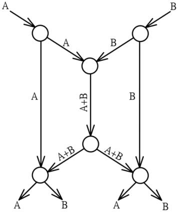
Upper bounds for partial spreads from divisible codes



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

joint work with

Daniel Heinlein, Michael Kiermaier, Alfred Wassermann
University of Bayreuth



Thomas Honold
Zhejiang University, Hangzhou

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 - 132	4097 - 4292
10				65

Fq13, Gaeta, Italy, 09.06.2017

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.

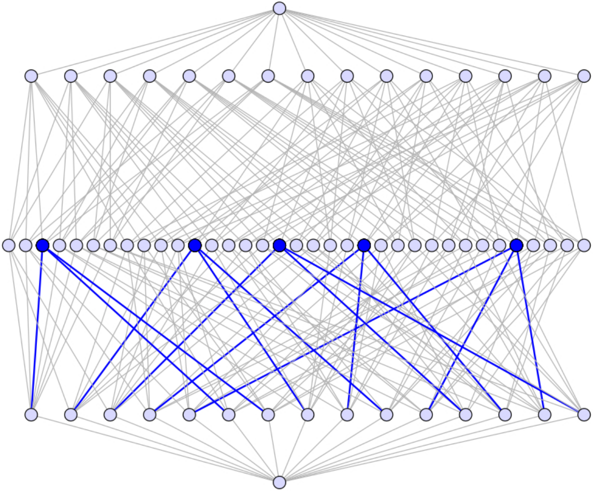
Problem

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 $2k$.

A 1-spread or line spread in $PG(3,2)$



Beutelspacher 1975: study the holes!

$r = 0$: Theorem Segre 1964

$A_q(tk + r, 2k; k) = q^r \cdot \frac{q^{tk}-1}{q^k-1}$ if and only if $r = 0$ (spreads)

$r \geq 1$: Theorem Beutelspacher 1975

$A_q(tk + r, 2k; k) \geq 1 + \sum_{i=1}^{t-1} q^{v-ik} = q^r \cdot \frac{q^{tk}-1}{q^k-1} - q^r + 1$ for all $t \geq 2$, $k \geq 2$, where $0 < r < k$ (equality for $r = 1$)

- point not covered by a partial spread: hole

Lemma

Let $\mathcal{N}$ be the set of holes of a partial $(k-1)$-spread (or vector space partitions of type $[t^{m_t} \dots k^{m_k} 1^{m_1}]$) in $\mathcal{V}$. For every hyperplane $H \subset \mathcal{V}$ we have $\#\mathcal{N} \cap H \equiv \#\mathcal{N} \pmod{q^{k-1}}$.

Holes and linear codes

- take points of $\mathcal{N}$ as columns of a $v \times n$ matrix G, where $v = \dim(\mathcal{V})$ and $n = \#\mathcal{N}$
- G is the generator matrix of a $[n, v]_q$ code $\mathcal{C}$
- codewords of $\mathcal{C}$: $c = H^T G$ for all hyperplanes $H \subset \mathcal{V}$
- $c_i = 0$: point $G_i \in H$; $c_i \neq 0$: point $G_i \notin H$; $\#(\mathcal{N} \cap H) = n - \mathrm{wt}(c)$, where $\mathrm{wt}(c)$ counts non-zeroes in c
- $\mathrm{wt}(c) \equiv 0 \pmod{q^{k-1}}$, i.e., $\mathcal{C}$ is a q^{k-1}-divisible code
- $\mathcal{N} \cap H$ corresponds to a q^{k-2}-divisible code; recursive

MacWilliams Identities

$$\sum_{j=0}^{n-i} \binom{n-j}{i} A_j = q^{\dim(\mathcal{C})-i} \cdot \sum_{j=0}^{i} \binom{n-j}{n-i} A_j^\perp \quad \text{for } 0 \le i \le n$$

- A_i: $\#$ codewords of weight i of $\mathcal{C}$
- $A_i^\perp$: # codewords of weight i of the dual code $\mathcal{C}^\perp$

In our application we have

- $A_0 = A_0^\perp = 1$
- $\mathcal{C}$ is projective: $A_1^\perp = 0$, $A_2^\perp = 0$
- $\mathcal{C}$ is q^{k-1}-divisible: $A_i = 0$ if i is not divisible by q^{k-1}

First 2 MacWilliams identities

$\mathcal{C}$ is a Δ-divisible $[n, v]_q$ code

$$
\begin{aligned}
A_0 + A_1 + \cdots + A_n &= q^v A_0^\perp \\
n \cdot A_0 + (n-1) \cdot A_1 + \cdots + 1 \cdot A_{n-1} &= q^{v-1} \cdot (nA_0^\perp + A_1^\perp)
\end{aligned}
$$

First 2 MacWilliams identities

$\mathcal{C}$ is a Δ-divisible $[n, v]_q$ code, where $n = u + m\Delta$, $m \geq 0$, and $A_i = 0$ for $i > n - u$

$$A_\Delta + A_{2\Delta} + \cdots + A_{m\Delta} = q^v - 1$$
$$(n - 1\Delta) \cdot A_\Delta + \cdots + (n - m\Delta) \cdot A_{m\Delta} = n\left(q^{v-1} - 1\right)$$

First 2 MacWilliams identities

$\mathcal{C}$ is a Δ-divisible $[n, v]_q$ code, where $n = u + m\Delta$, $m \geq 0$, and $A_i = 0$ for $i > n - u$

$$A_\Delta + A_{2\Delta} + \cdots + A_{m\Delta} = q^v - 1$$
$$(n - 1\Delta) \cdot A_\Delta + \cdots + (n - m\Delta) \cdot A_{m\Delta} = n\left(q^{v-1} - 1\right)$$

The second equation minus u times the the first equation gives

$$0 \leq \sum_{i=1}^{m} (m - i)\Delta \cdot A_{i\Delta} = (n - uq) \cdot q^{v-1} - m\Delta$$

so that $u < \frac{n}{q}$ or $n = u = m = 0$, i.e., q-divisible implies $n = 0$ or $n \geq q$.

First 2 MacWilliams identities

Applied recursively, we obtain:

Theorem Năstase and Sissokho 2016

Suppose $v = tk + r$ with $t \geq 1$ and $0 < r < k$. If $k > \frac{q^r-1}{q-1}$ then $A_q(v, 2k; k) = 1 + \sum_{i=1}^{t-1} q^{ik+r} = \frac{q^v-q^{k+r}+q^k-1}{q^k-1}$.

Remark

If k is *large*, then the construction of Beutelspacher is optimal.

Remark

We have utilized the non-negativity of a certain linear polynomial (in a given range).

First 3 MacWilliams identities

Lemma

Let $\mathcal{C}$ be a Δ-divisible $[n, v]_q$ code and $m \in \mathbb{Z}$, then

$$0 \leq \sum_{h=0}^{\lfloor n/\Delta \rfloor} (m-h)(m-h-1)A_{h\Delta} = \tau_q(n, \Delta, m) \cdot \frac{q^{v-2}}{\Delta^2} - m(m-1),$$

where $\tau_q(n, \Delta, m) =$

$$m(m-1)\Delta^2 q^2 - n(2m-1)(q-1)\Delta q + n(q-1)\Big(n(q-1)+1\Big).$$

Remark

We have utilized the non-negativity of a certain quadratic polynomial.

First 3 MacWilliams identities

Theorem K. 2016 implies Năstase, Sissokho 2016

For integers $r \geq 1$, $t \geq 2$, $u \geq 0$, and $0 \leq z \leq \frac{q^r-1}{q-1}/2$ with $k = \frac{q^r-1}{q-1} + 1 - z + u > r$ we have $A_q(v, 2k; k) \leq lq^k + 1 + z(q-1)$, where $l = \frac{q^{v-k}-q^r}{q^k-1}$ and $v = kt + r$.

Theorem K. 2016 $y = k$ is Drake, Freeman 1979

For integers $r \geq 1$, $t \geq 2$, $y \geq \max\{r, 2\}$, $z \geq 0$ with $\lambda = q^y$, $y \leq k$, $k = \frac{q^r-1}{q-1} + 1 - z > r$, $v = kt + r$, and $l = \frac{q^{v-k}-q^r}{q^k-1}$, we have $A_q(v, 2k; k) \leq$
$lq^k + \left\lceil \lambda - \frac{1}{2} - \frac{1}{2}\sqrt{1 + 4\lambda\left(\lambda - (z + y - 1)(q-1) - 1\right)} \right\rceil$.

Linear programming method

If the equation system has no solutions for $A_i, A_i^\perp \in \mathbb{R}_{\geq 0}$, then no such code exists.

Example $A_2(11, 8; 4) \neq 133$ since $2^{11} - 1 = (2^4 - 1) \cdot 133 + 52$

There is no 2^3-divisible linear code of length $n = 52$ in $\mathbb{F}_2^v$.

$$\begin{array}{rcrcrcrcrcl}
1 & + & A_8 & + & A_{16} & + & A_{24} & + & A_{32} & = & 8y, \\
52 & + & 44A_8 & + & 36A_{16} & + & 28A_{24} & + & 20A_{32} & = & 4y \cdot 52, \\
\binom{52}{2} & + & \binom{44}{2}A_8 & + & \binom{36}{2}A_{16} & + & \binom{28}{2}A_{24} & + & \binom{20}{2}A_{32} & = & 2y \cdot \binom{52}{2}, \\
\binom{52}{3} & + & \binom{44}{3}A_8 & + & \binom{36}{3}A_{16} & + & \binom{28}{3}A_{24} & + & \binom{20}{3}A_{32} & = & y\left(\binom{52}{3} + A_3^\perp\right)
\end{array}$$

are the first 4 MacWilliams Identities using $A_{40} = A_{48} = 0$ from a recursive application of the linear programming method, where $y = 2^{v-3}$.

Linear programming method

Example (cont.) $A_2(11, 8; 4) \neq 133$ since $2^{11} - 1 = (2^4 - 1) \cdot 133 + 52$

Substituting $x = yA_3^{\perp}$ and solving for A_8, A_{16}, A_{24}, A_{32} yields

$A_8 = -4 + \frac{1}{512}x + \frac{7}{64}y$, $A_{16} = 6 - \frac{3}{512}x - \frac{17}{64}y$,
$A_{24} = -4 + \frac{3}{512}x + \frac{397}{64}y$, and $A_{32} = 1 - \frac{1}{512}x + \frac{125}{64}y$.

Since $A_{16}, x \geq 0$, we have $y \leq \frac{384}{17} < 23$. On the other hand, since $3A_8 + A_{16} \geq 0$, we also have $-6 + \frac{y}{16} \geq 0$, i.e., $y \geq 96$ – a contradiction.

- $129 \leq A_2(11, 8; 4) \leq 132$
- There is a 2^3-divisible linear code of length $n = (2^{11} - 1) - (2^4 - 1) \cdot 132 = 67$ in $\mathbb{F}_2^{10}$.

First 4 MacWilliams identities

Lemma K. 2016

Let $\mathcal{C}$ be Δ-divisible over $\mathbb{F}_q$ of cardinality $n > 0$ and $t \in \mathbb{Z}$. Then $\sum_{i\geq 1}\Delta^2(i-t)(i-t-1)\cdot(g_1\cdot i+g_0)\cdot A_{i\Delta} + qhx = n(q-1)(n-t\Delta)(n-(t+1)\Delta)g_2$, where $g_1 = \Delta qh$, $g_0 = -n(q-1)g_2$, $g_2 = h-(2\Delta qt+\Delta q-2nq+2n+q-2)$ and $h = \Delta^2q^2t^2+\Delta^2q^2t-2\Delta nq^2t-\Delta nq^2+2\Delta nqt+n^2q^2+\Delta nq-2n^2q+n^2+nq-n$.

Corollary

If there exists $t \in \mathbb{Z}$, using the above notation, with $n/\Delta \notin [t, t+1]$, $h \geq 0$, and $g_2 < 0$, then there is no Δ-divisible set over $\mathbb{F}_q$ of cardinality n.

First 4 MacWilliams identities

Remark

We have utilized the non-negativity of a certain cubic polynomial in the stated Lemma.

- $2^4l + 1 \le A_2(4k+3, 8; 4) \le 2^4l + 4$, where $l = \frac{2^{4k-1} - 2^3}{2^4 - 1}$;
- $2^6l + 1 \le A_2(6k+4, 12; 6) \le 2^6l + 8$, where $l = \frac{2^{6k-2} - 2^4}{2^6 - 1}$;
- $2^6l + 1 \le A_2(6k+5, 12; 6) \le 2^6l + 18$, where $l = \frac{2^{6k-1} - 2^5}{2^6 - 1}$;
- $3^4l + 1 \le A_3(4k+3, 8; 4) \le 3^4l + 14$, where $l = \frac{3^{4k-1} - 3^3}{3^4 - 1}$;
- $3^5l + 1 \le A_3(5k+3, 10; 5) \le 3^5l + 13$, where $l = \frac{3^{5k-2} - 3^5}{3^3 - 1}$;
- $3^5l + 1 \le A_3(5k+4, 10; 5) \le 3^5l + 44$, where $l = \frac{3^{5k-1} - 3^4}{3^5 - 1}$;
- $3^6l + 1 \le A_3(6k+4, 12; 6) \le 3^6l + 41$, where $l = \frac{3^{6k-2} - 3^4}{3^6 - 1}$;
- $3^6l + 1 \le A_3(6k+5, 12; 6) \le 3^6l + 133$, where $l = \frac{3^{6k-1} - 3^5}{3^6 - 1}$;
- $3^7l + 1 \le A_3(7k+4, 14; 7) \le 3^7l + 40$, where $l = \frac{3^{7k-3} - 3^4}{3^7 - 1}$;

First 4 MacWilliams identities

- $4^5 l + 1 \le A_4(5k+3, 10; 5) \le 4^5 l + 32$, where $l = \frac{4^{5k-2} - 4^3}{4^5 - 1}$;
- $4^6 l + 1 \le A_4(6k+3, 12; 6) \le 4^6 l + 30$, where $l = \frac{4^{6k-3} - 4^3}{4^6 - 1}$;
- $4^6 l + 1 \le A_4(6k+5, 12; 6) \le 4^6 l + 548$, where $l = \frac{4^{6k-1} - 4^5}{4^6 - 1}$;
- $4^7 l + 1 \le A_4(7k+4, 14; 7) \le 4^7 l + 128$, where $l = \frac{4^{7k-3} - 4^4}{4^7 - 1}$;
- $5^5 l + 1 \le A_5(5k+2, 10; 5) \le 5^5 l + 7$, where $l = \frac{5^{5k-3} - 5^2}{5^5 - 1}$;
- $5^5 l + 1 \le A_5(5k+4, 10; 5) \le 5^5 l + 329$, where $l = \frac{5^{5k-1} - 5^4}{5^5 - 1}$;
- $7^5 l + 1 \le A_7(5k+4, 10; 5) \le 7^5 l + 1246$, where $l = \frac{7^{5k-1} - 7^2}{7^5 - 1}$;
- $8^4 l + 1 \le A_8(4k+3, 8; 4) \le 8^4 l + 264$, where $l = \frac{8^{4k-1} - 8^3}{8^4 - 1}$;
- $8^5 l + 1 \le A_8(5k+2, 10; 5) \le 8^5 l + 25$, where $l = \frac{8^{5k-3} - 8^2}{8^5 - 1}$;
- $8^6 l + 1 \le A_8(6k+2, 12; 6) \le 8^6 l + 21$, where $l = \frac{8^{6k-4} - 8^2}{8^6 - 1}$;
- $9^3 l + 1 \le A_9(3k+2, 6; 3) \le 9^3 l + 41$, where $l = \frac{9^{3k-1} - 9^2}{9^3 - 1}$;
- $9^5 l + 1 \le A_9(5k+3, 10; 5) \le 9^5 l + 365$, where $l = \frac{9^{5k-2} - 9^3}{9^5 - 1}$.

Visit us – join the hunt

All known upper bounds for partial spreads follow from the linear programming method applied to the first 4 MacWilliams identities. There remain 3 theorems (Segre, K.) and 21 sporadic series.

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**

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

Thank you very much for your attention!

$257 \le A_2(13, 10; 5) \le 259$

Lemma

Weight enumerator of a proj. 2^3-divisible binary code of length 51 is $1 + 204X^{24} + 51X^{32}$. (concatenation of an ovoid in $PG(3,4)$ with the binary [3, 2] simplex code)

Proof

There are 2 integral solutions of the first 4 MacWilliams identities. $1 + 2X^8 + 406X^{24} + 103X^{32}$ is impossible.

Proposition

No 2^4 -divisible set of cardinality 131 exists.

Proof

Otherwise a hyperplane with 51 points, i.e., a codeword c of weight 80 exists. Consider the split-weight enumerator of $\mathrm{supp}(c)$.

q^r-divisible sets with cardinality $n \le rq^{r+1}$

Theorem Heden 2009

Let $\mathcal{C}$ be a vector space partition of type $k^z \cdots d_2{}^b d_1{}^a$ of $\mathbb{F}_q^v$, where $a, b > 0$.

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

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

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

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

Theorem K. 2016

For the cardinality n of a q^r-divisible set $\mathcal{C}$ over $\mathbb{F}_q$ we have

$$n \notin \left[(a(q-1)+b)\begin{bmatrix} r+1 \\ 1 \end{bmatrix}_q + a + 1, (a(q-1)+b+1)\begin{bmatrix} r+1 \\ 1 \end{bmatrix}_q - 1\right],$$

where $a, b \in \mathbb{N}_0$ with $b \le q-2$, $a \le r-1$, and $r \in \mathbb{N}_{>0}$.
In other words, if $n \le rq^{r+1}$, then n can be written as $a\begin{bmatrix} r+1 \\ 1 \end{bmatrix}_q + bq^{r+1}$ for some $a, b \in \mathbb{N}_0$.

Upper bounds for constant dimension codes

All known upper bounds for the maximal size $A_q(n, d; k)$ of a constant dimension code refer back to bounds for partial spreads via recursive application of the Johnson bound

$$A_q(v, d; k) \le \frac{q^v - 1}{q^k - 1} A_q(v - 1, d; k - 1)$$

except

$$A_2(6, 4; 3) = 77 < 81 \quad \text{(Honold, Kiermaier, K., 2015)}$$

and

$$257 \le A_2(8, 6; 4) \le 272 < 289 \quad \text{(Heinlein, K., 2017 – WCC).}$$