Constant-Dimension Codes Exceeding the LMRD Code Bound

Joint work with Ai Jingmei and Liu Haiteng

Thomas Honold

Department of Information Science and Electronics Engineering
Zhejiang University

Network Coding and Designs
Dubrovnik, HRvatska
April 4–8, 2016

Outline

Outline

Subspace Coding

The constant-dimension case

Definition

A q-ary $(v, M, d; k)$ *(constant-dimension) subspace code* is a set $\mathcal{C}$ of k-dimensional subspaces of a v-dimensional vector space over $\mathbb{F}_q$ with size $\#\mathcal{C} = M$ and minimum subspace distance $\mathrm{d_s}(\mathcal{C}) := \min\{\mathrm{d_s}(X, Y); X, Y \in \mathcal{C}, X \neq Y\} = d$.

Subspace metric

$\mathrm{d_s}(X, Y) = \dim(X + Y) - \dim(X \cap Y) = 2k - 2\dim(X \cap Y)$

Geometric meaning

$d = 2\delta \in 2\mathbb{Z}$, and $t = k - \delta + 1$ is the smallest positive integer such that any t-dimensional subspace of V (or $t-1$-flat of $\mathrm{PG}(V) \cong \mathrm{PG}(v-1, \mathbb{F}_q)$) is covered by/contained in/incident with at most one member of $\mathcal{C}$.

Main Problem

For a given prime power $q > 1$ and given positive integers v, δ, k with $2 \leq \delta \leq k \leq v/2$ determine the maximum size $M = \mathrm{A}_q(v, 2\delta; k)$ of a q-ary $(v, M, 2\delta; k)$ subspace code.

The Case $k = 3$, $d = 4$

Plane subspace codes

The "easiest" "nontrivial" case

A q-ary $(v, M, 4; 3)$ subspace code is a set of M distinct planes in $\mathrm{PG}(V) \cong \mathrm{PG}(v-1, \mathbb{F}_q)$ mutually intersecting in at most a point (covering every line at most once).

Known exact results

1. $\mathrm{A}_q(5, 4; 3) = q^3 + 1$ ($\triangleq$ max. partial line spreads in $\mathrm{PG}(4, \mathbb{F}_q)$)
2. $\mathrm{A}_2(6, 4; 3) = 77$ (5 isomorphism types)
3. $\mathrm{A}_2(13, 4; 3) = 1\,597\,245$ (many isomorphism types)

The $(13, 1\,597\,245, 4; 3)$ codes in Case (3) form an exact line cover in $\mathrm{PG}(12, \mathbb{F}_2)$ (2-analog of a Steiner triple system on 13 points) and are invariant under the normalizer of a Singer group of $\mathrm{PG}(12, \mathbb{F}_2)$, which has order $(2^{13} - 1) \times 13 = 106\,483$.

It is not known whether an exact line cover (consisting of planes) in $\mathrm{PG}(6, \mathbb{F}_2)$ (2-analog of the Fano plane) or in $\mathrm{PG}(8, \mathbb{F}_2)$ (2-analog of the affine plane of order 3) exists.

Known Upper Bounds for $\mathrm{A}_q(v,4;3)$

Packing bound

$$\#\mathcal{C} \leq \frac{\text{total no. of lines}}{\text{no. of lines in a plane}} = \frac{(q^v-1)(q^{v-1}-1)}{(q^3-1)(q^2-1)}$$

with equality iff $\mathcal{C}$ forms an exact line cover (q-analog of a Steiner triple system on v points).

Best known upper bound

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

$$= \begin{cases} (q^3+1)^2 & \text{if } v = 6, \\ q^8+q^6+q^5+q^4+q^3+q^2+1 & \text{if } v = 7, \\ q^{2v-6}+q^{2v-8}+q^{2v-9}+\cdots & \text{if } v \geq 8. \end{cases}$$

A necessary condition for the existence of an exact cover is $v \equiv 1,3 \pmod 6$ (independently of q).

Known Lower Bounds for $\mathrm{A}_q(v,4;3)$

Mostly arising from constructions

- $\mathrm{A}_q(6,4;3) \geq q^6 + 2q^2 + 2q + 1$ for $q \geq 3$;
- $\mathrm{A}_2(7,4;3) \geq 333$, $\mathrm{A}_3(7,4;3) \geq 6977$, and $\mathrm{A}_q(7,4;3) \geq q^8 + q^5 + q^4 + q^2 - q$ for general q;
- $\mathrm{A}_q(v,4;3) \geq q^{2v-6} + \begin{bmatrix} v-3 \\ 2 \end{bmatrix}_q = q^{2v-6} + q^{2v-10} + \cdots$ for q large enough (*LMRD code bound*, constructive);
- $\mathrm{A}_q(v,4;3) \sim \frac{(q^v-1)(q^{v-1}-1)}{(q^3-1)(q^2-1)}$ for v large enough (packing bound, non-constructive).

The binary case

v	6	7	8	9	10	11
LMRD	71	291	1179	4747	19051	76331
EA+Ext	**77**	**329**	**1259**	**5014**	**20517**	**79306**
best known	77	333	1326	5986	23870	97526
upper bound	77	381	1493	6205	24698	99718

EA+Ext: Expurgation-Augmentation plus further extension by planes meeting the special flat S in a line

The Echelon-Ferrers Construction

The Echelon-Ferrers Multilevel Construction and its refinements (T. Etzion, N. Silberstein, J. Rosenthal, A. Horlemann-Trautmann) provides the best known lower bound for subspace codes with general parameters.

Idea (for the plane case)

Take

$$\mathcal{C} = \begin{pmatrix} 1 & 0 & 0 & * & \dots & * \\ 0 & 1 & 0 & * & \dots & * \\ 0 & 0 & 1 & * & \dots & * \end{pmatrix} \uplus \begin{pmatrix} 1 & * & * & 0 & 0 & * & \dots & * \\ 0 & 0 & 0 & 1 & 0 & * & \dots & * \\ 0 & 0 & 0 & 0 & 1 & * & \dots & * \end{pmatrix} \uplus \cdots$$

with the maximum number of planes from each Schubert cell.
$\Longrightarrow \#\mathcal{C} = 2^{2(v-3)} + 2^{2(v-5)} + \cdots$ in the binary case.

LMRD code bound

$$\#\mathcal{C} \leq 2^{2(v-3)} + \begin{bmatrix} v-3 \\ 2 \end{bmatrix}_2$$

Outline

Main Theorem (Ai-H.-Liu, 2016)

(i) *For* $v \equiv 7 \pmod 8$*, there exists a* Σ_v*-invariant* $(v, M, 4; 3)_2$ *subspace code with*

$$M \geq 2^{2(v-3)} + \frac{9}{8}\begin{bmatrix} v-3 \\ 2 \end{bmatrix}_2,$$

and consequently we have $\mathrm{A}_2(v, 4; 3) \geq 2^{2(v-3)} + \frac{9}{8}\left[\begin{smallmatrix} v-3 \\ 2 \end{smallmatrix}\right]_2$ *in this case.*

(ii) *For* $v \equiv 3 \pmod 8$*,* $v \geq 11$*, there exists a* Σ_v*-invariant* $(v, M, 4; 3)_2$ *subspace code with*

$$M \geq 2^{2(v-3)} + \frac{81}{64}\begin{bmatrix} v-3 \\ 2 \end{bmatrix}_2,$$

and consequently we have $\mathrm{A}_2(v, 4; 3) \geq 2^{2(v-3)} + \frac{81}{64}\left[\begin{smallmatrix} v-3 \\ 2 \end{smallmatrix}\right]_2$ *in this case.*

Maximum Net Gain Computations

v	n	#G-orbits	N_1	$(N_1)_{\mathrm{LMRD}}$	$\#\mathcal{C}$	W
7	4	1	3	2.33	$2^8 + 45$	$\langle 1, \alpha, \alpha^2 \rangle$
8	5	1	3	5.00	$2^{10} + 93$	$\langle 1, \alpha, \alpha^2 \rangle$
9	6	7	12	10.33	$2^{12} + 756$	$\langle 1, \alpha, \alpha^2 \rangle$
10	7	15	20	21.00	$2^{14} + 2540$	$\langle 1, \alpha, \alpha^{22} \rangle$
11	8	53	54	42.33	$2^{16} + 13770$	$\langle 1, \alpha^{17}, \alpha^{34} \rangle$
12	9	177	93	85.00	$2^{18} + 47523$	$\langle 1, \alpha^3, \alpha^{71} \rangle$
13	10	633	234	170.33	$2^{20} + 239382$	$\langle 1, \alpha, \alpha^{49} \rangle$
14	11	513	379	341.00	$2^{22} + 775813$	$\langle 1, \alpha^3, \alpha^{419} \rangle$
15	12	34	924	682.33	$2^{24} + 3783708$	$\langle 1, \alpha^{195}, \alpha^{1170} \rangle$
16	13	240	1526	1365.00	$2^{26} + 12499466$	$\langle 1, \alpha^{25}, \alpha^{1208} \rangle$

N_1 local max. net gain of the EA method

$(N_1)_{\mathrm{LMRD}}$ local max. net gain equivalent of the LMRD code bound

Outline

Coordinate-Free Represenation

From now on we restrict ourselves to $k = 3$, $d = 4$, $q = 2$.

Ambient space

$V = W \times \mathbb{F}_{2^n}$, where $n = v - 3$ and W is a 3-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$ (plane of $\mathrm{PG}(n-1, \mathbb{F}_2)$)

Gabidulin MRD codes

$\mathcal{G} = \{x \mapsto a_0x + a_1x^2; a_0, a_1 \in \mathbb{F}_{2^n}\} \subset \mathrm{Hom}(W, \mathbb{F}_{2^n})$
(for $n \geq 6$ this definition depends on the choice of W)

Lifted Gabidulin LMRD codes

$\mathcal{L}$ = set of all graphs (in the sense of Real Analysis) Γ_f, $f \in \mathcal{G}$; i.e.,

$$G(a_0, a_1) = \left\{(x, a_0x + a_1x^2); x \in W\right\} \subset W \times \mathbb{F}_{2^n}$$

Lines covered by $G(a_0, a_1)$

These have the form Γ_g, where g is the restriction of $a_0x + a_1x^2$ to a 2-dimensional subspace $Z \subset W$, and are disjoint from the special flat

$$S = \{0\} \times \mathbb{F}_{2^n} \cong \mathrm{PG}(n-1, \mathbb{F}_2).$$

The LMRD Code Bound

Valid for any subspace code $\mathcal{C}$ containing an LMRD code

Observation

The planes in $\mathcal{L}$ (more generally, the planes in any lifted MRD code with the same parameters as $\mathcal{G}$) form an exact cover of the set of lines of $\mathrm{PG}(v-1,\mathbb{F}_2)$ disjoint from S.

$\Longrightarrow$ No plane meeting S in a point can be added to $\mathcal{L}$ without decreasing the minimum subspace distance (since such planes contain lines disjoint from S, hence leading to a multiple cover of some line).

$$\Longrightarrow \#\mathcal{C} \leq \#\mathcal{L} + \text{no. of lines in } S = 2^{2v-6} + \begin{bmatrix} v-3 \\ 2 \end{bmatrix}_2$$

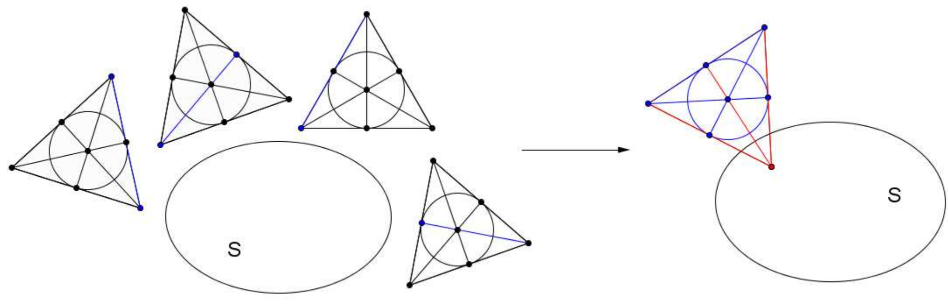
for any subspace code $\mathcal{C} \supseteq \mathcal{L}$.

Can the bound be reached?

For this the lines $L \subset S$ must be matched to planes $E \supset L$ in such a way that planes meeting in S (i.e., the corresponding lines meet) have no point outside S in common.

The answer is yes for $v \leq 11$ and probably in general.

Outline


S
S

Expurgation-Augmentation

The basic idea

Removing M_1 planes from $\mathcal{L}$ ("expurgating" $\mathcal{L}$) "frees" $7M_1$ lines disjoint from the special flat S. It is at least conceivable that the free lines can be rearranged, 4 lines at a time, into $7M_1/4$ new planes meeting S in a point.

Adding these planes to the expurgated LMRD code ("augmenting" the code) then produces a new subspace code $\mathcal{C}$ of size

$$\#\mathcal{C} = \#\mathcal{L} + 3M_1/4 > \#\mathcal{L}.$$

If we are "lucky", the new planes do not introduce a multiple cover of some line meeting S in a point.

If we are even more "lucky", the additional number of planes meeting S in a line that can be added to the code does not decrease (or decreases only slightly).

$\Longrightarrow \mathcal{C}$ improves on $\mathcal{L}$.

After some further work

There exists a distinguished 3-dimensional subspace $\mathcal{T} \subset \mathcal{G}$, viz.

$$\mathcal{T} = \{wx^2 + w^2x; w \in W\},$$

such that the corresponding 8 planes Γ_f, $f \in \mathcal{T}$, have the desired property.

The 14 new planes obtained by rearranging the 8×7 lines in Γ_f are

$$E = E(Z, P, g) = \bigl\{(x, g(x) + y); x \in Z, y \in P\bigr\},$$

where $Z = \langle a, b\rangle \subset W$ is 2-dimensional (7 choices), $g(x) = cx^2 + c^2x$ with $c \in W/Z$ (2 choices) and $P = \mathbb{F}_2(ab^2 + a^2b)$ (the intersection point of E and S).

Net gain: $\quad 14 - 8 = 6$ planes

Example ($v = 6$)

One of the five optimal $(6, 77, 4; 3)$ codes can be constructed in this way without using a computer. In this case $V = \mathbb{F}_8 \times \mathbb{F}_8$ (i.e. $W = \mathbb{F}_8$) and $\mathcal{T} = \{wx^2 + w^2x; w \in \mathbb{F}_8\}$.

Refinements for $v = 7$

For $v = 7$ the ambient space can be taken as $V = W \times \mathbb{F}_{16}$, with W the trace-zero subspace of $\mathbb{F}_{16}$.

1. Remove several additive cosets of $\mathcal{T}$ in $\mathcal{G}$ (maximum 2 cosets, netgain 12 planes).
2. Remove pairwise disjoint "rotated" cosets $r(\mathcal{T} + f)$, $f \in \mathcal{G}$, $r \in \mathbb{F}_{16}^{\times}$ (maximum 4 cosets, netgain 24 planes)
3. Remove all $\#\mathbb{F}_{16}^{\times} = 15$ rotations of the special coset $\mathcal{T} + cx^2 + c^2x$, $\mathrm{Tr}_{\mathbb{F}_{16}/\mathbb{F}_2}(c) = 1$, but drop the requirement of exact rearrangement of the free lines (net gain $15 \times 11 - 15 \times 8 = 45$ planes)

Why is Method (3) so much better?

- The expurgated code is invariant under the group Σ_v of all collinations $(x, y) \mapsto (x, ry)$, $r \in \mathbb{F}_{16}^{\times}$ (acting as a Singer group on $\mathrm{PG}(S) \cong \mathrm{PG}(3, \mathbb{F}_2)$). $\implies$ Simplification
- Surprisingly (at that time) as much as 11 out of 14 candidate new planes could be added through each point of S.

A Strange Invariant

determining the collision graph at a point of S

Collision graph

Vertices: the 14 new planes E through a fixed point of S, say $P_1 = \mathbb{F}_2(0,1) \in W \times \mathbb{F}_{16}$.
Edges: E_1 and E_2 are adjacent if they have a line through P_1 (or a point outside S) in common.

In the case $v = 7$ the graph turned out to consist of a K_4 and 10 isolated vertices ($\Longrightarrow$ independence number 11).

δ-invariant (last Dickson invariant)

Represent $\mathrm{PG}(n-1,\mathbb{F}_q)$ as $\mathrm{PG}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. For any $\mathbb{F}_q$-subspace U define the point $\delta(U)$ as the product of all points in U.

Note that for a line $Z = \langle a,b\rangle = \{a,b,a+b\} \in \mathrm{PG}(n-1,\mathbb{F}_2)$ we have $\delta(Z) = ab(a+b) = ab^2 + a^2b = \begin{vmatrix} a & b \\ a^2 & b^2 \end{vmatrix}$.

σ-invariant

For a plane E in $\mathrm{PG}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ intersecting W in a line Z define $\sigma(E) = \delta(E)/\delta(Z)^{q+1}$.

Theorem

1. *The 14 new planes through P_1 have the form $E(Z, P_1, g)$ with $Z = \langle a, b\rangle \subset W = \langle a, b, c\rangle \subset \mathbb{F}_{16} = \langle a, b, c, d\rangle$ and*

$$g(x) = \frac{(d+\mu c)x^2 + (d+\mu c)^2 x}{ab^2 + a^2 b}, \quad \mu \in \mathbb{F}_2.$$

   $E(Z, P_1, g) \mapsto Z + \mathbb{F}_q(d + \mu c)$ gives a parametrization of these new planes by the 14 planes $E \neq W$ in $\mathrm{PG}(S) \cong \mathrm{PG}(3, \mathbb{F}_2)$.

2. *Two new planes $E(Z, P_1, g)$, $E(Z', P_1, g')$ collide if and only if their corresponding planes E, E' have the same σ-invariant.*

Theorem (explicit computation of $\sigma(E)$ for $n = 4$)

For a plane $E = aW \neq W$ of $\mathrm{PG}(\mathbb{F}_{16}/\mathbb{F}_2)$ we have

$$\sigma(E) = a + a^2 + a^3 + a^4.$$

A further analysis shows that $E \mapsto \sigma(E)$ takes the value $\mathbb{F}_2 = \mathbb{F}_2 1$ precisely 4 times (on the planes of the form $a^3 W$) and is one-to-one on the complementary set of 10 planes.

The Case $v > 7$

or $n = \dim(S) = v - 3 > 4$

Parallels

The number of new planes meeting S in P_1 that can be added to the expurgated code (independence number of the collision graph) still equals the number of values taken by the σ-invariant.

Changes

- Dependence on the plane orbit of W in $\mathrm{PG}(\mathbb{F}_{2^n}/\mathbb{F}_2) \cong \mathrm{PG}(n-1, \mathbb{F}_2)$ (under the Singer+Frobenius action)
  $\Longrightarrow$ Exponential growth
- No explicit formula for the σ-invariant
- There are $2^{n-3} - 1$ cosets $\mathcal{T} + cx^2 + c^2x$, $c \in \mathbb{F}_{2^n} \setminus W$ suitable for removal. Any combination has to be considered.
  $\Longrightarrow$ Doubly exponential growth

For a plane orbit $[W]$ let $T_1, \dots, T_m$ ($m = 2^{n-3} - 1$) be the solids in $\mathrm{PG}(\mathbb{F}_{2^n}/\mathbb{F}_2)$ above W and $\mathbb{F}_{2^n}^\times = \{y_1, \dots, y_{2^n-1}\}$. Define an integral $m \times (2^n - 1)$ matrix $\mathbf{M}_W = (m_{ij})$ by

$$m_{ij} = \#\{E \in T_i; E \neq W \wedge \sigma(E) = y_j\}.$$

Combinatorial optimization problem

Determine the max. local net gain

$$N_1 = \max_{[W]} \max_{\mathbf{x} \in \{0,1\}^m} \bigl(\mathrm{w}_{\mathrm{Ham}}(\mathbf{x}\mathbf{M}_W) - 8\mathrm{w}_{\mathrm{Ham}}(\mathbf{x})\bigr).$$

Example ($v = 8$)

In this case $n = 5$ and the $\begin{bmatrix}5\\3\end{bmatrix}_2 = 155$ planes in $\mathrm{PG}(\mathbb{F}_{32}/\mathbb{F}_2)$ form a single Singer+Frobenius orbit.
Representing $\mathbb{F}_{32}$ as $\mathbb{F}_2[\alpha]$ with $\alpha^5 + \alpha^2 + 1 = 0$, we get

$$\mathbf{M} = \left(\begin{array}{ccc|ccccccccc|cccc} 2 & 2 & 2 & 1 & \dots & 1 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 0 & \dots & 0 & 1 & \dots & 1 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 0 & \dots & 0 & 0 & \dots & 0 & 1 & \dots & 1 & 0 & 0 & 0 & 0 \end{array}\right) \in \mathbb{Z}^{3\times 31}$$

with $\alpha^{23}, \alpha^{25}, \alpha^{28}$ as the first 3 column labels. $\Longrightarrow N_1 = 3$

Experimental Study

using SAGE (`www.sagemath.org`)

v	7	8	9	10	11
n	4	5	6	7	8
N_1	3	3	12	20	≥ 44
$(N_1)_{\text{LMRD}}$	2.33	5	10.33	21	42.33

N_1 Local max. net gain of the EA method

$(N_1)_{\text{LMRD}}$ Local net gain required to equalize the LMRD code bound

Notes

- Algorithm used: Essentially exhaustive search through all Singer+Frobenius orbits and coset combinations. (For $n = 8$ there are 53 orbits and $2^{2^5-1} - 1 = 2^{31} - 1$ coset combinations.
- $\mathcal{C}$ can be further extended by planes meeting S in a line, but computing maximal such extensions is not feasible.

Outline

MOORE's Identity . . .

2-Analog of the Vandermonde determinant evaluation

$$\delta(X_1,\dots,X_k)=\begin{vmatrix} X_1 & X_2 & \dots & X_k \\ X_1^2 & X_2^2 & \dots & X_k^2 \\ X_1^{2^2} & X_2^{2^2} & \dots & X_k^{2^2} \\ \vdots & \vdots & & \vdots \\ X_1^{2^{k-1}} & X_2^{2^{k-1}} & \dots & X_k^{2^{k-1}} \end{vmatrix}$$

$$=\prod_{\lambda\in\mathbb{F}_2^k\setminus\{\mathbf{0}\}}(\lambda_1X_1+\dots+\lambda_kX_k)\quad\text{in } \mathbb{F}_2[X_1,\dots,X_k].$$

Moore's Identity can be proved by induction on k, using

$$\delta(X_1,\dots,X_k)=\delta(X_1,\dots,X_{k-1})\prod_{\lambda\in\mathbb{F}_2^{k-1}}(X_k+\lambda_1X_1+\dots+\lambda_{k-1}X_{k-1}) \tag{1}$$

(in virtually the same way as Vandermonde's Identity).

… Leading to Subspace Polynomials

Suppose U is a k-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_2^n$ with basis $\beta_1, \dots, \beta_k$

$$\implies \prod_{u \in U}(X+u) = \prod_{\lambda \in \mathbb{F}_2^k}(X + \lambda_1\beta_1 + \dots + \lambda_k\beta_k)$$
$$= \frac{\delta(\beta_1, \dots, \beta_k, X)}{\delta(\beta_1, \dots, \beta_k)} = \sum_{i=0}^{k} a_i X^{2^i} \in \mathbb{F}_{2^n}[X].$$

Definition

The *subspace polynomial of U* is defined as $\mathrm{s}_U(X) = \prod_{u \in U}(X+u)$.

Properties

- By unique factorization, U is determined by $\mathrm{s}_U(X)$.
- $\mathrm{s}_U(X)$ is a monic, separable (i.e., $a_0 \neq 0$), linearized polynomial in $\mathbb{F}_{2^n}[X]$ of symbolic degree $k = \dim U$.
- Conversely, a polynomial with these properties is a subspace polynomial of $U \subseteq \mathbb{F}_{2^n}$ iff it splits into linear factors in $\mathbb{F}_{2^n}[X]$.

DICKSON Invariants

Definition (from Modular Invariant Theory)

The coefficients of the generic subspace polynomial $\prod(X+\lambda_1 X_1+\cdots+\lambda_k X_k)$ are called *Dickson invariants* and denoted by $\delta_i^{(k)}(X_1,\dots,X_k)$, $1\leq i\leq k$. The indexing is mutatis mutandis the same as for the elementary symmetric polynomials.

Theorem (Dickson)

The ring of $\mathrm{GL}(k,\mathbb{F}_2)$*-invariants in* $\mathbb{F}_2[X_1,\dots,X_k]$ *is freely generated by* δ_i^k*,* $1\leq i\leq k$*.*

Important Consequence

The "Dickson invariant" $\delta_i(U)=\delta_i^{(k)}(\beta_1,\cdots\beta_k)$ is well-defined, and

$$\mathrm{s}_U(X)=X^{2^k}+\delta_1(U)X^{2^k-1}+\cdots+\delta_{k-1}(U)X^2+\delta_k(U)X.$$

For our purposes the most important of these invariants is the *last Dickson invariant*

$$\delta(U)=\delta_k(U)=\prod_{u\in U}u.$$

Examples

Point Polynomials

$\mathrm{s}_P(X) = X(X+a) = X^2 + aX$
for any point $P = \mathbb{F}_2 a$ in $\mathrm{PG}(\mathbb{F}_{2^n}/\mathbb{F}_2) \cong \mathrm{PG}(n-1, \mathbb{F}_2)$

Line Polynomials

For lines $L = \langle a, b \rangle = \{a, b, a+b\}$ in $\mathrm{PG}(\mathbb{F}_{2^n}/\mathbb{F}_2)$ we have

$$\begin{aligned} \mathrm{s}_L(X) &= \left(X^2 + (b^2+ab)X\right) \circ (X^2 + aX) \\ &= (X^2+aX)^2 + (b^2+ab)(X^2+aX) \\ &= X^4 + (a^2+ab+b^2)X^2 + (ab^2+a^2b)X \end{aligned}$$

$\Longrightarrow \delta_1(L) = a^2 + ab + b^2$, $\delta_2(L) = \delta(L) = ab^2 + a^2 b = ab(a+b)$.

Examples (cont'd)

Subspace polynomials in $\mathrm{PG}(\mathbb{F}_{16}/\mathbb{F}_2) \cong \mathrm{PG}(3, \mathbb{F}_2)$

Plane polynomials:

$$
\begin{array}{ll}
W_0 = \{x \in \mathbb{F}_{16}; \mathrm{Tr}(x) = 0\}: & \mathrm{s}_{W_0}(X) = X^8 + X^4 + X^2 + X \\
W = rW_0,\ r \in \mathbb{F}_{16}^\times: & \mathrm{s}_W(X) = X^8 + r^4 X^4 + r^6 X^2 + r^7 X
\end{array}
$$

Line polynomials:

Write $\mathbb{F}_{16}^\times = \langle \xi \rangle$, $\mathbb{F}_4^\times = \langle \omega \rangle$ with $\omega = \xi^5$.
There are 2 Singer+Frobenius line orbits, $[\mathbb{F}_4]$ and $[L_0]$, $L_{)} = \xi^{10}\langle 1, \xi \rangle$, with sizes 5, 30 and line polynnomials

$$\mathrm{s}_{\mathbb{F}_4}[X] = X^4 + X. \quad \mathrm{s}_{L_0}(X) = X^4 + X^2 + \omega X,$$

respectively. The remaining line polynomials are determined from $\mathrm{s}_{rL}(X) = X^4 + r^2 a_1 X^2 + r^3 a_0 X$, $\mathrm{s}_{L^2}(X) = X^4 + a_1^2 X^2 + a_0^2 X$.

Ore's Work

On a Special Class of Polynomials, TAMS 35(1933)

The ring of 2-polynomials

With respect to composition $a(X) \circ b(X) = a\big(b(X)\big)$ ("symbolic multiplication"), the 2-polynomials in $\mathbb{F}_{2^n}[X]$ form a ring L_n. Via $X^{2^i} \mapsto Y^i$, the ring L_n is isomorphic to the skew polynomial ring $\mathbb{F}_{2^n}[Y;\phi]$ with $\phi(a) = a^2$.

The linear map view of 2-polynomials

$\mathrm{End}(\mathbb{F}_{2^n}/\mathbb{F}_2) \cong L_n/(X^{2^n} + X) \cong \mathbb{F}_2[Y;\phi]/(Y^n + 1)$.

Three subspaces associated with U

- $U^\perp$ The orthogonal subspace of U with respect to the trace bilinear form $(x, y) \mapsto \mathrm{Tr}(xy)$.
- U° The *opposite subspace* of U, defined by $\mathrm{s}_U(X) \circ \mathrm{s}_{U^\circ}(X) = \mathrm{s}_{U^\circ}(X) \circ \mathrm{s}_U(X) = X^{2^n} + X$.
- U^* The *adjoint subspace* of U, which may be defined as the subspace $\langle \delta(V)/\delta(U); V \subseteq U \text{ a hyperplane}\rangle$.

Key Facts

Implicit in Ore's work

Relation between $U^\perp$, U°, U^*

$(U^*)^2 = (U^\circ)^\perp$

Theorem

Let U be a k-subspace of $\mathbb{F}_{2^n}$.

1. *$V \mapsto \delta(V)$ maps the $(k+1)$-subspaces of $\mathbb{F}_{2^n}$ containing U bijectively onto the 1-subspaces of the space $\delta(U)U^\circ$. The induced map from $\mathrm{PG}(\mathbb{F}_{2^n})/U$ to $\mathrm{PG}\big(\delta(U)U^\circ\big)$ is a collineation.*
2. *$V \mapsto \delta(V)$ maps the $(k-1)$-subspaces of $\mathbb{F}_{2^n}$ contained in U bijectively onto the 1-subspaces of $\delta(U)U^*$. The induced map from $\mathrm{PG}(U)$ to $\mathrm{PG}\big(\delta(U)U^*\big)$ is a correlation.*

Sketch of proof.

For Part (1) use $\delta(V) = \mathrm{s}_U(x)\delta(U)$ for any β satisfying $V = U + \mathbb{F}_2 x$, together with $U^\circ = \mathrm{Im}\big(x \mapsto \mathrm{s}_U(x)\big)$. For Part (2) the roles of U, V are reversed. □

A Nice Application to Subspace Codes

Corollary

The k-subspaces $U \subseteq \mathbb{F}_{2^v}$ with fixed last Dickson invariant $\delta(U) = a$, $a \in \mathbb{F}_{2^v}^\times$, form a subspace code $\mathcal{C}(a)$ with minimum distance at least 4.

Notes

- By the corollary, the set of k-subspaces of $\mathbb{F}_2^v$ is partitioned into $2^v - 1$ (possibly empty) subspace codes of minimum distance ≥ 4. Viewed as single codes, these are not very interesting, since they are too small. In the case $k = 3$ the largest of these codes has guaranteed size

$$\#\mathcal{C}(a) \geq \frac{1}{2^v - 1}\begin{bmatrix} v \\ 3 \end{bmatrix}_2 = \frac{(2^{v-1} - 1)(2^{v-2} - 1)}{21} \approx \frac{8}{21} \times \#\mathcal{G}.$$

- Compare the corollary with the Gap Theorem in Ben-Sasson et al. 2014.

Outline

The Collision Space

Theorem

The set of multiple values of $\sigma_W(E) = \delta(E)/\delta(Z)^3$, $Z = E \cap W$, is precisely the $(n-3)$-dimensional subspace $(W^2)^\perp$.

Sketch of proof.

For each of the 7 lines (2-dimensional subspaces) $Z \subset W$, $E \mapsto \sigma_W(E)$ maps the planes $E \supset Z$ bijectively to the points in $\delta(Z)^{-2}Z^\circ$, a space of dimension $n-2$. Using $(Z^*)^2 = (Z^\circ)^\perp$, one can show that $\delta(Z)^{-2}Z^\circ = (Z^2)^\perp$.

$$\Longrightarrow (W^2)^\perp = \bigcap_{Z \subset W} \delta(Z)^{-2}Z^\circ.$$

$\Longrightarrow$ The points in $(W^2)^\perp$ (outside $(W^2)^\perp$) have multiplicity 7 (resp., 1), except for the 7 *missing values* $\delta(W)/\delta(Z)^3$. $\square$

Definition

The space $C_W = (W^2)^\perp \subset \mathbb{F}_{2^n}$ is called *collision space* and the corresponding $m \times m$ submatrix $\mathbf{C}_W$ of $\mathbf{M}_W$ *collision matrix* (relative to W).

Simplified optimization problem

Determine the max. local net gain N_1 as the optimal solution of

$$\begin{array}{ll} \text{Maximize} & \sum_{i=1}^{m}(6-r_i)x_i + \mathrm{w}_{\mathrm{Ham}}(\mathbf{x}\mathbf{C}_W) \\ \text{subject to} & \mathbf{x} \in \{0,1\}^m, \end{array} \tag{2}$$

where $r_1, \dots, r_m$ denote the row sums of $\mathbf{C}_W$.

Example ($v = 9$)

There are 7 plane orbits $[W]$ in $\mathrm{PG}(\mathbb{F}_{64}/\mathbb{F}_2)$ with collision matrices

$$\begin{pmatrix} 1&1&2&1&2&0&1\\ 1&1&0&1&0&0&1\\ 1&1&0&1&0&0&1\\ 1&1&0&1&0&0&1\\ 1&1&0&1&0&0&1\\ 1&1&2&1&2&0&1\\ 1&1&2&1&2&4&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&1&1&1&2\\ 2&2&1&1&1&1&0\\ 0&0&1&1&1&1&0\\ 2&0&1&1&1&1&0\\ 0&2&1&1&1&1&0\\ 2&0&1&1&1&1&2\\ 0&2&1&1&1&1&2 \end{pmatrix}, \begin{pmatrix} 2&1&1&1&1&1&1\\ 0&1&1&1&1&1&1\\ 0&1&1&1&1&1&1\\ 2&1&1&1&1&1&1\\ 2&1&1&1&1&1&1\\ 0&1&1&1&1&1&1\\ 0&1&1&1&1&1&1 \end{pmatrix}, \begin{pmatrix} 1&2&1&1&0&1&1\\ 1&0&1&1&2&1&1\\ 1&0&1&1&0&1&1\\ 1&0&1&1&2&1&1\\ 1&0&1&1&0&1&1\\ 1&2&1&1&2&1&1\\ 1&2&1&1&0&1&1 \end{pmatrix},$$

$$\begin{pmatrix} 2&0&0&1&2&1&0\\ 2&0&2&1&0&1&2\\ 2&2&0&1&0&1&0\\ 0&0&0&1&0&1&2\\ 0&2&2&1&0&1&0\\ 0&2&0&1&2&1&2\\ 0&0&2&1&2&1&0 \end{pmatrix}, \begin{pmatrix} 1&1&0&0&1&0&0\\ 1&1&2&2&1&0&2\\ 1&1&0&0&1&0&0\\ 1&1&2&2&1&0&2\\ 1&1&0&0&1&0&0\\ 1&1&2&2&1&0&2\\ 1&1&0&0&1&4&0 \end{pmatrix}, \begin{pmatrix} 0&2&0&2&0&2&0\\ 2&0&0&2&2&0&0\\ 0&0&2&2&0&0&2\\ 2&0&0&0&0&2&2\\ 0&0&2&0&2&2&0\\ 2&2&2&0&0&0&0\\ 0&2&0&0&2&0&2 \end{pmatrix}. \implies N_1 = 12$$

Outline

Properties of Collision Matrices

1. Only columns of type 1^7, 2^3 or 4^1 can occur. More precisely, a column labeled with $y \in (W^2)^\perp$ has type 1^7 if y is not a missing value of σ_W (i.e., $y \neq \delta(W)/\delta(Z)^3$ for all lines $Z \subset W$), type 2^3 if y is a missing value of multiplicity 1 (i.e., $y = \delta(W)/\delta(Z)^3$ for exactly one line $Z \subset W$), and type 4^1 if y is a missing value of multiplicity 3 (i.e., $y = \delta(W)/\delta(Z)^3$ for three lines $Z \subset W$). Moreover, Type 4^1 does not occur if n is odd, and occurs at most once as a column of $\mathbf{C}_W$ if n is even.

   1^7 if y is not a missing value of σ_W,
   2^3 if y is a missing value of multiplicity 1,
   4^1 if y is a missing value of multiplicity 3.

   (The multiplicity is the number of lines $Z \subset W$ with $y = \delta(W)/\delta(Z)^3$.)

2. The support of each column is a subspace of $\mathbb{F}_{2^n}/W$.

3. All row sums have the same parity, equal to the parity of the number of columns of type 1^7.

Properties of Collision Matrices (Cont'd)

4. The row sum spectrum of $\mathbf{C}_W$ can be computed from the geometric configuration formed by the multiset of $\mu \leq 7$ missing points of σ_W contained in $(W^2)^\perp$ (in terms of the weight distribution of the associated binary linear $[\mu, k]$ code).
5. Plane orbits $[W]$ with a column of type 4^1 in $\mathbf{C}_W$ (equivalently, with a missing point in $(W^2)^\perp$ of multiplicity 3) can be characterized algebraically: They occur iff n is even and are represented by $W = \langle 1, a, b \rangle$ with a, b satisfying $b^2 + b = \omega(a^2 + a)$, where ω is a generator of $\mathbb{F}_4 \subseteq \mathbb{F}_{2^n}$. The missing points in this case are 1 (of multiplicity 3) and $(b + \omega a + x)^{-3}$ for $x \in \mathbb{F}_4$ (of multiplicity 1).

Proof of the Main Theorem

Idea.

Choose W as the trace-zero plane of the subfield $\mathbb{F}_{16} \subseteq \mathbb{F}_{2^n}$.
$\implies \mathbf{C}_W$ is of the type discussed in Property 5 above. The missing points are 1 (of multiplicity 3) and the primitive 5th roots of unity in $\mathbb{F}_{16}$.

Case 1: $n \equiv 4 \pmod 8$
In this case $(W^2)^\perp \cap \mathbb{F}_{16} = \mathbb{F}_2$
$\implies$ 1 is the only missing point contained in $(W^2)^\perp$.
$\implies \mathbf{C}_W$ has row sums 4 and 10 with corresponding frequencies $f_4 = 2^{n-4}$, $f_{10} = 2^{n-4} - 1$.
This leads to the stated lower bound for the max. (global) net gain.

Case 2: $n \equiv 0 \pmod 8$
In this case $F_{16} \subset (W^2)^\perp$, so that $(W^2)^\perp$ contains all $3 + 1 + 1 + 1 + 1 = 7$ missing points.
The proof is similar to that in Case 1 but more difficult. One can show that $N_1 \geq 2^{n-8} \times 54$ using $n = 8$ as an “anchor”. □

Outline

Open Problems/Future Work

- We conjecture that the main theorem remains true for all lengths $v \geq 7$, $v \neq 8, 10$. Prove this conjecture!
For the yet unsettled case $v \equiv 1 \pmod 4$, or $n \equiv 2 \pmod 4$, there is overwhelming computational evidence for the truth. (Here it suffices to exhibit a plane $W = \langle 1, a, b \rangle$ of the type considered in Case 1 of the proof.)
- Use Expurgation-Augmentation with non-Gabidulin MRD codes.
- Investigate non-standard rearrangements of free lines into new planes.
- Determine the structure of the set of free planes of $\mathcal{C}$ meeting S in a line, and use this structure to solve the extension problem efficiently.
- Generalize Expurgation-Augmentation to constant dimensions $k > 3$.

Thank You

Outline

J. Ai, T. Honold, and H. Liu.
The expurgation-augmentation method for constructing good plane subspace codes.
Preprint arXiv:1601.01502 [math.CO], Jan. 2016.

E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv,
Subspace polynomials and cyclic subspace codes, 2014,
Preprint arXiv:1404.7739 [cs.IT].

E. R. Berlekamp,
Algebraic coding theory,
McGraw-Hill, 1968.

S. R. Blackburn and T. Etzion,
The asymptotic behavior of Grassmannian codes,
IEEE Transactions on Information Theory, **58** (2012), 6605–6609.

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, P. Östergård, and A. Wassermann.
New lower bounds for binary constant dimension subspace codes.
Preprint, Apr. 2015.

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].

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.

T. Etzion and N. Silberstein.

Codes and designs related to lifted MRD codes.

IEEE Transactions on Information Theory, 59(2):1004–1017, Feb. 2013.

Erratum ibid. 59(7):4730, 2013.

T. Honold and M. Kiermaier.

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

In T. Hagen, F. Rupp, and J. Scheurle, editors, *Dynamical Systems, Number Theory and Applications: A Festschrift in Honor of Armin Leutbecher's 80th Birthday*, chapter 8, pages 141–175. World Scientific, 2016.

Preprint arXiv:1504.06688 [math.CO].

T. Honold, M. Kiermaier, and S. Kurz.
Optimal binary subspace codes of length 6, constant dimension 3 and minimum subspace distance 4.
In G. Kyureghyan, G. L. Mullen, and A. Pott, editors, *Topics in Finite Fields. 11th International Conference on Finite Fields and their Applications, July 22–26, 2013, Magdeburg, Germany*, volume 632 of *Contemporary Mathematics*, pages 157–176. American Mathematical Society, 2015.
Preprint arXiv:1311.0464 [math.CO].

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.

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].

O. Ore,
On a special class of polynomials,
Transactions of the American Mathematical Society, **35** (1933), 559–584,
Corrigendum ibid. 36(2):275, 1934.

N. Silberstein and A.-L. Trautmann,
Subspace codes based on graph matchings, Ferrers diagrams, and pending blocks,
IEEE Transactions on Information Theory, **61** (2015), 3937–3953.

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].