Remarks on Constant-Dimension Subspace Codes

Thomas Honold

Department of Information Science and Electronics Engineering
Zhejiang University

ALCOMA15
Kloster Banz
March 16, 2015

Outline

In Memoriam Axel Kohnert

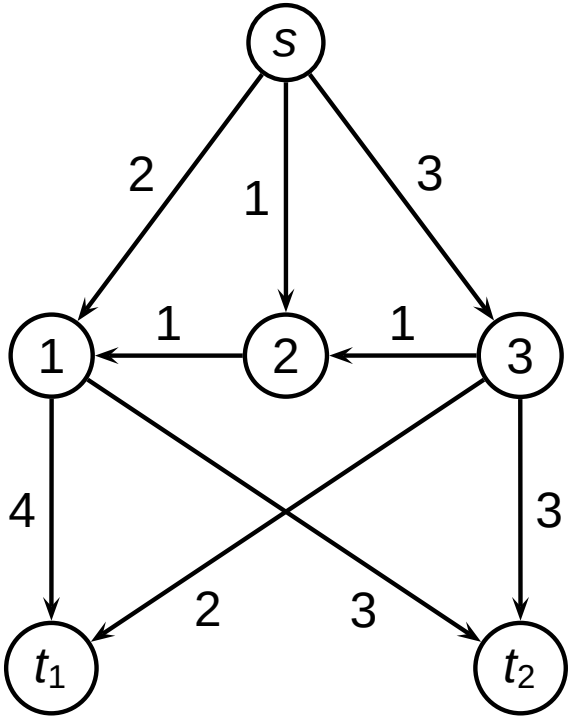
Outline

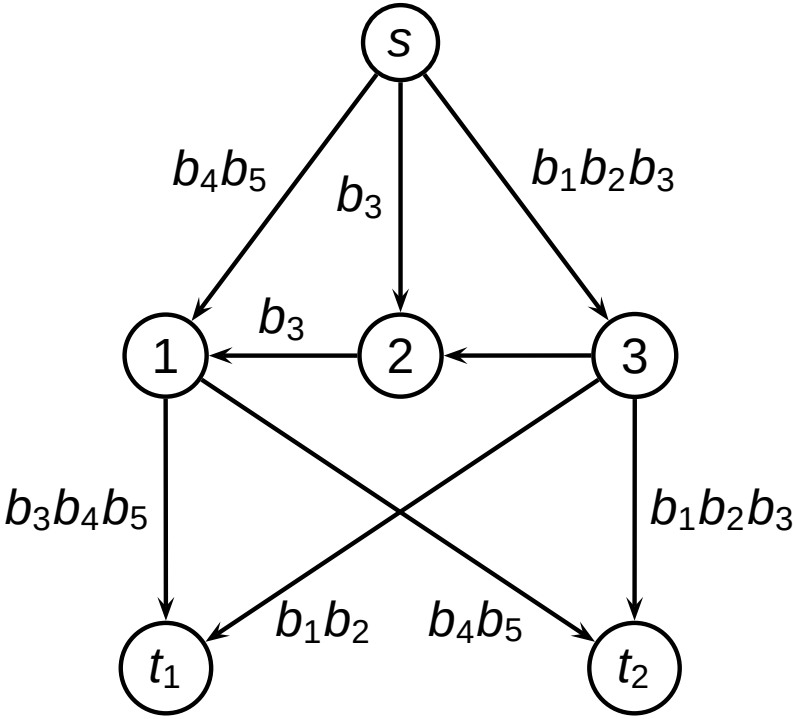
The Basic Idea of Network Coding

Coding replaces Routing

Instead of simply replicating some of the incoming information packets at an outgoing link (*routing*), network nodes compute the outgoing packets as a function of the incoming packets (*network coding*).

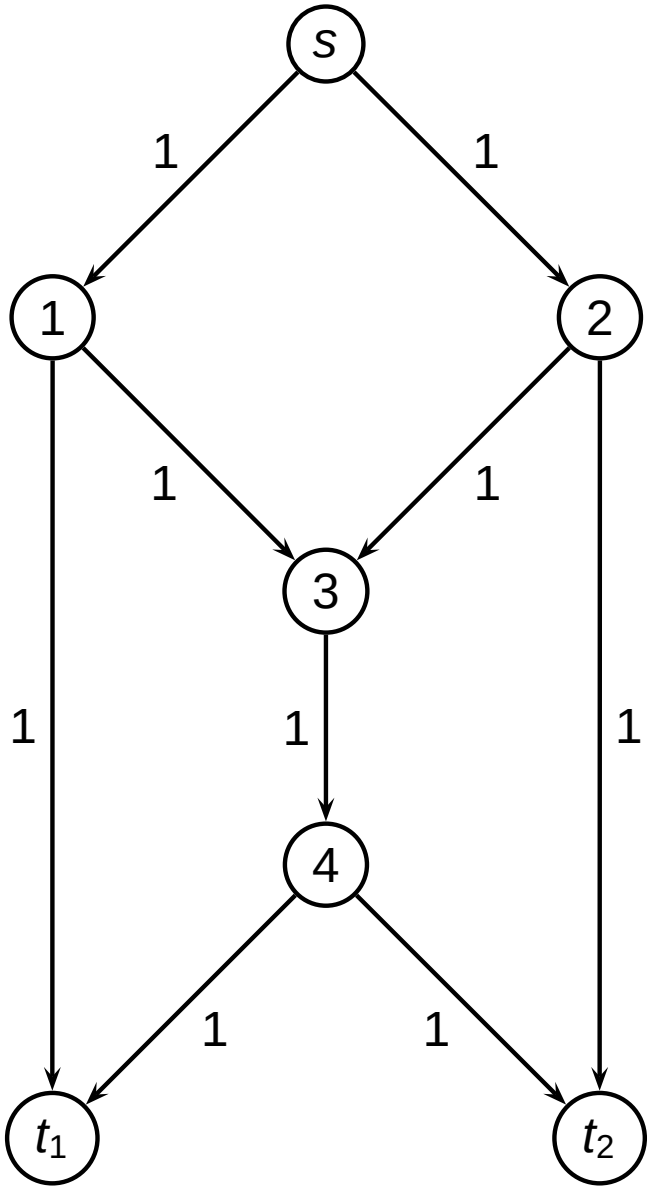
Optimal Routing Solution

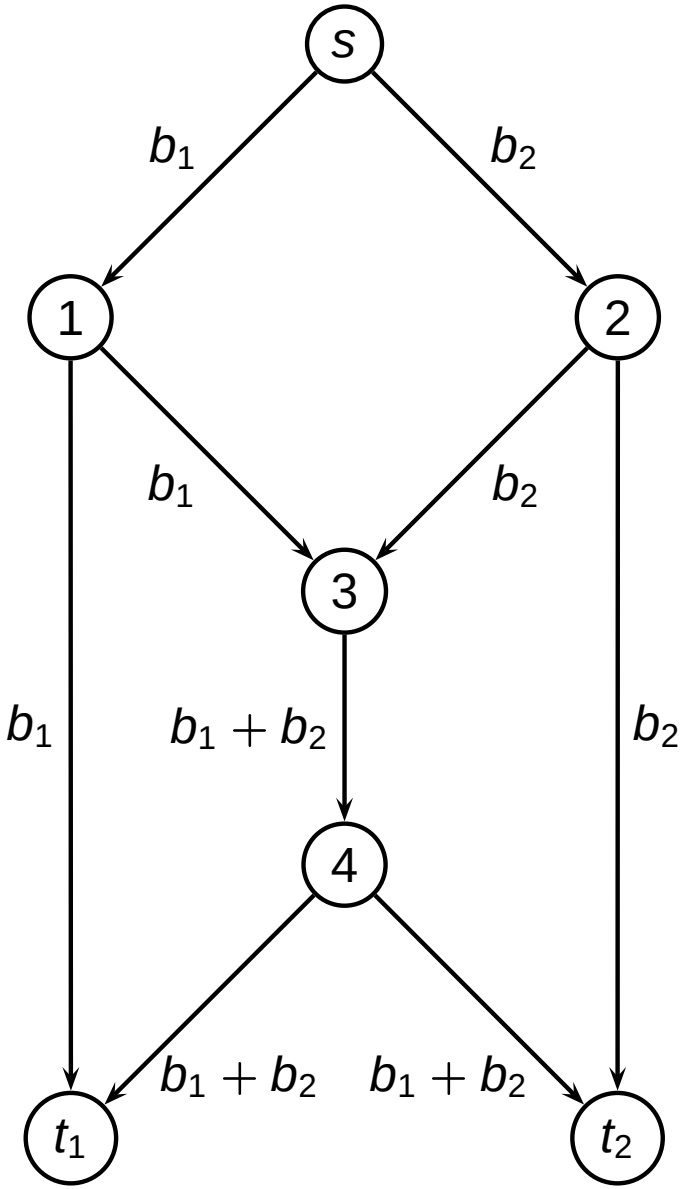




Optimal Coding Solution

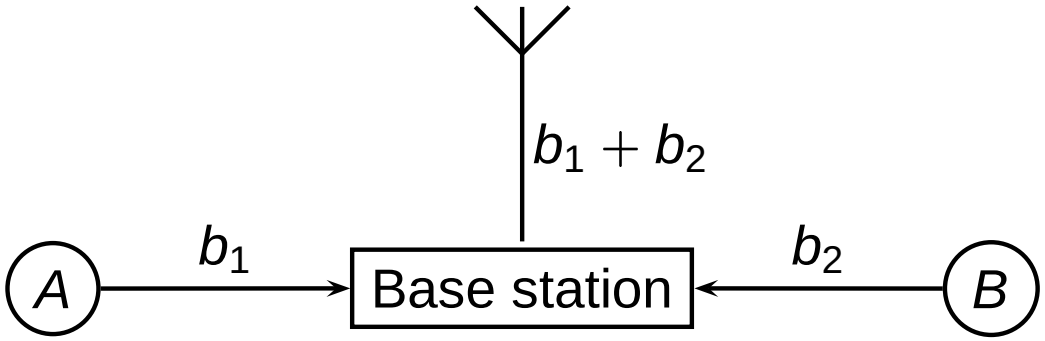
Cannot be achieved by routing





Two-Way Wireless Relay Channel

Suppose two mobile stations want to send each other one bit of information.



Store and Forward

- A sends b_1 to the relay
- B sends b_2 to the relay
- The relay broadcasts b_1 (to A)
- The relay broadcasts b_2 (to B)

Requires 4 timeslots

Network Coding

- A sends b_1 to the relay
- B sends b_2 to the relay
- The relay broadcasts $b_1 + b_2$ (to both A and B)

Requires only 3 timeslots

The Main Results

Ahlwede-Cai-Li-Yeung (2000)

Information can be transmitted from a single source node to multiple sink nodes simultaneously at a rate equal to the minimum of the different unicast capacities (given by the Max-Flow Min-Cut Theorem from Graph Theory).

This maximum transmission rate is called *multicast capacity* of the network.

Li-Yeung-Cai (2003)

Linear Network Coding over a sufficiently large finite field achieves multicast capacity.

Ho-Médard-Koetter-Karger-Effros-Shi-Leong (2006)

Random Linear Network Coding achieves multicast capacity with high probability.

Yeung-Li-Cai-Zhang (2006)

Error-Correcting Network Codes in the “coherent” setting

Linear Operator Channels

Koetter-Kschischang (2008)

Consider a packet network capable of transmitting packets of length v over a finite field $\mathbb{F}_q$ (i.e. elements of $\mathbb{F}_q^v$) along its edges (links) and employing (random) linear network coding.

- **X** matrix having as its rows the packets injected by the source s into the network.
- **Y** matrix of packets (again considered as row vectors) received by a particular sink node t.
- **G** *Global Transfer Matrix* of t (the matrix describing the overall linear relation between source packets and packets received by t in the error-free case).
- **Z** matrix of error packets added to the information packets at the various edges (one error packet for each edge of the network)
- **H** *Error Transfer Matrix* of t

Random Linear Matrix Channel

$\mathbf{Y} = \mathbf{GX} + \mathbf{HZ}$ with $\mathrm{p}(\mathbf{Y}|\mathbf{X}) = \sum_{\mathbf{GX}+\mathbf{HZ}=\mathbf{Y}} \mathrm{p}(\mathbf{G}, \mathbf{H}, \mathbf{Z})$ for some probability distribution $\mathrm{p}(\mathbf{G}, \mathbf{H}, \mathbf{Z})$.

Observation of Koetter-Kschischang

In the error-free case ($\mathbf{Z} = \mathbf{0}$) the row space $\langle \mathbf{Y} \rangle$ is a subspace of $\langle \mathbf{X} \rangle$, and is equal to $\langle \mathbf{X} \rangle$ if $\mathbf{G}$ has full column rank.

Moreover, under reasonable assumptions on the distribution of the encoding vectors at the network nodes and the error vectors at the network links, the channel reduces to a *subspace channel*

$$\mathrm{p}(V|U) = \sum_{\mathbf{Y}=V} \mathrm{p}(\mathbf{Y}|\mathbf{X}), \quad \text{where } \mathbf{X} \text{ satisfies } \langle \mathbf{X} \rangle = U.$$

Encoding

The source node selects a matrix $\mathbf{X} \in \mathbb{F}_q^{k \times v}$, $k = \dim(U)$, such that $\langle \mathbf{X} \rangle = U$ and injects the rows of $\mathbf{X}$ as packets into the network.

Decoding

A sink node tries to reconstruct the sent subspace U from the received subspace $V = \langle \mathbf{Y} \rangle$, which is generated by the packets received at the sink node (the rows of $\mathbf{Y}$).

Outline

$\mathbb{F}_q^v$ Vector space of v-tuples $\mathbf{x} = (x_1, \ldots, x_v)$, $x_i \in \mathbb{F}_q$, over the finite field $\mathbb{F}_q = \mathrm{GF}(q)$ ("ambient space", "packet space")

$\mathcal{S} = \mathcal{S}(\mathbb{F}_q^v)$ Lattice of subspaces of $\mathbb{F}_q^v$

$\mathcal{S}_k$ Subset ("Grassmannian") consisting of all k-dimensional subspaces in $\mathcal{S}$ (where $0 \leq k \leq v$)

For $U, V \in \mathcal{S}$ one defines

Subspace Distance

$$\begin{aligned} \mathrm{d_s}(U, V) &= \dim(U + V) - \dim(U \cap V) \\ &= \dim(U) + \dim(V) - 2\dim(U \cap V) \end{aligned}$$

Injection Distance

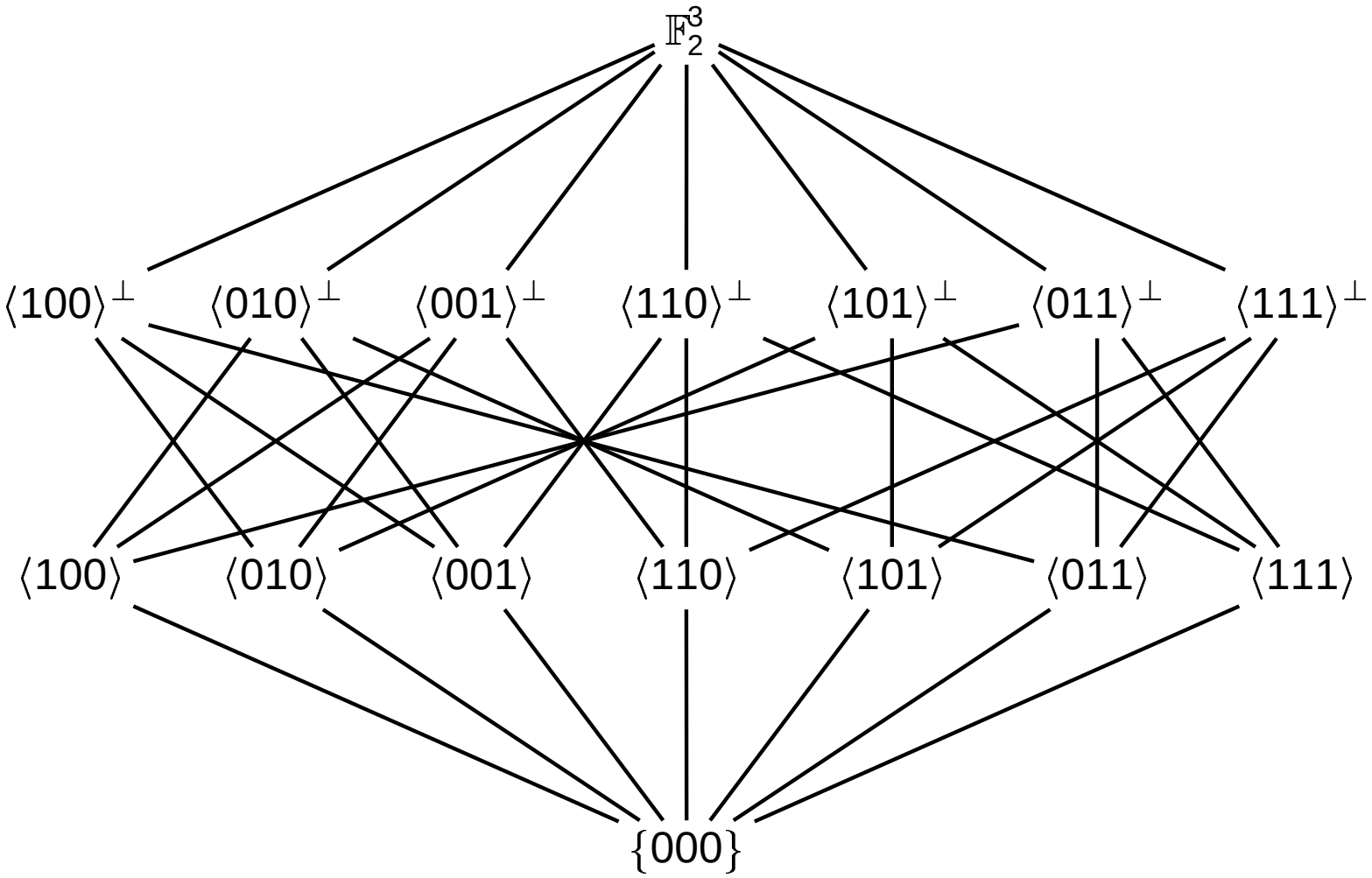
$$\mathrm{d_i}(U, V) = \max\{\dim(U), \dim(V)\} - \dim(U \cap V)$$

q-ary (v, M, d) Subspace Code

A subset $\mathcal{C} \subseteq \mathcal{S}$ of size (cardinality) $\#\mathcal{C} = M$ and *minimum distance* (say, in the subspace metric)
$\mathrm{d_s}(\mathcal{C}) := \min\{\mathrm{d_s}(U, V); U, V \in \mathcal{C}, U \neq V\} = d$

Example setting ($q = 2$, $v = 3$)

$$\mathbb{F}_2^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}.$$



Hasse diagram of $\mathcal{S}(\mathbb{F}_2^3)$

The Main Problem of Subspace Coding

Akin to the Main Problem of Algebraic Coding Theory

The main problem of classical Algebraic Coding Theory asks for the determination of the maximum dimension k of a linear $[n, k, d]$ code over $\mathbb{F}_q$ (i.e. a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d).

Main Problem of Subspace Coding

For a given prime power $q > 1$ and given positive integers $2 \leq d \leq v - 1$ determine the maximum size M of a q-ary (v, M, d) subspace code.

Constant-Dimension Codes

A *constant-dimension code* is a subspace code all of whose members have the same dimension k; notation $(v, M, d; k)$.

For $U, V \in \mathcal{S}_k$ we have $\mathrm{d_s}(U, V) = 2\mathrm{d_i}(U, V) = 2k - 2\dim(U \cap V)$.

Main Problem for Constant-Dimension Codes

Given q and $1 \leq \delta \leq k \leq v - 1$, determine the maximum size M of a q-ary $(v, M, 2\delta; k)$ constant-dimension code in $(\mathbb{F}_q^v, \mathrm{d_s})$.

Tables

$\mathrm{A}_q(v, d)$ Maximum size of a q-ary (v, M, d) subspace code

$\mathrm{A}_q(v, d; k)$ Maximum size of a q-ary $(v, M, d; k)$ constant-dimension subspace code

In the constant-dimension case it suffices to consider (v, d, k) with $1 \leq k \leq v/2$ (since $\mathcal{C} \mapsto \mathcal{C}^\perp = \{U^\perp; U \in \mathcal{C}\}$ defines an automorphism of the metric space $(\mathbb{F}_q^v, \mathrm{d_s})$) and $d \in \{2, 4, \ldots, 2k\}$.

$k \backslash d$	2	4	6
1	63		
2	651	21	
3	1395	77	9

$\mathrm{A}_2(6, d; k)$

$k \backslash d$	2	4	6
1	127		
2	2667	41	
3	11811	329–381	17

$\mathrm{A}_2(7, d; k)$

$k \backslash d$	2	4	6	8
1	255			
2	10795	85		
3	97155	1326–1493	34	
4	200787	4797–6477	257–289	17

$\mathrm{A}_2(8, d; k)$

Geometric View of Subspace Codes

A set $\mathcal{C}$ of k-dimensional subspaces of $\mathbb{F}_q^v$ forms a $(v, M, 2\delta; k)$ subspace code if and only if $t = k - \delta + 1$ *is the smallest positive integer such that any t-dimensional subspace of $\mathbb{F}_q^v$ is contained in at most one member of $\mathcal{C}$.*

$\Longrightarrow$ Constant-dimension codes may as well be defined by this geometric "packing condition". The nontrivial range for t is $0 \leq t \leq k - 2$.

A standard double-counting argument gives

$$\#\mathcal{C} \times \begin{bmatrix} k \\ t \end{bmatrix}_q \leq \begin{bmatrix} v \\ t \end{bmatrix}_q, \quad \text{or} \quad \#\mathcal{C} \leq \prod_{i=0}^{t-1} \frac{q^{v-i} - 1}{q^{k-i} - 1},$$

with equality if and only if each t-dimensional subspace of $\mathbb{F}_q^v$ is contained in precisely one codeword of $\mathcal{C}$. Such structures are known as *Steiner systems over finite fields* (*q-analogues of ordinary Steiner systems*) and form the "best" subspace codes (provided, of course, that they exist).

Better Upper Bounds

Integrality Conditions

A Steiner system $\mathrm{S}_q(t,k,v)$ over $\mathbb{F}_q$ can only exist if the numbers $\lambda_s = \prod_{i=s}^{t-1} \frac{q^{v-i}-1}{q^{k-i}-1}$ are integers for $1 \le s \le t$. This gives

$$\#\mathcal{C} \le \left\lfloor \frac{q^v-1}{q^k-1} \left\lfloor \frac{q^{v-1}-1}{q^{k-1}-1} \cdots \left\lfloor \frac{q^{v-t+1}-1}{q^{k-t+1}-1} \right\rfloor \cdots \right\rfloor \right\rfloor .$$

Using available information on smaller cases

The recursive version of the above bound is

$$\mathrm{A}_q(v,d;k) \le \left\lfloor \frac{q^v-1}{q^k-1} \cdot \mathrm{A}_q(v-1,d;k-1) \right\rfloor .$$

This gives a better bound if a stronger bound for $\mathrm{A}_q(v-1,d;k-1)$ (or $\mathrm{A}_q(v-2,d;k-2)$, $\mathrm{A}_q(v-3,d;k-3)$, etc.) is known.

Example ($k = 3$, $t = 2$)

For a q-ary $(v, M, 4; 3)$ constant-dimension code the best known general upper bound is

$$\#\mathcal{C} \leq \begin{cases} \left\lfloor \frac{(q^v-1)(q^{v-1}-1)}{(q^3-1)(q^2-1)} \right\rfloor & \text{if } v \equiv 1 \pmod 2, \\ \left\lfloor \frac{q^v-1}{q^3-1} \left(\frac{q^{v-1}-q}{q^2-1} - q + 1 \right) \right\rfloor & \text{if } v \equiv 0 \pmod 2. \end{cases}$$

The sharper bound for $v \equiv 0 \pmod 2$ follows from the fact that a $(v-1, M, 4; 2)$ code (partial line spread in $\mathrm{PG}(v-2, q)$) has size at most

$$q^{v-3} + q^{v-5} + \cdots + q^3 + 1 = \frac{q^{v-1} - q}{q^2 - 1} - q + 1.$$

Further the bound excludes the existence of q-analogues $\mathrm{STS}_q(v)$ of Steiner triple systems in the case $v \equiv 5 \pmod 6$.

$\Longrightarrow$ The necessary condition for the existence of an $\mathrm{STS}_q(v)$ is $v \equiv 1, 3 \pmod 6$ (the same as for an ordinary $\mathrm{STS}(v)$).

Steiner Systems over Finite Fields

Known Results

In fact only very little is known about the existence problem for $\mathrm{S}_q(t, k, v)$.

- The cases $\mathrm{STS}_q(v)$, $v \in \{7, 9\}$, any q, are all unsolved
- There exists an $\mathrm{STS}_2(13)$ (in fact many non-isomorphic ones) [2].

The known $\mathrm{STS}_2(13)$ are invariant under the normalizer of a Singer group of $\mathrm{PG}(6, q)$, which has order $(2^{13} - 1) \times 13 = 106\,483$. This greatly facilitates a computer search and was the route to success.

Singer-invariant $\mathrm{STS}_q(7)$ do not exist for the first few small values of q. This perhaps explains why the case $v = 13$ was solved first (for $q = 2$).

Outline

The Lifting Construction

Silva-Kschischang-Koetter (2008)

The lifting construction yields q-ary $\left(v, q^{(v-k)(k-\delta+1)}, 2\delta; k\right)$ constant-dimension codes of fairly large (though not optimal) size.

Idea

Restrict attention to the k-dimensional subspaces U of $\mathbb{F}_q^v$ whose canonical matrices have their pivots in the first k columns; i.e. $U = \langle(\mathbf{I}_k|\mathbf{A})\rangle$ for some $\mathbf{A} \in \mathbb{F}_q^{k\times(v-k)}$. For such subspaces we have

$$\begin{aligned}
\mathrm{d_s}(U, V) &= 2\dim(U+V) - 2k \\
&= 2\,\mathrm{rk}\begin{pmatrix}\mathbf{I}_k & \mathbf{A}\\ \mathbf{I}_k & \mathbf{B}\end{pmatrix} - 2k = 2\,\mathrm{rk}\begin{pmatrix}\mathbf{I}_k & \mathbf{A}\\ \mathbf{0} & \mathbf{B}-\mathbf{A}\end{pmatrix} - 2k \\
&= 2\ \mathrm{rk}(\mathbf{B}-\mathbf{A}) = 2\mathrm{d_r}(\mathbf{A}, \mathbf{B}),
\end{aligned}$$

where $\mathrm{d_r}$ denotes the so-called *rank distance*.

$\Longrightarrow$ A matrix code $\mathcal{A} = \{\mathbf{A}_1, \ldots, \mathbf{A}_M\} \subseteq \mathbb{F}_q^{k\times(v-k)}$ of minimum *rank distance* $\mathrm{d_r}(\mathcal{A}) = \delta$ yields a $(v, M, 2\delta, k)$ constant-dimension code $\mathcal{C} = \{U_1, \ldots, U_M\}$ via $U_i = \langle(\mathbf{I}_k|\mathbf{A}_i)\rangle$.

MRD Codes

The maximum size of a matrix code $\mathcal{A} \subseteq \mathbb{F}_q^{k\times l}$ with minimum rank distance $\delta \in \{1, 2, \ldots, \min(k, l)\}$ is fortunately known. In order to simplify the statement of the result, we assume $k \leq l$. (This is no restriction, since we can transpose everything.)

Theorem (Delsarte-Gabidulin-Roth, 1978–1991)

The maximum size of a q-ary (k, l, δ) rank-distance code is $q^{(k-\delta+1)l}$. A particular example of such a code is the Gabidulin code

$$\mathcal{G} = \{x \mapsto a_0 x + a_1 x^q + a_2 x^{q^2} + \cdots + a_{k-\delta} x^{q^{k-\delta}}; a_i \in \mathbb{F}_{q^l}\},$$

defined in a basis-independent manner as a space of $\mathbb{F}_q$-linear maps $W \to \mathbb{F}_{q^l}$ on a k-dimensional $\mathbb{F}_q$-subspace W of $\mathbb{F}_{q^l}$.

Notes

- Matrix codes meeting the bound in the Theorem are called *maximum rank distance (MRD) codes*. MRD codes are analogous to maximum distance separable (MDS) codes in Hamming spaces, and the Gabidulin codes can be seen as q-analogs of Reed-Solomon codes.

Notes cont'd

- Polynomials in $\mathbb{F}_{q^l}[X]$ of the special form $a(X) = a_0X + a_1X^q + a_2X^{q^2} + \cdots + a_nX^{q^n}$ are called *linearized polynomials* or *q-polynomials*. They define $\mathbb{F}_q$-linear endomorphisms of $\mathbb{F}_{q^l}[X]$ via $x \mapsto a(x)$, since $(x+y)^q = x^q + y^q$ for $x, y \in \mathbb{F}_{q^l}$ and $x^q = x$ for $x \in \mathbb{F}_q$.
- $\mathrm{d_r}(\mathcal{G}) \geq \delta$ follows from the degree bound for polynomials: A nonzero map $x \mapsto a_0x + a_1x^q + \cdots + a_{k-\delta}x^{q^{k-\delta}}$ has at most $q^{k-\delta}$ zeros in $\mathbb{F}_{q^l}$, i.e. a kernel of dimension $\leq k - \delta$, and hence rank at least δ.
- $\#\mathcal{A} = q^{(k-\delta+1)l}$ is reflected in the following characteristic property of q-ary (k, l, δ) MRD codes: With $r := k - \delta + 1$ we have that for any full-rank matrix $\mathbf{Z} \in \mathbb{F}_q^{r\times k}$ the map $\mathcal{A} \to \mathbb{F}_q^{r\times l}$, $\mathbf{A} \to \mathbf{ZA}$ is a bijection.

Example ($q = 2, k = l = 3$)

The maximum size of a set of binary 3×3 matrices of rank distance 3 (equivalently the sum of any two distinct matrices is non-singular) is $2^{1\cdot 3} = 8$. As a particular example we can take a maximal subfield ($\cong \mathbb{F}_8$) of the matrix ring $\mathrm{M}_3(\mathbb{F}_2)$, for example

$$\mathcal{G}_1 = \left\{ \begin{pmatrix} a & c & b+c \\ b & a & c \\ c & b+c & a+b+c \end{pmatrix} ; a, b, c \in \mathbb{F}_2 \right\},$$

the subfield generated by the companion matrix $\mathbf{A}$ of $X^3 + X + 1$.

If we stipulate instead rank distance 2, the maximum size is $2^{2\times 3} = 64$, realized by

$$\mathcal{G}_2 = \{a_0 x + a_1 x^2; a_0, a_1 \in \mathbb{F}_8\} \subset \mathrm{End}(\mathbb{F}_8/\mathbb{F}_2).$$

Using the same basis of $\mathbb{F}_8$ as above and denoting the matrix of the Frobenius automorphism $\mathbb{F}_8 \to \mathbb{F}_8$, $x \mapsto x^2$ by $\mathbf{F}$, we have $\mathcal{G}_2 \supset \mathcal{G}_1$, and $\mathcal{G}_2$ is generated over $\mathbb{F}_2$ by the 6 matrices $\mathbf{I}$, $\mathbf{A}$, $\mathbf{A}^2$, $\mathbf{F}$, $\mathbf{AF}$, $\mathbf{AF}^2$.

The Echelon-Ferrers Construction

From now on we will focus on the determination of the best (i.e. largest) $(7, M, 4; 3)$ constant-dimension codes and use the case $q = 2$ as a showcase.

Applying the lifting construction to $\mathcal{G}_2$ ($\delta = 2 \Longrightarrow d = 4$), we obtain a binary $(7, 256, 4; 3)$ constant-dimension code $\mathcal{C}$. The 256 canonical matrices representing the subspaces in $\mathcal{C}$ have shape

$$\begin{pmatrix} 1 & 0 & 0 & * & * & * & * \\ 0 & 1 & 0 & * & * & * & * \\ 0 & 0 & 1 & * & * & * & * \end{pmatrix}.$$

In projective geometry terms, $\mathcal{C}$ consists of 256 planes in $\mathrm{PG}(6, 2)$ mutually intersecting in at most a point (since distinct subspaces in $\mathcal{C}$ intersect at most in a 1-dimensional subspace of $\mathbb{F}_2^7$). Moreover, all planes in $\mathcal{C}$ are disjoint from the special solid $S = (000 * * * *)$.

Question

How far can $\mathcal{C}$ be extended?

The answer ($M = 291$) is provided by an extension of the echelon-Ferrers construction and a “geometric” upper bound.

The Upper Bound

Lemma

The planes in $\mathcal{C}$ cover every line disjoint from S exactly once.

In particular, the number of lines in $\mathrm{PG}(6,2)$ disjoint from S must be $7 \times 256 = 1792$ (since every plane containes 7 lines). This can be checked independently by a counting argument.

Proof.

A line L disjoint from S has a canonical matrix of the form $(\mathbf{Z}|\mathbf{B})$ with $\mathbf{Z} \in \mathbb{F}_2^{2\times 3}$, $\mathbf{B} \in \mathbb{F}_2^{2\times 4}$ and $\mathrm{rk}(\mathbf{Z}) = 2$ (in fact $\mathbf{Z}$ must be itself canonical).
By what we have seen, there exists $\mathbf{A} \in \mathcal{G}_2$ such that $\mathbf{ZA} = \mathbf{B}$.
$\Longrightarrow \mathbf{Z}(\mathbf{I}_3|\mathbf{A}) = (\mathbf{Z}|\mathbf{ZA}) = (\mathbf{Z}|\mathbf{B})$, implying that L is contained in the plane of $\mathcal{C}$ with canonical matrix $(\mathbf{I}_3|\mathbf{A})$. $\square$

From the lemma the upper bound $M \leq 291$ is now easy to derive: We cannot add a plane to $\mathcal{C}$ meeting S in a point (since such a plane would contain lines disjoint from S and lead to a multiple line cover. Hence the best we can do is adding $\begin{bmatrix}4\\2\end{bmatrix}_2 = 35$ planes to $\mathcal{C}$, meeting S in the 35 lines contained in S.

The Construction

First we describe the general idea of the echelon-Ferrers construction in our special setting $q = 2$, $(v, k, d) = (7, 3, 4)$.

Identifying vector

To a 3-dimensional subspace U of $\mathbb{F}_2^7$ assign the vector $\mathrm{v}(U) \in \mathbb{F}_2^7$ having 1's in the positions of the pivot columns of U and 0's elsewhere. The vector $\mathrm{v}(U)$ has Hamming weight 3 and determines the shape of the canonical matrix of U. It is called *identifying vector* of U.

Key Observation

The subspace distance $\mathrm{d_s}(U, V)$ is lower-bounded by the Hamming distance $\mathrm{d_{Ham}}\big(\mathrm{v}(U), \mathrm{v}(V)\big)$.

Echelon-Ferrers construction (Etzion-Silberstein 2009)

1. Select a set I of identifying vectors of constant Hamming weight 3 and minimum Hamming distance 4.
2. For each $\mathbf{v} \in I$ determine the largest $(3, 4, 2)$ rank distance code with the particular shape imposed by $\mathbf{v}$ and lift it to a subspace code $\mathcal{C}(\mathbf{v})$. The union $\bigcup_{\mathbf{v} \in I} \mathcal{C}(\mathbf{v})$ then has $d = 4$.

Specifically we choose
$I = \{1110000, 1001100, 1000011, 0101010, 0100101, 0011001, 0010110\}$,
corresponding to the 7 shapes

$$\begin{pmatrix} 1&0&0&*&*&*&* \\ 0&1&0&*&*&*&* \\ 0&0&1&*&*&*&* \end{pmatrix}, \begin{pmatrix} 1&*&*&0&0&*&* \\ 0&0&0&1&0&*&* \\ 0&0&0&0&1&*&* \end{pmatrix}, \begin{pmatrix} 1&*&*&*&*&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&1&*&0&*&0&* \\ 0&0&0&1&*&0&* \\ 0&0&0&0&0&1&* \end{pmatrix},$$

$$. \begin{pmatrix} 0&1&*&*&0&*&0 \\ 0&0&0&0&1&*&0 \\ 0&0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&0&*&*&0 \\ 0&0&0&1&*&*&0 \\ 0&0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&*&0&0&* \\ 0&0&0&0&1&0&* \\ 0&0&0&0&0&1&* \end{pmatrix}.$$

From the first shape we can select $2^8 = 256$ matrices (as we have seen), from the second shape $2^4 = 16$ matrices (project the first 256 onto the lower left 2×2 square and use the kernel), etc. We obtain a binary $(7, 289, 4; 3)$ constant dimension code, as asserted.

$\mathbf{v}$	1110000	1001100	1000011	0101010	0100101	0011001	0010110	$\sum$
$\#\mathcal{C}(\mathbf{v})$	2^8	2^4	2^0	2^3	2^1	2^2	2^1	289

How to Achieve $M = 291$?

This can be done using the concept of *pending dots* [1], a refinement of the echelon-Ferrers construction.

Alternative Construction

A plane E meeting S in a line L has the form $E = \langle P, L\rangle = P + L$ for some point P outside S; $F = \langle E, S\rangle$ is a 4-flat above S.

$$\#\text{4-flats above } S = 7$$
$$\#\text{lines in } S = 35 = 7 \times 5$$

$\Longrightarrow$ It is reasonable to choose 5 points in every F and connect them to 5 lines in S.

Condition: $E_1 \cap E_2 \cap (\mathcal{P} \setminus S) \neq \emptyset \Longrightarrow L_1 \cap L_2 = \emptyset$

Now recall that $\mathrm{PG}(S) \cong \mathrm{PG}(3, 2)$ admits a decomposition of its 35 lines into 7 spreads (called a *packing* or *parallelism*).

$\Longrightarrow$ We can match the 4-flats above S to the spreads and connect a fixed point in $F \setminus S$ to the 5 lines of the corresponding spread.

Outline

Definition of the δ-invariant

Represent $\mathrm{PG}(3, q) = \mathrm{PG}(\mathbb{F}_q^4/\mathbb{F}_q)$ as $\mathrm{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$.

Definition

For $a, b \in \mathbb{F}_{q^4}$ set $\delta(a, b) = ab^q - a^q b = a\prod_{\lambda\in\mathbb{F}_q}(b - \lambda a)$ and for a line $L = \langle a, b\rangle$ of $\mathrm{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$

$$\delta(L) = \mathbb{F}_q\,\delta(a, b).$$

Notes

- $\delta(L)$ is simply the product of all points on L in $\mathbb{F}_{q^4}/\mathbb{F}_q^\times$. Hence $L \mapsto \delta(L)$ maps lines to points.
- $\delta(L)$ is the projective version of the 2nd Dickson line invariant from Modular Invariant Theory.
- $\delta(E)$ for a plane E can be defined as in Note 1 (but not as in the definition).

Properties of δ

- $b \mapsto \delta(a, b)$ is $\mathbb{F}_q$-linear with kernel $\mathbb{F}_q a$, hence maps line pencils (the set of lines through a point $\mathbb{F}_q a$) bijectively onto the points of a plane (the plane with equation $\mathrm{T}(a^{-q-1}x) = 0$).
  $\Longrightarrow \delta$ is one-to-one on the lines in every plane.
- δ maps the lines in a plane bijectively to the points of another plane.

Outline

Previous Constructions

M	Construction	Ref.
q^8	lifting construction	[3]
$q^8 + q^4 + q^3 + q^2 + 2q + 1$	echelon-Ferrers	[1]
$q^8 + q^4 + q^3 + 2q^2 + q + 1$	pending dots	[1]

LMRD Bound

$M \leq q^8 + \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = q^8 + q^4 + q^3 + 2q^2 + q + 1$

New Result (H.-Kiermaier, 2015)

1. There exists a q-ary $(7, q^8 + q^5 + q^4 - q - 1, 4; 3)$ subspace code $\mathcal{C}$ with the following additional properties:
   - (i) The planes in $\mathcal{C}$ meet a fixed 3-flat S of $\mathrm{PG}(6, q)$ in at most a point.
   - (ii) $\mathcal{C}$ is invariant under a Singer group of S (acting trivially on a complementary plane).
2. There exists a ternary $(7, 6976, 4; 3)$ subspace code.

Notes on the new result

- $3^8 + 3^5 + 3^4 - 3 - 1 = 6881$
  In Part (2) it is claimed that in the ternary case the code $\mathcal{C}$ of Part (1) can be augmented by $3^4 + 3^2 + 3 = 95$ further planes meeting S in a line.
- $2^8 + 2^5 + 2^4 - 2 - 1 = 301$. In the binary case the code $\mathcal{C}$ of Part (1) can be augmented by 28 further planes meeting S in a line to a $(7, 329, 4; 3)$ code [1], the largest size currently known [3].
- The code $\mathcal{C}$ of Part (1) contains a distinguished subcode $\mathcal{C}_0$ with $\#\mathcal{C}_0 = q^8 + q^5 - q = \#\mathcal{C} - (q^4 - 1)$, which can be augmented by $q^4 - 1$ further planes in myriads of ways. Thus $\mathcal{C}$ is far from being the unique code of its size.
- The proof uses the same approach as in the first computer-free construction of an optimal $(6, 77, 4; 3)$ subspace code in [1] but introduces several new concepts.

Putative q-Analogues of the Fano Plane

Forming the motivation for this work

For a q-ary $(7, M, 4; 3)$ subspace code $\mathcal{C}$ we have the bound

$$\#\mathcal{C} \leq q^8 + q^6 + q^5 + q^4 + q^3 + q^2 + 1$$

with equality iff $\mathcal{C}$ is an $\mathrm{STS}_q(7)$ (i.e. every line of $\mathrm{PG}(6, q)$ is contained in a unique plane of $\mathcal{C}$).

Structure of a putative $\mathrm{STS}_q(7)$

1. $\#\mathcal{C} = q^8 + q^6 + q^5 + q^4 + q^3 + q^2 + 1$, with $q^4 + q^2 + 1$ planes in $\mathcal{C}$ passing through any point of $\mathrm{PG}(6, q)$.
2. The intersection vector $\alpha(S) = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$, $\alpha_i = \#\{E \in \mathcal{C}; \dim(E \cap S) = i\}$ takes the 2 values

$$(q^8 - q^7 + q^3, q^7 + q^6 + q^5 - q^3 - q^2 - q, q^4 + q^3 + 2q^2 + q + 1, 0),$$
$$(q^8 - q^7, q^7 + q^6 + q^5, q^4 + q^3 + q^2, 1)$$

In particular we can arrange things such that S contains no plane of $\mathcal{C}$ and $q^8 - q^7 + q^3$ planes disjoint from S.

Overview of the Proof

Starting configuration

A lifted $(7, q^8, 4; 3)$ LMRD code $\mathcal{L}$.

- In matrix terms, $\mathcal{L}$ consists of q^8 matrices $\mathbf{A} \in \mathbb{F}_q^{3\times 4}$ at pairwise rank distance ≥ 2 (the corresponding MRD code), each bordered by the 3×3 identity matrix to yield the canonical matrix $(\mathbf{I}_3|\mathbf{A})$.
- In geometric terms, $\mathcal{L}$ consists of q^8 planes in $\mathrm{PG}(6, q)$ that are disjoint from the special solid $S = (0, 0, 0, *, *, *, *)$ (the solid with equation $x_1 = x_2 = x_3 = 0$) and cover each line disjoint from S exactly once.

The LMRD code constraint

The lines disjoint from S are *bound* by $\mathcal{L}$.
Any plane E meeting S in a point contains such lines, hence cannot be added to $\mathcal{L}$. This leads to the LMRD code bound

$$M \leq q^8 + \#\text{lines in } S = q^8 + \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = q^8 + q^4 + \cdots.$$

Consequence

In order to overcome the LMRD code bound, some planes from $\mathcal{L}$ must be removed. This *frees* some lines disjoint from S, possibly making enough space for new planes that meet S in a point to be added.

Why this might work

Removing M_1 planes from $\mathcal{L}$ frees $M_1(q^2+q+1)$ lines.
If the free lines can be exactly covered by "new" planes meeting S in a point, the number of new planes will be $M_1(q^2+q+1)/q^2$.

$\Longrightarrow$ The overall code size has increased by
$M_1(q^2+q+1)/q^2 - M_1 = M_1(q^{-1}+q^{-2}) > 0$.

Questions

- *Which subsets $\mathcal{L}_1 \subseteq \mathcal{L}$ have the property that the lines covered by the planes in $\mathcal{L}_1$ can be exactly rearranged into planes meeting S in a point?*
- *Which of these rearrangements satisfy the subspace distance condition (equivalently, cover no line through a point of S twice)?*

A necessary condition for an exact rearrangement is $q^2 \mid M_1$.

Condition for Exact Rearrangement

The planes in $\mathcal{L}$ are transversal to the $q^2 + q + 1$ hyperplanes H above L.

Every hyperplane section $\mathcal{L} \to \mathrm{PG}(H)$, $E \mapsto E \cap H$ can be described, in matrix terms, as $(\mathbf{I}|\mathbf{A}) \mapsto (\mathbf{Z}|\mathbf{ZA})$ with a canonical 2×3 matrix $\mathbf{Z}$ ($\mathbf{Z} = \mathrm{cm}(Z)$, where Z is the 2-dimensional subspace of $\mathbb{F}_q^3$ determined by $H = Z \times S$).

By the MRD code property, the section determines the set of all lines disjoint from S in $\mathrm{PG}(H)$.

Fact (from the Geometry of Matrices)

The constant-rank 1 subspaces of $\mathbb{F}_q^{m \times n}$ are of the following two types.

1. All matrices with a fixed 1-dimensional row space $\mathbb{F}_q \mathbf{u} \subseteq \mathbb{F}_q^n$.
2. All matrices with a fixed 1-dimensional column space $\mathbb{F}_q \mathbf{v} \subseteq \mathbb{F}_q^m$.

Lemma

Suppose $\mathcal{L}$ arises from a linear MRD code $\mathcal{A} \subset \mathbb{F}_q^{3\times 4}$ and H is a hyperplane of $\mathrm{PG}(6,q)$ containing S with $\mathrm{cm}(H) = \begin{pmatrix} \mathbf{Z} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_4 \end{pmatrix}$. Then for $\mathcal{R} \subset \mathcal{A}$ with $\#\mathcal{R} = q^2$ the following are equivalent:

1. *The q^2 planes in $\mathcal{L}$ corresponding to $\mathcal{R}$ determine a plane in H that meets S in a point P.*
2. *$\mathbf{Z}\mathcal{R} = \mathbf{B}_0 + \mathcal{U}$ for some constant-rank 1 subspace $\mathcal{U} \subset \mathbb{F}_q^{2\times 4}$ of the first type.*
3. *$\mathcal{R} = \mathbf{A}_0 + \mathcal{D}$ for some $\mathbf{A}_0 \in \mathcal{A}$ and some 2-dimensional $\mathbb{F}_q$-subspace $\mathcal{D}$ of $\mathcal{A}$ with the following properties: $\mathcal{D}$ has constant rank 2, and the (1-dimensional) left kernels of the nonzero members of $\mathcal{D}$ generate the row space Z of $\mathbf{Z}$.*

If these conditions are satisfied then the new plane N has $\mathrm{cm}(N) = \begin{pmatrix} \mathbf{Z} & \mathbf{Z}\mathbf{A}_0 \\ \mathbf{0} & \mathbf{s} \end{pmatrix}$, where $\mathbf{s} \in \mathbb{F}_q^4$ is a generator of the common 1-dimensional row space of the nonzero matrices in $\mathbf{Z}\mathcal{D}$. Moreover, $N \cap S = \mathbb{F}_q\,\mathbf{s}$.

Important Note

In view of the MRD code property of $\mathcal{A}$, there exists precisely one such matrix space $\mathcal{D} = \mathcal{D}(Z, P)$ (for each pair Z and P).

For an exact rearrangement of the planes determined by $\mathcal{R}$, the conditions of the lemma must be satisfied *simultaneously* for all $q^2 + q + 1$ hyperplanes H above S (or the corresponding Z).

Theorem

Let $\mathcal{R}$ be a t-dimensional $\mathbb{F}_q$-subspace of a q-ary linear $(3, 4, 2)$ MRD code $\mathcal{A}$, having the following properties:

1. *For each 2-dimensional subspace Z of $\mathbb{F}_q^3$ there exists a 1-dimensional subspace $P = Z'$ of $\mathbb{F}_q^4$ such that $\mathcal{D}(Z, P) \subseteq \mathcal{R}$.*
2. *The map $Z \mapsto Z'$ is one-to-one.*
3. $\operatorname{rk}\begin{pmatrix} \mathbf{Z}\mathbf{A}_1 - \mathbf{Z}\mathbf{A}_2 \\ \mathbf{s} \end{pmatrix} = 3$ *whenever $\mathbf{A}_1$, $\mathbf{A}_2$ are in different cosets of $\mathcal{D}(Z, P)$ in $\mathcal{R}$, where $P = Z'$, $\mathbf{Z} = \operatorname{cm}(Z)$, and $\mathbf{s} = \operatorname{cm}(P)$.*

Then the $(q^2 + q + 1)q^t$ "free" lines contained in the planes corresponding to $\mathcal{R}$ can be rearranged into $(q^2 + q + 1)q^{t-2}$ new planes meeting S in a point and such that the set $\mathcal{N}$ of new planes has minimum subspace distance 4. Consequently, the remaining $q^8 - q^t$ planes in $\mathcal{L}$ and the new planes in $\mathcal{N}$ constitute a $(7, q^8 + q^{t-1} + q^{t-2}, 4; 3)_q$ subspace code.

Questions

1. *Are there such subspaces $\mathcal{R}$ at all?*
2. *Provided the answer to Question 1 is yes, what is the maximal dimension t of such a subspace (clearly, $3 \leq t \leq 5$).*

Observation

The rearrangement condition (Condition (1) of the theorem) is inherited to unions of cosets of $\mathcal{R}$ in $\mathcal{A}$.

Answers

For the Gabidulin code the answers turns out to be "yes" and $t = 4$. Moreover, there are "canonical" 3-and 4-dimensional subspaces $\mathcal{T}$, $\mathcal{R}$ with these properties, from which every further such subspace is obtained by "rotation" with a Singer cycle of S. (The number of choices for $\mathcal{T}$ and $\mathcal{R}$ is therefore $\frac{q^4-1}{q-1}$.)

$\Longrightarrow$ There exist q-ary $(7, q^8 + q^3 + q^2, 4; 3)$ subspace codes consisting of planes meeting S in at most a point.

These codes are extendable to $(7, q^8 + q^4 + 2q^3 + 3q^2 + q + 1, 4; 3)$ subspace codes using the packing construction described earlier.

The Basis-Free View . . .

and how the extension field $\mathbb{F}_{q^4}$ comes into play

Idea

Take the ambient space of $\mathrm{PG}(6, q)$ as $W \times \mathbb{F}_{q^4}$, where $W = \{x \in \mathbb{F}_{q^4}; x + x^q + x^{q^2} + x^{q^3} = 0\}$ is the trace-zero subspace of $\mathbb{F}_{q^4}/\mathbb{F}_q$.

Special solid	$S = \{0\} \times \mathbb{F}_{q^4} \triangleq \mathbb{F}_{q^4}$
3×4 matrices	$\mathrm{Hom}(W, \mathbb{F}_q^4) = \{x \mapsto a_0 x + a_1 x^q + a_2 x^{q^2}; a_i \in \mathbb{F}_{q^4}\}$
Gabidulin code	$\mathcal{G} = \{a_0 x + a_1 x^q; a_0, a_1 \in \mathbb{F}_{q^4}\}$.
LMRD code	$\mathcal{L} = \{\Gamma_f; f \in \mathcal{G}\}$, where $\Gamma_f = \{(x, f(x)); x \in W\}$ denotes the graph of f (as in Real Analysis)

Arbitrary 3-dimensional subspaces of $W \times \mathbb{F}_{q^4}$ are parametrized as $U = \{(x, f(x) + y); x \in Z, y \in T, f \in \mathrm{Hom}(Z, \mathbb{F}_{q^4}/T)\} = U(Z, T, f)$, where

$$Z = \{x \in W; \exists y \in \mathbb{F}_{q^4} \text{ such that } (x, y) \in U\} \subseteq W,$$

$$T = \{y \in \mathbb{F}_{q^4}; (0, y) \in U\} \subseteq \mathbb{F}_{q^4}.$$

The Basis-Free View cont'd

Incidence $U(Z', T', f') \subseteq U(Z, T, f)$ if and only if $Z' \subseteq Z$, $T' \subseteq T$ ans $f|_{Z'} - f' \in \mathrm{Hom}(Z', T)$

Our special subspaces of $\mathcal{G}$

$$\begin{aligned}
\mathcal{G} &= \{a_0 x + a_1 x^q; a_0, a_1 \in \mathbb{F}_{q^4}\},\\
\mathcal{R} &= \{a x^q - a^q x; a \in \mathbb{F}_{q^4}\},\\
\mathcal{T} &= \{a x^q - a^q x; a \in W\},\\
\mathcal{D}(Z, P) &= s(ab^q - a^q b)^{-1}\langle a x^q - a^q x, b x^q - b^q x\rangle
\end{aligned}$$

for a 2-dimensional subspace $Z = \langle a, b\rangle$ of W and a point $P = \mathbb{F}_q(0, s)$ of the special solid S (i.e. $s \in \mathbb{F}_{q^4}^\times$).

Notes

- $a x^q - a^q x = a \prod_{\lambda \in \mathbb{F}_q}(x - \lambda a)$ has kernel $\mathbb{F}_q a$
- $\mathcal{D}(Z, P) = \{f \in \mathcal{G}; f(Z) \subseteq \mathbb{F}_q s\}$, as follows by scaling from $\mathcal{D}\big(Z, \mathbb{F}_q(ab^q - a^q b)\big) = \langle a x^q - a^q x, b x^q - b^q x\rangle$

$\Longrightarrow \mathcal{R}, \mathcal{T}$ have the properties required in the theorem.

Going Beyond the Theorem

First Idea

Remove disjoint unions of "rotated" cosets $r(f+\mathcal{T}) = \{(r(ax^q - a^q x; a \in W\}$ from $\mathcal{G}$, where $r \in \mathbb{F}_{q^4}^\times$, $f \in \mathcal{G}$.

Computer experiments [1] for the case $q = 2$ showed that at most 4 rotated cosets of $\mathcal{T}$ can be used. This gives a binary subspace code of size $M = 256 + 4 \cdot 6 + 34 = 314$.

Key idea

Drop the requirement of an exact rearrangement, but make the removal step invariant under the collineation group Σ of $\mathrm{PG}(6, q)$ consisting of all transformations $(x, y) \mapsto (x, ry)$, $r \in \mathbb{F}_{q^4}^\times$ (essentially a Singer subgroup of S).

Then it suffices to check how many new planes through one particular point of S, say $P_1 = \mathbb{F}_q(0, 1)$, can be added in accordance with Condition (3) of the theorem.

If N_1 new planes through P_1 can be added, then $\#\mathcal{N} = N_1(q^3 + q^2 + q + 1)$ new planes can be added in total.

Notes

- Initially this idea was used for $q = 2$, in which case there is only one candidate for the removed set: All cosets $r(\mathcal{R} \setminus \mathcal{T})$, $r \in \mathbb{F}_{16}^{\times}$ (since $\mathcal{R} \setminus \mathcal{T}$ is a single coset).

  The no. of removed planes is $15 \cdot \#(\mathcal{T} \setminus \mathcal{R}) = 15 \times 8 = 120$ (exactly what would be needed for a 2-analogue of the Fano plane, coordinatized such that no plane contained in S).

  The no. of new planes through P_1 that can be added was found by computer to be 11 (out of 14 candidate planes), with 4 different choices for the 11-set.
  $\Longrightarrow M = 256 - 120 + 15 \times 11 + 28 = 329$.

- For $q > 2$ we remove all $q^4 - 1 = (q-1) \times \frac{q^4-1}{q-1}$ rotated cosets
  $$r(f + \mathcal{T}), \quad f \in \mathcal{R} \setminus \mathcal{T}, \quad r \in \mathbb{F}_{q^4}^{\times} / \mathbb{F}_q^{\times}.$$

  This is also the size of the corresponding plane subset of a putative q-analogue of the Fano plane.

The Collision Graph

Definition

The *collision graph* Γ has as its vertices the $q^4 - q$ "candidate new planes" through P_1 that can be added to the expurgated LMRD code without introducing a multiple cover of a line disjoint from S (the relaxed rearrangement condition).

Two vertices (new planes) are adjacent in Γ if they have a line through S (or a point outside S) in common.

The maximal sets of new planes through P_1 that can be added to the expurgated LMRD code are precisely the maximal independent sets (cocliques) of the collision graph.

Notes

- A collision graph may be defined w.r.t. any Σ-invariant set of removed planes (and also LMRD codes other than the Gabidulin code, "non-standard" rearrangements of the free lines into new planes, etc.)
- In the case $q = 2$ considered initially the collision graph turned out to be a K_4 (which has 4 maximum cocliques) by inspection.

Analysis of the Collision Graph

The end of the story

Step 1

Find the representation $N = N(Z, T, g)$ of the vertices of Γ.
The result is:

$N = N(Z, P_1, g)$, where $Z \subset W$ is 2-dimensional and $g\colon Z \to \mathbb{F}_{q^4}$ is of the form

$$g(x) = \delta(a,b)^{-1}\left(\lambda(dx^q - d^q x) + \mu(cx^q - c^q x)\right) = \frac{\delta(\lambda d + \mu c, x)}{\delta(a,b)}$$

with $\lambda \in \mathbb{F}_q^\times$, $\mu \in \mathbb{F}_q$ ($q^4 - q$ choices for N).

Step 2

Translate the collision condition into Algebra.
The points outside S covered by N are

$$\mathbb{F}_q\left(x, \frac{\delta(\lambda d + \mu c, x)}{\delta(a,b)} + \nu\right), \quad \mathbb{F}_q x \in Z,\ \nu \in \mathbb{F}_q;$$

alltogether $(q+1)q$ choices.

New planes corresponding to the same point $\mathbb{F}_q(d + \mu c)$ ($q - 1$ different choices for λ) do not collide, and we can reduce the analysis to collisions between two such plane "bundles".

Geometric View

$\mathbb{F}_q(d + \mu c)$ and Z generate a plane E of $\mathrm{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q) \cong \mathrm{PG}(3, q)$, which meets the trace-zero plane W in a line. This sets up a bijection between the $\frac{q^4-q}{q-1} = q^3 + q^2 + q$ plane bundles and the planes $E \neq W$ of $\mathrm{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$

Then use that $x \mapsto (x^q - x)^{q-1}$ forms a complete invariant for the orbits of $\mathrm{AGL}(1, q) = \{x \mapsto \lambda x + \nu; \lambda \in \mathbb{F}_q^\times, \nu \in \mathbb{F}_q\}$ acting on $\mathbb{F}_{q^4}$.

Result

Two plane bundles $N(Z, P_1, \mathbb{F}_q^\times g)$, $N(Z', P_1, \mathbb{F}_q^\times g')$ represented by planes E, E' of $\mathrm{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ have collisions between them if and only if

$$\frac{\delta(E)}{\delta(Z)^{q+1}} = \frac{\delta(E')}{\delta(Z')^{q+1}}.$$

$\Longrightarrow$ The collision graph between planes bundles is a union of complete graphs, one for each value taken by the σ-*invariant* $\sigma(E) = \delta(E)/\delta(Z)^{q+1}$.

Step 3

Explicit computation of the σ-invariant.

Use that every plane of $\mathrm{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ has the form $E = aW$ for some $a \in \mathbb{F}_{q^4}^\times$ (e.g. by Singer's Theorem) and $Z = W \cap aW$. The quantities $\delta(W)$ and $\delta(Z) = \delta(W \cap aW)$ can be determined from the corresponding subspace polynomials.

Result

For a plane $E = aW \neq W$ of $\mathrm{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ we have

$$\sigma(E)^{q-1} = 1 - \frac{a^{(q-1)(q^2+1)} - 1}{a^{q-1} - 1}.$$

This shows that there are always collisions, viz. between planes of the form $E = a^{q+1}W$, for which $\sigma(E)^{q-1} = 1$ and hence $\sigma(E) = \mathbb{F}_q$.

There are $q^2 + 1$ such planes (including W), forming a dual ovoid (more precisely, a dual elliptic quadric) in $\mathrm{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q) \cong \mathrm{PG}(3, q)$.

$\Longrightarrow$ No q-analogue of the Fano plane can be constructed in this way.

Last Step

Determine the values of $E \mapsto \sigma(E)$ and their multiplicities.

Lemma

$E \mapsto \sigma(E)$ maps all dual ovoid planes to the point $\mathbb{F}_q = \mathbb{F}_q 1$ (hence the multiplicity of $\mathbb{F}_q$ is q^2) and is one-to-one on the complementary set of planes.

Hence the collision graph on bundles of new planes consists of a K_{q^2} and $q^3 + q$ isolated vertices and has maximum coclique size $q^3 + q + 1$.

Proof of the lemma.

The statement is equivalent to

$$\frac{x-1}{y-1} \neq \frac{x^{q^2+1}-1}{y^{q^2+1}-1} \qquad (\star)$$

for any pair of distinct elements $x, y \in \mathbb{F}_{q^4}^{\times}$ that are $(q-1)$-th powers but not (q^2+1)-th roots of unity.

Assume by contradiction that equality holds in $(\star)$ for some pair x, y.

Proof cont'd.

$$\Longrightarrow \frac{x-1}{y-1} = \left(\frac{x-1}{y-1}\right)^{q^2} = \frac{x^{q^2}-1}{y^{q^2}-1},$$

since right-hand side of $(\star)$ is in the subfield $\mathbb{F}_{q^2}$.

The two equations can be rewritten as

$$\sum_{i=0}^{q^2} x^i = \frac{x^{q^2+1}-1}{x-1} = \frac{y^{q^2+1}-1}{y-1} = \sum_{i=0}^{q^2} y^i,$$

$$\sum_{i=0}^{q^2-1} x^i = \frac{x^{q^2}-1}{x-1} = \frac{y^{q^2}-1}{y-1} = \sum_{i=0}^{q^2-1} y^i,$$

and together imply $x^{q^2} = y^{q^2}$ and hence $x = y$; contradiction. $\square$

Theorem (H.-Kiermaier, 2015)

1. *There exists a q-ary $(7, q^8 + q^5 + q^4 - q - 1, 4; 3)$ subspace code $\mathcal{C}$ with the following additional properties:*
   - (i) *The planes in $\mathcal{C}$ meet a fixed 3-flat S of $\mathrm{PG}(6, q)$ in at most a point.*
   - (ii) *$\mathcal{C}$ is invariant under a Singer group of S (acting trivially on a complementary plane).*
2. *There exists a ternary $(7, 6973, 4; 3)$ subspace code.*

Proof.

(1)–(3) It only remains to check the size of $\mathcal{C}$.

$$\begin{aligned}\#\mathcal{C} &= q^8 - (q^4 - 1)q^3 + (q^3 + q + 1)(q - 1)(q^3 + q^2 + q + 1)\\ &= q^8 + (q^4 - 1)(q + 1) = q^8 + q^5 + q^4 - q - 1\end{aligned}$$

(4) (Non-exhaustive) computer search for extensions of the distinguished $(7, 6801, 4; 3)$ subcode $\mathcal{C}_0$. $\square$

Further Notes/Open Problems

- It can be shown that $\mathcal{C}$ can be extended by $q^2 + 1$ further planes meeting the special solid $S \triangleq \mathbb{F}_{q^4}$ in the lines of a spread (in fact the standard spread formed by the 1-dimensional subspaces of $\mathbb{F}_{q^4}/\mathbb{F}_{q^2}$).
- The extension problem of $\mathcal{C}_0$ is closely related to the maximal size of partial spreads contained in the q different regular Singer line orbits of $\mathrm{PG}(3, q)$. What is known about these sizes?
- So far the extension problem for $\mathcal{C}$ or $\mathcal{C}_0$ has been solved only in the smallest case $q = 2$, where the answer is $M = 329$.
- Generalize our approach to other subspace code parameters. The case $v = 8$, $k = 3$ (and $d = 4$) seems the most appropriate. M.Sc. student J. Ai of Zhejiang University has shown by experimental study that for $q = 2$ a subspace code of size $M = 1286$ can be obtained in this way.
- Find q-analogues of the Fano plane by applying our method to other MRD codes than the Gabidulin code, or to appropriate smaller-than-MRD codes.

Thank You

Outline

R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung.
Network information flow.
IEEE Transactions on Information Theory, 46(4):1204–1216, July 2000.

M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, and A. Wassermann.
Existence of q-analogs of Steiner systems.
Preprint arXiv:1304.1462 [math.CO], Apr. 2013.

M. Braun and J. Reichelt.
q-analogs of packing designs.
Journal of Combinatorial Designs, 22(7):306–321, July 2014.
Preprint arXiv:1212.4614 [math.CO].

P. Delsarte.
Bilinear forms over a finite field, with applications to coding theory.
Journal of Combinatorial Theory, Series A, 25:226–241, 1978.

T. Etzion and N. Silberstein.

Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams.

IEEE Transactions on Information Theory, 55(7):2909–2919, July 2009.

E. M. Gabidulin.

Theory of codes with maximum rank distance.

Problems of Information Transmission, 21(1):1–12, 1985.

T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong.

A random linear network coding approach to multicast.

IEEE Transactions on Information Theory, 52(10):4413–4430, Oct. 2006.

T. Honold and M. Kiermaier.

On putative q-analogues of the Fano plane and related combinatorial structures.

Preprint, Feb. 2015.

T. Honold, M. Kiermaier, and S. Kurz.

Optimal binary subspace codes of length 6, constant dimension 3 and minimum subspace distance 4.

To appear in the proceedings volume of the 11th International Conference on Finite Fields and their Applications (Magdeburg, July 22–26, 2013), AMS Contemporary Mathematics Series, Vol. 632, 2015. Preprint arXiv:1311.0464 [math.CO], Nov. 2013.

R. Koetter and F. Kschischang.

Coding for errors and erasures in random network coding.

IEEE Transactions on Information Theory, 54(8):3579–3591, Aug. 2008.

S.-Y. R. Li, R. W. Yeung, and N. Cai.

Linear network coding.

IEEE Transactions on Information Theory, 49(2):371–381, Feb. 2003.

H. Liu and T. Honold.

Poster: A new approach to the main problem of subspace coding.

In *9th International Conference on Communications and Networking in China (ChinaCom 2014, Maoming, China, Aug. 14–16)*, pages 676–677, 2014.

Full paper available as arXiv:1408.1181 [math.CO].

R. M. Roth.

Maximum-rank array codes and their application to crisscross error correction.

IEEE Transactions on Information Theory, 37(2):328–336, Mar. 1991.

Comments by Emst M. Gabidulin and Author's Reply, ibid. 38(3):1183, 1992.

D. Silva, F. Kschischang, and R. Koetter.

A rank-metric approach to error control in random network coding.

IEEE Transactions on Information Theory, 54(9):3951–3967, Sept. 2008.

A.-L. Trautmann and J. Rosenthal.

New improvements on the Echelon-Ferrers construction.

In A. Edelmayer, editor, *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2010)*, pages 405–408, Budapest, Hungary, 5–9 July 2010.

Reprint arXiv:1110.2417 [cs.IT].

R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang.

Network coding theory.

Foundations and Trends in Communications and Information Theory, 2(4/5):241–381, 2006.