Coset Construction for Subspace Codes

Network Coding and Designs, Dubrovnik, April 4 - 8, 2016

joined work with

Daniel Heinlein
Daniel.Heinlein@uni-bayreuth.de

Sascha Kurz
Sascha.Kurz@uni-bayreuth.de

2016-04-05

How it started

T. Etzion and N. Silberstein, *Codes and designs related to lifted mrd codes*, IEEE Transactions on Information Theory 59 (2013), no. 2, 1004–1017.

... contained a construction for the special case $A_2(8, 4; 4) \geq 4797$.

The *coset construction* is a generalization of the construction in the paper and is able to generate new largest codes that sometimes attain the MRD bound.

Basics and Notation

Grassmannian: Set of k dimensional subspaces in $\mathbb{F}_q^n = G_q(n,k)$
subspace code: $C \subseteq \bigcup_{k=0}^{n} G_q(n,k)$
constant dimension code (cdc): $C \subseteq G_q(n,k)$
subspace distance: $d_S(U,V) = \dim(U+V) - \dim(U \cap V)$

MRD = maximum rank distance code
LMRD = lifted MRD
MRD bound = upper bound for cdc that contain the LMRD [5]
rref = reduced row echelon form

$$\tau : G_q(n,k) \to \left\{ M \in \mathbb{F}_q^{k\times n} \;\middle|\; \mathrm{rk}(M) = k, M \text{ in rref} \right\}$$

$\Rightarrow \tau$ is bijective

pivot vector of subspace V is called $p(V)$

Idea of the Construction

Take matrices of

$\mathcal{A} \subseteq G_q(n_1, k_1)$ $\qquad$ $\mathcal{B} \subseteq G_q(n_2, k_2)$ $\qquad$ $\overline{F} \subseteq \mathbb{F}_q^{k_1, n_2 - k_2}$ MRD

$$\begin{pmatrix} k_1 \times n_1 & k_1 \times n_2 \\ 0 & k_2 \times n_2 \end{pmatrix}$$

$\Rightarrow$ is in rref

Comparison to Echelon Ferrers [6]: $p(V) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$
Here:

$$p(V) = (\qquad \underbrace{\cdot \quad \cdot \quad \cdot \quad \cdot}_{k_1 \text{ pivots in } n_1 \text{ columns}} \qquad \underbrace{\cdot \quad \cdot \quad \cdot}_{k_2 \text{ pivots in } n_2 \text{ columns}} \qquad)$$

Preliminaries

$\varphi_B(F)$

Let B be a matrix in rref of shape $k_2 \times n_2$. Let F be an arbitrary matrix of shape $k_1 \times (n_2 - k_2)$. Then $\varphi_B(F)$ is the matrix of shape $k_2 \times n_2$ with zero columns in the pivot columns of B and the columns of F otherwise.

Example:

$$\begin{pmatrix} k_1 \times n_1 & k_1 \times n_2 \\ 0 & k_2 \times n_2 \end{pmatrix}$$

$$F = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$B = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$p(B) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\Rightarrow \varphi_B(F) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Construction

The new Code

Under certain requirements (next slide):

$$C := \left\{ \tau^{-1} \begin{pmatrix} A & \varphi_B(F) \\ 0 & B \end{pmatrix} \;\middle|\; \tau^{-1}(A) \in \mathcal{A}_i, \tau^{-1}(B) \in \mathcal{B}_i, 1 \le i \le l, F \in \overline{F} \right\}$$

is a cdc, $C \subseteq G_q(n_1 + n_2, k_1 + k_2)$, $D_S(C) \ge d_1 + d_2$ and size

$$|C| = |\overline{F}| \cdot \sum_{i=1}^{l} |\mathcal{A}_i| \cdot |\mathcal{B}_i|$$

Construction

Requirements

q is a prime power,
$2 \leq d_1$ even, $1 \leq k_1 \leq n_1$, $2 \leq d_2$ even, $1 \leq k_2 \leq n_2$,
$1 \leq k_1 + k_2 \leq (n_1 + n_2)/2$.

$\mathcal{A} := \dot{\bigcup}_{1 \leq i \leq l} \mathcal{A}_i$, $\emptyset \neq \mathcal{A}_i \subseteq G_q(n_1, k_1)$,
such that $D_S(\mathcal{A}_i) \geq d_1 + d_2$ and $D_S(\mathcal{A}) \geq d_1$.

$\mathcal{B} := \dot{\bigcup}_{1 \leq i \leq l} \mathcal{B}_i$, $\emptyset \neq \mathcal{B}_i \subseteq G_q(n_2, k_2)$,
such that $D_S(\mathcal{B}_i) \geq d_1 + d_2$ and $D_S(\mathcal{B}) \geq d_2$.

Let $\overline{F}$ be a rank metric code with distance $\delta := (d_1 + d_2)/2$ and shape $k_1 \times (n_2 - k_2) \rightarrow$ MRD [7]

Construction

The new Code

Under these requirements:

$$C := \left\{ \tau^{-1} \begin{pmatrix} A & \varphi_B(F) \\ 0 & B \end{pmatrix} \;\middle|\; \tau^{-1}(A) \in \mathcal{A}_i, \tau^{-1}(B) \in \mathcal{B}_i, 1 \le i \le l, F \in \overline{F} \right\}$$

is a cdc, $C \subseteq G_q(n_1 + n_2, k_1 + k_2)$, $D_S(C) \ge d_1 + d_2$ and size

$$|C| = |\overline{F}| \cdot \sum_{i=1}^{l} |\mathcal{A}_i| \cdot |\mathcal{B}_i|$$

Note the *packing*:

$D_S(\mathcal{A}) \ge d_1$, $\mathcal{A}$ *packing* of $\mathcal{A}_i$, $D_S(\mathcal{A}_i) \ge d_1 + d_2$

$D_S(\mathcal{B}) \ge d_2$, $\mathcal{B}$ *packing* of $\mathcal{B}_i$, $D_S(\mathcal{B}_i) \ge d_1 + d_2$

Connection Echelon Ferrers - Coset Construction

$$\text{EF} \overset{[6]}{-} \text{EF} \overset{[2]}{-} \text{CC} \overset{[2]}{-} \text{CC}$$

... worst case analysis of pivot vectors and Hamming distance and $d_S(U, V) \geq d_H(p(U), p(V))$ [6]

Especially the LMRD can sometimes be joined with the coset constructed part.
They don't need to have the same dimension!

Example

Two Parallelisms

spread in $G_q(n,k)$ = subset of $G_q(n,k)$ that contains each nonzero vector in $\mathbb{F}_q^n$ exactly once ($\exists$ iff $k \mid n$ [9])
parallelism of $G_q(n,k)$ = partitioning of $G_q(n,k)$ into spreads ($\exists$ sometimes [4])
$\Rightarrow$ subspace distance of spread is $2k$ and size is $\binom{n}{1}_q / \binom{k}{1}_q = \frac{q^n-1}{q^k-1}$

Theorem

Let $\mathcal{A}$ be a parallelism in $G_q(n_1,k_1)$ and $\mathcal{B}$ be a parallelism in $G_q(n_2,k_2)$ with $d_1 = d_2 = 2$. Then the new code is in $G_q(n_1+n_2,k_1+k_2)$, has subspace distance of ≥ 4 and size

$$q^{\max\{0,\max\{k_1,n_2-k_2\}(\min\{k_1,n_2-k_2\}-2+1)\}} \cdot \sum_{i=1}^{\min\{|\mathcal{A}|,|\mathcal{B}|\}} \frac{q^{n_1}-1}{q^{k_1}-1} \cdot \frac{q^{n_2}-1}{q^{k_2}-1}$$

Example

Two Parallelisms, continued

$A_2(8,4;4) \geq 4797$ [5] is a special case of our construction:

For both $\mathcal{A}$ and $\mathcal{B}$ take the parallelism in $G_2(4,2)$.
This yields a code of size

$$2^{\max\{2,4-2\}(\min\{2,4-2\}-2+1)} \cdot \sum_{i=1}^{\min\{|\mathcal{A}|,|\mathcal{B}|\}} \frac{2^4-1}{2^2-1} \cdot \frac{2^4-1}{2^2-1}$$

$$= 2^{2(1)} \cdot \sum_{i=1}^{7} 5 \cdot 5 = 700$$

This can be joined with the lifted MRD code of size 2^{12} and the single codeword that has all pivot columns at the end to get the stated lower bound.
This attains the MRD bound [5] and our bound for $\sum_{i=1}^{l} |\mathcal{A}_i| \cdot |\mathcal{B}_i|$.

Example

Infinite series

Theorem

$$A_q(3k-3, 2k-2; k) \geq \underbrace{q^{4k-6}}_{LMRD} + \underbrace{\frac{q^{2k-3}-q}{q^{k-2}-1} - q + 1}_{=:\alpha} \qquad \textit{for } k \geq 4$$

This attains the MRD bound [5].

Proof.

$n_1 = k, k_1 = 1, d_1 = 2$ $\qquad$ $n_2 = 2k-3, k_2 = k-1, d_2 = 2k-4$

Since $A_q(n_2, d_2; k_2) \overbrace{=}^{[8]} \alpha < \binom{k}{1}_q = A_q(n_1, d_1; k_1)$ take trivial packings of $\mathcal{A}$ and $\mathcal{B}$. □

Example

Recycling the 77 [3]

Theorem

$A_2(10,6;4) \geq 4173 = \underbrace{4096}_{LMRD} + \underbrace{76}_{=:\alpha} + \underbrace{1}_{=:\beta}$

This attains the MRD bound [5].

Proof.

$n_1 = 4, k_1 = 1, d_1 = 2 \Rightarrow \mathcal{A} = G_2(4,1)$ $(\rightarrow \# = 15)$

$n_2 = 6, k_2 = 3, d_2 = 4 \Rightarrow \mathcal{B} \subseteq A_2(6,4;3)$ $(\rightarrow \# = 77)$

Problem: Pack a $(6,77,4;3)_2$ cdc into ≤ 15 cdcs $\mathcal{B}_i$ with $D_S(\mathcal{B}_i) \geq 6$.

Solution: Exactly one isomorphism type admits a packing of 76 elements $\Rightarrow \alpha$.

This code is not maximal and can be extended trivially $\Rightarrow \beta$. □

Open question:

Is it possible to pack the $(6, q^6 + 2q^2 + 2q + 1, 4; 3)_q$ code from [3] into $\binom{4}{1}_q$ sets with minimum subspace distance 6?

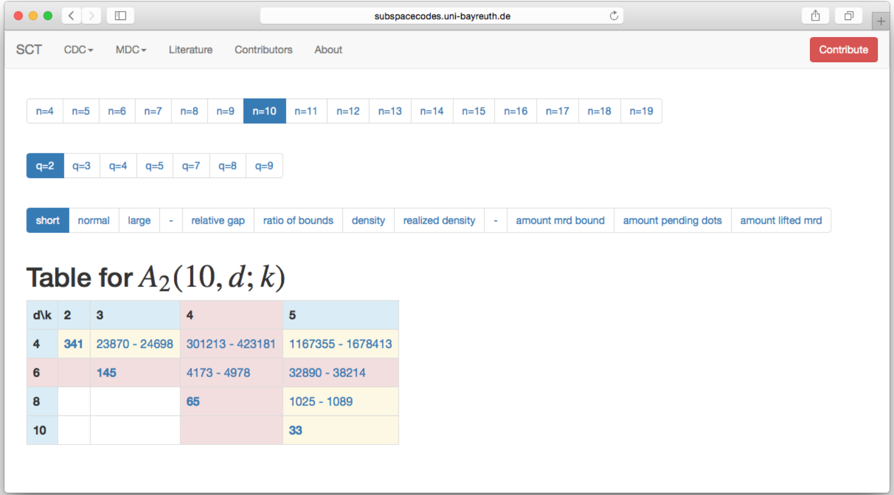

Table for $A_2(10, d; k)$

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**

http://subspacecodes.uni-bayreuth.de

Thank you for your Attention

http://subspacecodes.uni-bayreuth.de

D. Heinlein and S. Kurz, *Coset Construction for Subspace Codes*, arXiv preprint arXiv:1512.07634 (2015).

T. Honold, M. Kiermaier, and S. Kurz, Optimal binary subspace codes of length 6, constant dimension 3 and minimum distance 4, Contemp. Math. 632 (2015), 157–176.

T. Etzion and L. Storme, *Galois geometries and coding theory*, Designs, Codes and Cryptography (2015), 1–40.

T. Etzion and N. Silberstein, *Codes and designs related to lifted mrd codes*, IEEE Transactions on Information Theory 59 (2013), no. 2, 1004–1017.

T. Etzion and N. Silberstein, *Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams*, IEEE Transactions on Information Theory 55 (2009), no. 7, 2909–2919.

E.M. Gabidulin, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii 21 (1985), no. 1, 3–16.

A. Beutelspacher, *Partial spreads in finite projective spaces and partial designs*, Mathematische Zeitschrift 145 (1975), no. 3, 211–229.

J. André, *Über nicht-desarguessche Ebenen mit transitiver Translationsgruppe*, Mathematische Zeitschrift 60 (1954), no. 1, 156–186.