Asymptotic bounds for the sizes of constant dimension codes and an improved lower bound

5th ICMCTA

Vihula Manor, 28 - 31 August 2017

Daniel Heinlein
University of Bayreuth, Germany
Daniel.Heinlein@uni-bayreuth.de

joined work with Sascha Kurz

2017-08-28

Notation

Grassmannian: Set of k dimensional subspaces in $\mathbb{F}_q^v = \begin{bmatrix} v \\ k \end{bmatrix}$

... of size $\begin{bmatrix} v \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^v - q^i}{q^k - q^i}$

bijection: $\tau : \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} \to \{X_U \in \mathbb{F}_q^{k \times v} | \, \mathrm{rk}(X_U) = k, X_U \text{ is in rref}\}$

constant dimension code (cdc): $C \subseteq \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$

subspace distance: $d_S(U, W) = \dim(U + W) - \dim(U \cap W)$

maximum cdc size: $A_q(v, d; k)$

standard parameters: $2 \leq d/2 \leq k \leq v/2$ and $2 \leq q$ prime power

dominance: "$\leq$" means "dominates" for the parameters applicable

q-Pochhammer symbol: $(a; q)_n := \prod_{i=0}^{n-1} \left(1 - aq^i\right)$

Upper bounds

Anticode type bounds

Theorem ((**Sphere-packing bound**)[KK08, Theorem 6])

$$A_q(v,d;k) \leq \frac{\begin{bmatrix} v \\ k \end{bmatrix}_q}{\sum_{i=0}^{\lfloor (d/2-1)/2 \rfloor} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} v-k \\ i \end{bmatrix}_q}$$

Theorem ((**Anticode bound**), cf. [FW86, Theorem 1], [AA09, Lemma 1], [WXSN03, Theorem 5.2])

$$A_q(v,d;k) \leq \frac{\begin{bmatrix} v \\ k \end{bmatrix}_q}{\begin{bmatrix} \max\{k,v-k\}+d/2-1 \\ d/2-1 \end{bmatrix}_q}$$

Anticode $\leq$ *Sphere Packing*

Upper bounds

Johnson type bounds

Theorem ((**Johnson type bound I**) [XF09, Theorem 2])

If $\left(q^k-1\right)^2 > \left(q^v-1\right)\left(q^{k-d/2}-1\right)$, *then*

$$A_q(v,d;k) \leq \frac{\left(q^k-q^{k-d/2}\right)\left(q^v-1\right)}{\left(q^k-1\right)^2-\left(q^v-1\right)\left(q^{k-d/2}-1\right)}.$$

Proposition ((**Trivial spread bound**) [HK17a, Proposition 1])

For $0 \leq k < v$, *the bound in Johnson I is applicable iff* $d = 2\min\{k, v-k\}$ *and* $k \geq 1$. *Then, it is equivalent to*

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

Trivial spread bound $\leq$ *Johnson I*

Upper bounds

Johnson type bounds, cont.

Theorem ((**Johnson type bound II**) [XF09, Theorem 3], [EV11, Theorem 4,5])

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

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

$\Rightarrow$ equivalent using orthogonality, cf. [EV11, Section III, esp. Lemma 13] and [HK17a, Proposition 2].

Proposition ([HK17a, Proposition 3])

For $k \leq v/2$ we have Johnson II.1 $\leq$ Johnson II.2.

Upper bounds

Johnson type bounds, cont.

Corollary ((**Recursive Johnson II.1**))

$$A_q(v,d;k) \leq \left\lfloor \frac{q^v-1}{q^k-1} \left\lfloor \frac{q^{v-1}-1}{q^{k-1}-1} \left\lfloor \dots \left\lfloor \frac{q^{v-k+d/2+1}-1}{q^{d/2+1}-1} A_q(v-k+d/2,d;d/2) \right\rfloor \dots \right\rfloor \right\rfloor \right\rfloor$$

Recursive Johnson II.1 $\leq$ *Anticode*

Upper bounds

Improved Johnson bound

Theorem ((**Improved Johnson bound**)[KK17, Theorem 3])

Let

$$m = \begin{bmatrix} v \\ 1 \end{bmatrix}_q \cdot A_q(v-1, d; k-1) - \begin{bmatrix} k \\ 1 \end{bmatrix}_q \cdot \left\lfloor \frac{\begin{bmatrix} v \\ 1 \end{bmatrix}_q \cdot A_q(v-1,d;k-1)}{\begin{bmatrix} k \\ 1 \end{bmatrix}_q} \right\rfloor + \begin{bmatrix} k \\ 1 \end{bmatrix}_q \cdot \delta$$

for some $\delta \in \mathbb{N}_0$. *If no* q^{k-1}*-divisible multiset of points in* $\mathbb{F}_q^v$ *of cardinality* m *exists, then*

$$A_q(v, d; k) \leq \left\lfloor \frac{\begin{bmatrix} v \\ 1 \end{bmatrix}_q \cdot A_q(v-1, d; k-1)}{\begin{bmatrix} k \\ 1 \end{bmatrix}_q} \right\rfloor - \delta - 1.$$

Theorem ([KK17, Theorem 4])

There exists a q^r*-divisible multiset of points of cardinality* n *if and only if there are non-negative integers* $a_0, \ldots, a_r$ *with* $n = \sum_{i=0}^{r} a_i s_{i,r}^q$ *and* $s_{i,r}^q = q^{r-i} \cdot \frac{q^{i+1}-1}{q-1}$.

Improved Johnson Bound $\leq$ *Johnson II.1*

Upper bounds

Theorem ((**Ahlswede Aydinian**) [AA09, Theorem 3])

For integers $0 \leq t < r \leq k$, $k - t \leq m \leq v$, *and* $t \leq v - m$ *we have*

$$A_q(v, 2r; k) \leq \frac{\begin{bmatrix} v \\ k \end{bmatrix}_q A_q(m, 2r - 2t; k - t)}{\sum_{i=0}^{t} q^{i(m+i-k)} \begin{bmatrix} m \\ k-i \end{bmatrix}_q \begin{bmatrix} v-m \\ i \end{bmatrix}_q}.$$

Theorem ((**Singleton bound**) [KK08, Theorem 9])

$$A_q(v, d; k) \leq \begin{bmatrix} v-d/2+1 \\ \max\{k, v-k\} \end{bmatrix}_q$$

Ahlswede Aydinian $\leq$ *Johnson II.1*
Anticode $\leq$ *Singleton*

Linear Programming Bound

Theorem ((**Linear Programming Bound**) [ZJX11, Section III])

For integers $0 \leq k \leq v$ *and* $2 \leq d \leq 2\min\{k, v-k\}$ *such that* d *is even, we have*

$$A_q(v,d;k) \leq \max 1 + \sum_{i=d/2}^{k} x_i \text{ st}$$

$$\sum_{i=d/2}^{k} -Q_j(i)x_i \leq u_j \; \forall j = 1,2,\ldots,k \text{ and}$$

$$x_i \geq 0 \; \forall i = d/2, d/2+1, \ldots, k$$

with

- $E_i(j) = \sum_{m=0}^{i} (-1)^{i-m} q^{\binom{i-m}{2}+jm} \begin{bmatrix} k-m \\ k-i \end{bmatrix}_q \begin{bmatrix} k-j \\ m \end{bmatrix}_q \begin{bmatrix} v-k-j+m \\ m \end{bmatrix}_q$
- $v_i = q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} v-k \\ i \end{bmatrix}_q$, $u_j = \begin{bmatrix} v \\ j \end{bmatrix}_q - \begin{bmatrix} v \\ j-1 \end{bmatrix}_q$, $Q_j(i) = \frac{u_j}{v_i} E_i(j)$

Linear Programming Bound $\leq$ *Anticode*

Upper bounds

Theorem ([HKK15, Theorem 1])

$$A_2(6, 4; 3) = 77$$

Proposition ([HHK$^+$], cf. [HK17b], respective later today)

$$A_2(8, 6; 4) = 257$$

Upper bounds

MRD Bound

Theorem ([ES13, Theorem 10 and 11])

Let $\mathcal{C} \subseteq \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ *be a constant dimension code, with* $v \geq 2k$ *and minimum subspace distance* d*, that contains a lifted MRD code.*

- *If* $d = 2(k-1)$ *and* $k \geq 3$*, then* $\#\mathcal{C} \leq q^{2(v-k)} + A_q(v-k, 2(k-2); k-1)$;
- *if* $d = k$*, where* k *is even, then* $\#\mathcal{C} \leq q^{(v-k)(k/2+1)} + \begin{bmatrix} v-k \\ k/2 \end{bmatrix}_q \frac{q^v - q^{v-k}}{q^k - q^{k/2}} + A_q(v-k, k; k)$.

Upper bounds

Partial spreads

Theorem ((**Spread**) [Seg64, §VI])

$\mathbb{F}_q^v$ contains a spread if and only if k is a divisor of v.

Theorem ((**Beutelspacher**) [Beu75])

For positive integers v, k satisfying $v = tk + r$, $t \geq 2$ and $1 \leq r \leq k-1$ we have $A_q(v, 2k; k) \geq 1 + \sum_{i=1}^{t-1} q^{ik+r} = \frac{q^v - q^{k+r} + q^k - 1}{q^k - 1}$ with equality for $r = 1$.

Upper bounds

Partial spreads, cont.

Theorem ((**Drake Freeman**) [DF79, Corollary 8])

If $v = kt + r$ *with* $0 < r < k$, *then*

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

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

Theorem ((**Kurz 2.10**) [Kur17, Theorem 2.10])

For integers $r \geq 1$, $t \geq 2$, $y \geq \max\{r, 2\}$, $z \geq 0$ *with* $\lambda = q^y$, $y \leq k$, $k = \begin{bmatrix} r \\ 1 \end{bmatrix}_q + 1 - z > r$, $v = kt + r$, *and* $l = \frac{q^{v-k} - q^r}{q^k - 1}$, *we have* $A_q(v, 2k; k) \leq$

$$lq^k + \left\lceil \lambda - \tfrac{1}{2} - \tfrac{1}{2}\sqrt{1 + 4\lambda\left(\lambda - (z + y - 1)(q - 1) - 1\right)} \right\rceil.$$

Kurz 2.10 $\leq$ *Drake Freeman*

Upper bounds

Partial spreads, cont.

Theorem ((**Năstase Sissokho**) [NS16, Theorem 5])

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

Theorem ((**Kurz 2.9**)[Kur17, Theorem 2.9])

For integers $r \geq 1$, $t \geq 2$, $u \geq 0$, *and* $0 \leq z \leq \begin{bmatrix} r \\ 1 \end{bmatrix}_q / 2$ *with* $k = \begin{bmatrix} r \\ 1 \end{bmatrix}_q + 1 - z + u > r$ *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* $v = kt + r$.

. . . 21 special cases

Kurz 2.10 $\leq$ *Drake Freeman*

Kurz 2.9 $\leq$ *Năstase Sissokho* $\leq$ *Beutelspacher*

Overview upper bounds for cdcs

for $2 \leq d/2 \leq k \leq v/2$ and $2 \leq q$ prime power

Ahlswede Aydinian $\leq$ Johnson II.1 $\leq$ Recursive Johnson II.1 $\leq$ Anticode $\leq$ Sphere Packing

Improved Johnson bound $\leq$ Johnson II.1 $\leq$ Johnson II.2
Linear Programming Bound $\leq$ Anticode $\leq$ Singleton
2 special cases

Spread
Kurz 2.10 $\leq$ Drake Freeman $\leq$ Trivial spread bound $\leq$ Johnson I
Kurz 2.9 $\leq$ Năstase Sissokho $\leq$ Beutelspacher
21 special cases

Revisited linkage construction

Theorem ([GLT16, Theorem 2.3], cf. [ST15, Corollary 39])

Let C_i be a $(v_i, N_i, d_i; k)_q$ constant dimension code for $i = 1, 2$ and let C_r be a $(k \times v_2, N_r, d_r)_q$ linear rank metric code. Then

$$\{\tau^{-1}(\tau(U) \mid M) : U \in C_1, M \in C_r\} \cup \{\tau^{-1}(0_{k \times v_1} | \tau(W)) : W \in C_2\}$$

is a $(v_1 + v_2, N_1 N_R + N_2, \min\{d_1, d_2, 2d_r\}; k)_q$ constant dimension code.

Theorem ([HK17a, Theorem 19])

Let C_i be a $(v_i, N_i, d_i; k)_q$ constant dimension code for $i = 1, 2$, $d \in 2\mathbb{N}_{\geq 0}$ and let C_r be a $(k \times (v_2 - k + d/2), N_r, d_r)_q$ linear rank metric code. Then

$$\{\tau^{-1}(\tau(U) \mid M) : U \in C_1, M \in C_r\} \cup \{\tau^{-1}(0_{k \times m} | \tau(W)) : W \in C_2\}$$

is a $(v_1 + v_2 - k + d/2, N_1 N_R + N_2, \min\{d_1, d_2, 2d_r, d\}; k)_q$ constant dimension code with $m = v_1 - k + d/2$.

Asymptotic bounds

Proposition ([HK17a, Proposition 7])

For $k \leq v - k$ the ratio of the size of a lifted MRD code divided by the size of the Singleton bound converges for $v \to \infty$ monotonically decreasing to $(1/q; 1/q)_{k-d/2+1} \geq (1/2; 1/2)_\infty > 0.288788$.

Proposition ([HK17a, Proposition 8], cf. [ES13, Lemma 9])

For $k \leq v - k$ the ratio of the size of a lifted MRD code divided by the size of the Anticode bound converges for $v \to \infty$ monotonically decreasing to
$\frac{(1/q;1/q)_k}{(1/q;1/q)_{d/2-1}} \geq \frac{q}{q-1} \cdot (1/q; 1/q)_k \geq 2 \cdot (1/2; 1/2)_\infty > 0.577576$.

$\Rightarrow$ Improved Johnson bound (and especially Johnson II.1) does not improve this limit.

Codes better than the MRD bound

Proposition ([HK17a, Proposition 10])

For $q \geq 3$ *we have* $\lim_{v\to\infty} \frac{A_q(v,4;3)}{q^{2v-6}+\begin{bmatrix} v-3 \\ 2 \end{bmatrix}_q} \geq 1 + \frac{1}{2q^3}$.

Proposition ([HK17a, Proposition 11])

For $v \geq 19$ *we have* $\frac{A_2(v,4;3)}{2^{2v-6}+\begin{bmatrix} v-3 \\ 2 \end{bmatrix}_2} \geq 1.3056$.

Thank you for your attention !

R Ahlswede and H Aydinian.

On error control codes for random network coding.

In *Network Coding, Theory, and Applications, 2009. NetCod'09. Workshop on*, pages 68–73. IEEE, 2009.

A. Beutelspacher.

Partial spreads in finite projective spaces and partial designs.

Mathematische Zeitschrift, 145(3):211–229, 1975.

D.A. Drake and J.W. Freeman.

Partial t-spreads and group constructible (s, r, μ)-nets.

Journal of Geometry, 13(2):210–216, 1979.

Tuvi Etzion and Natalia Silberstein.

Codes and designs related to lifted MRD codes.

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

Thank you for your attention II

Tuvi Etzion and Alexander Vardy.

Error-correcting codes in projective space.

IEEE Transactions on Information Theory, 57(2):1165–1173, 2011.

P. Frankl and R. M. Wilson.

The Erdős-Ko-Rado theorem for vector spaces.

Journal of Combinatorial Theory, Series A, 43(2):228–236, 1986.

Heide Gluesing-Luerssen and Carolyn Troha.

Construction of subspace codes through linkage.

Advances in Mathematics of Communications, 10(3):525–540, 2016.

Daniel Heinlein, Thomas Honold, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann.

Classification of optimal binary subspace codes of length 8, constant dimension 4 and minimum distance 6.

in preparation.

Thank you for your attention III

Daniel Heinlein and Sascha Kurz.

Asymptotic bounds for the sizes of constant dimension codes and an improved lower bound.

arXiv preprint arXiv:1705.03835, 2017.

Daniel Heinlein and Sascha Kurz.

A new upper bound for subspace codes.

arXiv preprint 1703.08712, 2017.

Thomas Honold, Michael Kiermaier, and Sascha Kurz.

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

In *Topics in finite fields*, volume 632 of *Contemp. Math.*, pages 157–176. Amer. Math. Soc., Providence, RI, 2015.

Thank you for your attention IV

Ralf Kötter and Frank R. Kschischang.

Coding for errors and erasures in random network coding.

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

Michael Kiermaier and Sascha Kurz.

An improvement of the johnson bound for subspace codes.

arXiv preprint arXiv:1707.00650, 2017.

Sascha Kurz.

Packing vector spaces into vector spaces.

The Australasian Journal of Combinatorics, 68(1):122–130, 2017.

Esmeralda Năstase and Papa Sissokho.

The maximum size of a partial spread in a finite projective space.

arXiv preprint 1605.04824, 2016.

Thank you for your attention V

B. Segre.

Teoria di galois, fibrazioni proiettive e geometrie non desarguesiane.

Annali di Matematica Pura ed Applicata, 64(1):1–76, 1964.

Natalia Silberstein and Anna-Lena Trautmann.

Subspace codes based on graph matchings, ferrers diagrams, and pending blocks.

IEEE Transactions on Information Theory, 61(7):3937–3953, 2015.

Huaxiong Wang, Chaoping Xing, and Reihaneh Safavi-Naini.

Linear authentication codes: bounds and constructions.

IEEE Transactions on Information Theory, 49(4):866–872, 2003.

Shu-Tao Xia and Fang-Wei Fu.

Johnson type bounds on constant dimension codes.

Designs, Codes and Cryptography, 50(2):163–172, 2009.

Thank you for your attention VI

Zong-Ying Zhang, Yong Jiang, and Shu-Tao Xia.

On the linear programming bounds for constant dimension codes.

In *Network Coding (NetCod), 2011 International Symposium on*, pages 1–4. IEEE, 2011.