Improved upper bounds for partial spreads

Sascha Kurz
University of Bayreuth
sascha.kurz@uni-bayreuth.de

Table for $A_2(10, d; k)$

d\k	2	3	4	5
4	341	23870 - 24698	301213 - 423181	1167355 - 1678413
6		145	4173 - 4978	32890 - 38214
8			65	1025 - 1089
10				33

Network Coding and Designs, Dubrovnik, Croatia, 04.-08.04.2016

Partial spreads

Definition

A *partial* $(k-1)$*-spread* in $\mathrm{PG}(n-1,q)$ is a collection of $(k-1)$-dimensional subspaces with trivial intersection such that each *point* is covered exactly once.

Problem

Determine the maximum size $A_q(n, 2k; k)$ of a partial $(k-1)$-spread in $\mathrm{PG}(n-1,q)$.

Remark

A *partial* $(k-1)$*-spread* in $\mathrm{PG}(n-1,q)$ corresponds to a constant dimension code with codewords of dimension k in $\mathbb{F}_q^n$ and subspace distance $2k$.

Upper bounds

Drake, Freeman 1979 (Cor. from Bose, Bush 1952)

If $n = k(t+1) + r$ with $0 < r < k$, then

$$A_q(n, 2k; k) \le \sum_{i=0}^{t} q^{ik+r} - \lfloor\theta\rfloor - 1 = q^r \cdot \frac{q^{k(t+1)} - 1}{q^k - 1} - \lfloor\theta\rfloor - 1,$$

where $2\theta = \sqrt{1 + 4q^k(q^k - q^r)} - (2q^k - 2q^r + 1)$.

Observation

For $r \ge 1$ and $k \ge 2r$ we have $\lfloor\theta\rfloor = \left\lfloor \frac{q^r - 2}{2} \right\rfloor$.

If $r = 0$ then $A_q(n, 2k; k) \le q^r \cdot \frac{q^{k(t+1)}-1}{q^k-1}$. (counting points)

If $n < 2k$ then $A_q(n, 2k; k) \le 1$.

Lower bounds (a modern view)

Let $v \in \mathbb{F}_2^n$ be a binary vector of weight $1 \le k \le n$. By $\mathrm{EF}_q(v)$ we denote the set of all $k \times n$-matrices over $\mathbb{F}_q$ that are in row-reduced echelon form and the pivot columns coincide with the positions where v has a 1-entry.

Multi-level construction; Etzion, Silberstein 2009

- $1 \le k \le n$, $1 \le d \le \min(k, n-k)$;
- $\mathcal{B}$ a binary constant weight code of length n, weight k, and minimum Hamming distance $2d$;
- $\forall\, b \in \mathcal{B}$ let $\mathcal{C}_b \subseteq \mathrm{EF}_q(b)$ with minimum rank distance $\ge d$.

$\cup_{b\in\mathcal{B}} \mathcal{C}_b$ has a subspace distance $\ge 2d$.

Lower bounds (a modern view)

Take $\mathcal{B} =$

$$\begin{array}{c} 1\ldots10\ldots00\ldots00\ldots \\ 0\ldots01\ldots10\ldots00\ldots \\ 0\ldots00\ldots01\ldots10\ldots \\ \ldots \end{array}$$

and $\mathcal{C}_b$ as a corresponding lifted MRD code:

Observation

For $n = k(t+1) + r$ with $0 \le r < k$ and $n \ge 2k$ we have

$$\begin{aligned} A_q(n, 2k; k) &\ge 1 + \sum_{i=1}^{\lfloor n/k \rfloor - 1} q^{n-ik} = 1 + q^{k+r} \cdot \frac{q^{tk} - 1}{q^k - 1} \\ &= q^r \cdot \frac{q^{k(t+1)} - 1}{q^k - 1} - q^r + 1 \end{aligned}$$

Exact values

$r = 0$: André 1954

$A_q((t+1)k, 2k; k) = \frac{q^{(t+1)k}-1}{q^k-1}$ for all $t \geq 0$, $k \geq 1$ (matches both bounds)

$r = 1$: Beutelspacher 1975; Hong, Patel 1972 for $q = 2$

$A_q((t+1)k+1, 2k; k) = q^1 \cdot \frac{q^{k(t+1)}-1}{q^k-1} - q + 1$ for all $t \geq 0$, $k \geq 2$

(matches lower bound)

$r = 2$: El-Zanati, Jordon, Seeliger, Sissokho 2010

$A_2(3m+2, 6; 3) = \frac{2^{3m+2}-18}{7}$ for all $m \geq 2$ (matches upper bound)

The case $r = 1$ revisited

- Beutelspacher 1975: clever divisibility arguments; here: a more simple-minded variant
- size of the code: $|\mathcal{C}| = q \cdot \frac{q^{k(t+1)}-1}{q^k-1} - x$, where $x \le q-1$
- av. numb. codewords per hyperplane: $\frac{|\mathcal{C}| \cdot \left[{kt+1 \atop 1}\right]_q}{\left[{k(t+1)+1 \atop 1}\right]_q} > q \cdot \frac{q^{kt}-1}{q^k-1}$

The case $r = 1$ revisited

- Beutelspacher 1975: clever divisibility arguments; here: a more simple-minded variant
- size of the code: $|\mathcal{C}| = q \cdot \frac{q^{k(t+1)}-1}{q^k-1} - x$, where $x \le q-1$
- av. numb. codewords per hyperplane: $\frac{|\mathcal{C}| \cdot \begin{bmatrix} kt+1 \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k(t+1)+1 \\ 1 \end{bmatrix}_q} > q \cdot \frac{q^{kt}-1}{q^k-1}$
- there exists a hyperplane containing at least $\alpha := q \cdot \frac{q^{kt}-1}{q^k-1} + 1$ codewords
- $$\alpha \cdot \begin{bmatrix} k \\ 1 \end{bmatrix}_q + (|\mathcal{C}| - \alpha) \cdot \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q \le \begin{bmatrix} k(t+1) \\ 1 \end{bmatrix}_q$$
  $$\Rightarrow \quad |\mathcal{C}| \le q \cdot \frac{q^{k(t+1)}-1}{q^k-1} - (q-1)$$
- intersection of the code with a hyperplane

Vector space partitions

- partition $\mathcal{P}$ of $\mathbb{F}_q^n$ into subspaces
- type $k^{m_k} \dots 1^{m_1}$, i.e., m_i subspaces of dimension i
- tail: set of subspaces, in $\mathcal{P}$, having the smallest dimension

Vector space partitions

- partition $\mathcal{P}$ of $\mathbb{F}_q^n$ into subspaces
- type $k^{m_k} \ldots 1^{m_1}$, i.e., m_i subspaces of dimension i
- tail: set of subspaces, in $\mathcal{P}$, having the smallest dimension

Heden 2009

Let $\mathcal{P}$ be a vector space partition of $\mathbb{F}_q^n$, let n_1 denote the length of the tail of $\mathcal{P}$, let d_1 denote the dimension of the vector spaces in the tail of $\mathcal{P}$, and let d_2 denote the dimension of the vector spaces of the second lowest dimension.

(i) if $q^{d_2-d_1}$ does not divide n_1 and if $d_2 < 2d_1$, then $n_1 \ge q^{d_1}+1$;

(ii) if $q^{d_2-d_1}$ does not divide n_1 and if $d_2 \ge 2d_1$, then either d_1 divides d_2 and $n_1 = \left(q^{d_2}-1\right)/\left(q^{d_1}-1\right)$ or $n_1 > 2q^{d_2-d_1}$;

(iii) if $q^{d_2-d_1}$ divides n_1 and $d_2 < 2d_1$, then $n_1 \ge q^{d_2}-q^{d_1}+q^{d_2-d_1}$;

(iv) if $q^{d_2-d_1}$ divides n_1 and $d_2 \ge 2d_1$, then $n_1 \ge q^{d_2}$.

The case $r = 2$ for $k \geq 4$ and $q = 2$

A forbidden vector space partition

For two integers $t \geq 1$ and $k \geq 4$ no vector space partition of type $k^{n_k}(k-1)^{n_{k-1}}1^{1+2^{k-1}}$ exists in $\mathbb{F}_2^{k(t+1)+1}$, where $n_k = \frac{2^{kt+2}+2^k-5}{2^k-1}$ and $n_{k-1} = 2^{kt+2}-3$.

The case $r = 2$ for $k \geq 4$ and $q = 2$

A forbidden vector space partition

For two integers $t \geq 1$ and $k \geq 4$ no vector space partition of type $k^{n_k}(k-1)^{n_{k-1}}1^{1+2^{k-1}}$ exists in $\mathbb{F}_2^{k(t+1)+1}$, where $n_k = \frac{2^{kt+2}+2^k-5}{2^k-1}$ and $n_{k-1} = 2^{kt+2} - 3$.

Proof

- consider an intersection with a hyperplane H
- the *non-holes* are cut into subspaces with dimensions in $\{k, k-1, k-2\}$
- number of holes in H: $L \equiv 1 \pmod{2^{k-2}}$, $L \leq 1 + 2^{k-1}$
- counting the number of holes yields a contradiction ($L = 1$ impossible due to Heden 2009)

The case $r = 2$ for $k \geq 4$ and $q = 2$

Main theorem

For each pair of integers $t \geq 1$ and $k \geq 4$ we have
$A_2(k(t+1)+2, 2k; k) = \frac{2^{k(t+1)+2} - 3 \cdot 2^k - 1}{2^k - 1}$.

The case $r = 2$ for $k \geq 4$ and $q = 2$

Main theorem

For each pair of integers $t \geq 1$ and $k \geq 4$ we have $A_2(k(t+1)+2, 2k; k) = \frac{2^{k(t+1)+2} - 3 \cdot 2^k - 1}{2^k - 1}$.

Proof

Let $\mathcal{C}$ be a code attaining the upper bound and consider an intersection with a hyperplane. 5 possible types:

- $k^{n_k+1}(k-1)^{n_{k-1}-1}1^1$; $k^{n_k}(k-1)^{n_{k-1}}1^{1+2^{k-1}}$
- $k^{n_k-1}(k-1)^{n_{k-1}+1}1^{1+2^k}$; $k^{n_k-2}(k-1)^{n_{k-1}+2}1^{1+3\cdot 2^{k-1}}$; $k^{n_k-3}(k-1)^{n_{k-1}+3}1^{1+2^{k+1}}$,

where $n_k = \frac{2^{kt+2}+2^k-5}{2^k-1}$ and $n_{k-1} = 2^{kt+2} - 3$.

The case $r = 2$ for $k \geq 4$ and $q = 2$

Main theorem

For each pair of integers $t \geq 1$ and $k \geq 4$ we have
$A_2(k(t+1)+2, 2k; k) = \frac{2^{k(t+1)+2}-3\cdot 2^k-1}{2^k-1}$.

Proof

Let $\mathcal{C}$ be a code attaining the upper bound and consider an intersection with a hyperplane. 5 possible types:

- $k^{n_k+1}(k-1)^{n_{k-1}-1}1^1$; $k^{n_k}(k-1)^{n_{k-1}}1^{1+2^{k-1}}$ excluded
- $k^{n_k-1}(k-1)^{n_{k-1}+1}1^{1+2^k}$; $k^{n_k-2}(k-1)^{n_{k-1}+2}1^{1+3\cdot 2^{k-1}}$; $k^{n_k-3}(k-1)^{n_{k-1}+3}1^{1+2^{k+1}}$,

where $n_k = \frac{2^{kt+2}+2^k-5}{2^k-1}$ and $n_{k-1} = 2^{kt+2} - 3$.

Counting the number of k-dimensional subspaces yields a contradiction.

The case $r = 2$ for $k \geq 4$ and $q > 2$

Lemma

For integers $t \geq 1$, $k \geq 4$, and odd q no vector space partition of type $k^{p-1}(k-1)^{m-p+1}1^{\frac{q+1}{2}+q^{k-1}}$ exists in $\mathbb{F}_q^{k(t+1)+1}$, where $p = \frac{q^{kt+2}-q^2}{q^k-1} + \frac{q+1}{2}$ and $m = \frac{q^{k(t+1)+2}-q^2}{q^k-1} - \frac{q^2-1}{2}$.

Lemma

For integers $t \geq 1$ and $k \geq 4$ we have
$A_3(k(t+1)+2, 2k; k) \leq \frac{3^{k(t+1)+2}-3^2}{3^k-1} - \frac{3^2+1}{2}$.

(reduction of the upper bound by 1; still a gap of 3)

The case $r = 2$ for $k = 3$, $q = 2$, $n = 8$

Let a_i denote the number of hyperplanes containing exactly $2 \le i \le 5$ three-dimensional codewords. standard equations:

$$
\begin{aligned}
a_2 + a_3 + a_4 + a_5 &= \begin{bmatrix} 8 \\ 7 \end{bmatrix}_2 = 255 \\
2a_2 + 3a_3 + 4a_4 + 5a_5 &= \begin{bmatrix} 5 \\ 1 \end{bmatrix}_2 \cdot A_2(8,6;3) = 1054 \\
a_2 + 3a_3 + 6a_4 + 10a_5 &= \begin{bmatrix} 3 \\ 1 \end{bmatrix}_2 \cdot \binom{A_2(8,6;3)}{2} = 1683
\end{aligned}
$$

consideration of the subspace generated by the holes

$\Rightarrow$ theo. possible *spectra*: $(0,17,187,51)$, $(1,14,190,50)$, $(3,8,196,48)$, i.e., at least 48 hyperplanes of type $3^5 2^{29} 1^5$

(c.f. approach of El-Zanati et al.)

(Less than 3000 cases for five planes in $\mathbb{F}_2^7$.)

What have we done?

What have we done?

intersected two times (Beutelspacher one time; André zero times)

What have we done?

intersected two times (Beutelspacher one time; André zero times)

intersected three times ...

Table for $A_2(13, d; k)$

d\k	2	3	4	5	6
4	**2729**	**1597245**	157319501 - 217544769	4794061075 - 7193022828	38325127529 - 57886442918
6		**1169**	266891 - 319449	16835124 - 20918757	269057345 - 339835228
8			**545**	65793 - 72133	2097225 - 2284118
10				257 - 260	16385 - 16772
12					**129**

Visit us

Table for $A_2(11, d; k)$

d\k	2	3	4	5
4	681	97526 - 99718	2383041 - 3370453	18728043 - 27943597
6		290	16669 - 19787	262996 - 328708
8			129 - 133	4097 - 4292
10				65

http://subspacecodes.uni-bayreuth.de/

Thank you very much for your attention!