k}$	$\begin{bmatrix} v \\ k \end{bmatrix}_q$
cardinality	dimension
$\cap$	$\cap$
$\cup$	$+$

- The subset lattice corresponds to the limit when $q \to 1$.
- A groaner: This comes from the unary field $\mathbb{F}_1$.

What is the definition of a q-analog of a design?

We follow the above recipe and make the transit from sets to vector spaces:

Definition (subspace design)

Let V be a v-dimensional $\mathbb{F}_q$ vector space. $D \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is a t-$(v, k, \lambda)_q$ (subspace) design if each $T \in \begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in exactly λ elements of D.

- If $\lambda = 1$: D is called a q-Steiner system
- If $\lambda = 1$, $t = 2$, $k = 3$: D is referred to as q-Steiner triple system $\mathrm{STS}_q(v)$
- Geometrically, the $\mathrm{STS}_q(v)$ is a set of planes in $\mathrm{PG}(v-1, q)$ which cover each line exactly once.

Lemma

Let D be a t-$(v, k, \lambda)_q$ design and $i \in \{0, \ldots, t\}$. Then D is also an i-$(v, k, \lambda_i)_q$ design with

$$\lambda_i = \frac{\begin{bmatrix} v-i \\ t-i \end{bmatrix}_q}{\begin{bmatrix} k-i \\ t-i \end{bmatrix}_q} \cdot \lambda. \quad \text{In particular, } \#D = \lambda_0.$$

Corollary: Integrality conditions

If a t-$(v, k, \lambda)_q$ design exists, then $\lambda_0, \lambda_1, \ldots, \lambda_t \in \mathbb{Z}$, i.e. all of these Parameters must be admissible.

Lemma

$\mathrm{STS}_q(v)$ admissible $\iff v \equiv 1, 3 \pmod 6$.

$\mathrm{STS}_q(v)$ for small v

- The famous q-analog of the Fano plane $\mathrm{STS}_q(7)$. Problem: its existence is open for every field order q.
- $\mathrm{STS}_q(9)$ which could be called the q-analog of the binary affine plane. Problem: its existence is open for every q.
- Good News: A non-trivial q-Steiner system is known to exist: $\mathrm{STS}_2(13)$ and was discovered by Braun, Etzion, Ostergard, Vardy, Wassermann in 2013.

Focus on binary q-analog of the Fano plane $\mathrm{STS}_2(7)$.

$$\lambda_2 = 1, \quad \lambda_1 = 21, \quad \lambda_0 = 381$$

- $\mathrm{STS}_2(7)$ consists of $\lambda_0 = 381$ blocks which need to be found in a set of $\begin{bmatrix}7\\3\end{bmatrix}_2 = 11811$ planes of that projective space!
- This is a huge search space, as $\binom{11811}{381}$ has 730 decimal digits.

Additional properties and insight is required!

- Through each point P there are $\lambda_1 = 21$ blocks. Image in $V/P \cong \mathrm{PG}(5,2)$ is a line spread, (cf. Mateva, Topalova 2009): There are 131044 types of spreads.
- More refined information by intersection numbers (see Kiermaier and Pavcevic 2014).

Definition (Recall: Steiner system)

$D \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is a t-$(v, k, 1)_q$ Steiner system
if each $T \in \begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in exactly one element of D.

Definition ((constant dimension) subspace code)

$C \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is a $(v, 2(k - t + 1); k)_q$ subspace code
if each $T \in \begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in at most one element of C.

- q-Fano setting: $(7, 4; 3)_q$ subspace code C.
- For $q = 2$:
  - $\#C \leq 381$
  - $\#C = 381 \iff C$ is a $\mathrm{STS}_2(7)$
- Task: Find maximum size $A_q(7, 4; 3)$ of $(7, 4; 3)_q$ subspace code!

History

- Silberstein 2008: $A_2(7,4;3) \geq 289$

  Based on lifted rank metric codes.
- Vardy 2008: $A_2(7,4;3) \geq 294$
- Kohnert, Kurz 2008: $A_2(7,4;3) \geq 304$

  Prescribe group of order 21
- Braun, Reichelt 2012: $A_2(7,4;3) \geq 329$

  Prescribe group of order 15, modify large solutions.
- Liu, Honold 2014; Honold, K. 2015:

  explicit construction of $\#C = 329$
  via expurgation and augmentation of the lifted
  Gabidulin code

More-over: $A_3(7,4;3) \geq 6977$ for $q = 3$ (which means $\mathrm{STS}_3(7)$ would have size 7651.)

Recent approach

by Daniel Heinlein, Sascha Kurz and Alfred Wassermann.

- Systematically check $G < \mathrm{GL}(7, 2)$ for admitting large G-invariant codes.
- Found $\#G = 64$ admitting $\#C = 319$.
- $\ldots$ having a subgroup of order 32 admitting $\#C = 327$.
- $\ldots$ having a subgroup of order 16 admitting $\#C = 329$.
- $\ldots$ having a subgroup of order 4 admitting

$$\#C = 333.$$

- Code provided at subspacecodes.uni-bayreuth.de