New Lower Bounds for Constant Dimension Subspace Codes

Patric R. J. Östergård

Department of Communications and Networking
Aalto University School of Electrical Engineering
P.O. Box 13000, 00076 Aalto, Finland
E-mail: patric.ostergard@aalto.fi

Joint work with Michael Braun and Alfred Wassermann.

Supported in part by the Academy of Finland and
COST Action 1104.

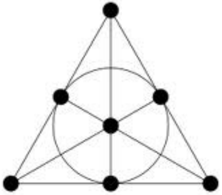
The Other Authors

Block Designs

t-(v, k, λ) (packing, covering) design A collection of k-subsets, called *blocks*, of a v-set of *points*, such that each t-subset of points is contained in exactly (at most, at least) λ blocks.

Example. The Fano plane, a 2-$(7, 3, 1)$ design.

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



q-Analogs of Sets

Jacques Tits (1957): Sets are vector spaces over the finite field $\mathbb{F}_q$ in the limit as $q \to 1$.

$q \to 1$	q-analog
set	vector space
subset	vector subspace
size (of set)	dimension (of space)
complement set	dual space

Based on this, we can define q-analogs of block designs.

q-Analogs of Block Designs

q-analog of t-(v, k, λ) (packing, covering) design: A collection C of k-dimensional subspaces of a v-dimensional space V over $\mathbb{F}_q$, such that each t-dimensional subspace of V is contained in exactly (at most, at least) λ elements of C.

Finding q-analogs of t-$(v, k, 1)$ designs, that is, *q-Steiner systems*, has turned out to be a challenge.

Application (Kötter & Kschischang, 2007)

A q-Steiner system can be used for error-correction in networks, under randomized network coding.

Theorem (Braun, Etzion, Östergård, Vardy & Wassermann)

There exist 2-(13, 3, 1) *q-Steiner systems.*

Why is This So Hard?

A necessary condition for the existence of a 2-$(v, 3, 1)$ design over $\mathbb{F}_q$ is that $v \equiv 1, 3 \pmod{6}$. The q-analog of a Fano plane is the smallest nontrivial case. Consider $\mathbb{F}_2$.

Number of 3-subspaces of a 7-space: $\begin{bmatrix}7\\3\end{bmatrix} = 11811$.
Number of 2-subspaces of a 7-space: $\begin{bmatrix}7\\2\end{bmatrix} = 2667$.
Number of 2-subspaces of a 3-space: $\begin{bmatrix}3\\2\end{bmatrix} = 7$.

$\Rightarrow$

Number of 3-subspaces in a q-Fano plane: $2667/7 = 381$.

q-Analogs of Packing Designs

With parameters for which q-Steiner systems don't exist (or have not been found) one may focus on the packing version of the problem.

Our Approach:

- Lower bounds for the size of q-packing designs by construction.
- Prescription of group of automorphisms (Kramer–Mesner).
- Construction by stochastic search.

Symmetries (1)

The available group G of symmetries is the general semilinear group $\Gamma L(n, q)$. If q is a prime, we have $GL(n, q)$ (assumed in the sequel).

isomorphism An element $g \in G$ for which $\mathcal{S}_2 = \mathcal{S}_1^g$, where $\mathcal{S}_1$ and $\mathcal{S}_2$ are sets of subspaces.

automorphism An element $g \in G$ for which $\mathcal{S} = \mathcal{S}^g$, where $\mathcal{S}$ is a set of subspaces.

(full) automorphism group The group formed by the automorphisms under composition.

group of automorphisms Subgroup of the full automorphism group.

Symmetries (2)

"Nice" subgroups of $\mathrm{GL}(n, q)$:

View vectors in $\mathbb{F}_q^n$ as elements of $\mathbb{F}_{q^n}$.

Singer cyclic group, of order $q^n - 1$: $\langle\sigma\rangle$

Galois group, $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, of order n: $\langle\phi\rangle$

$\langle\sigma, \phi\rangle$ normalizer of Singer cyclic group, order $n(q^n - 1)$.

$\langle\sigma^i, \phi^j\rangle$ subgroups of the previous group (several groups if n and/or $q^n - 1$ are not primes)

Constructing q-Packing Designs with $\lambda = 1$ via Cliques

The prescribed group partitions the k-dimensional subspaces into orbits. Such orbits that fulfill the packing criterion (each t-dimensional subspace occurs at most once) are called admissible. Two different orbits whose union fulfills the packing criterion are called compatible.

Construct a weighted graph $G = (V, E)$.

V: one vertex for each admissible orbit
E: one edge for each pair of compatible orbits
$w(v)$, $v \in V$: length of orbit

Computational Problem: Find a maximum weight clique in G.

Stochastic Search for Maximum Weight Cliques

For small parameters, an exact solver can be used, like Cliquer:
http://users.aalto.fi/pat/cliquer.html

Old stochastic methods
: Maintain a clique by adding and removing vertices, one at a time. Does *not* work well for weighted graphs.

Montemanni & Smith, 2009
: Remove many vertices (random choice) and add vertices using an exact algorithm.

New stochastic method
: Remove many vertices (which are "close" in a packing sense) and add vertices using an exact algorithm.

Results

Table: Lower bounds for the size of q-analogs of t-$(v, k, 1)$ designs

v	k	t	Old bound	New bound	Density	Group
8	3	2	1312	1326	0.860	$\langle\sigma^5\rangle$
9	3	2	5694	5986	0.965	$\langle\sigma^7, \phi\rangle$
10	3	2	21483	23870	0.959	$\langle\sigma^3, \phi^2\rangle$
11	3	2	92411	97526	0.978	$\langle\sigma, \phi\rangle \times 1$
13	*3*	*2*		*1597245*	*1.000*	$\langle\sigma, \phi\rangle$
8	4	3	4797	4801	0.741	$\langle\sigma^{17}, \phi\rangle$

Thank You!

And welcome to NORCOM in Finland, 13-15.6.2016: