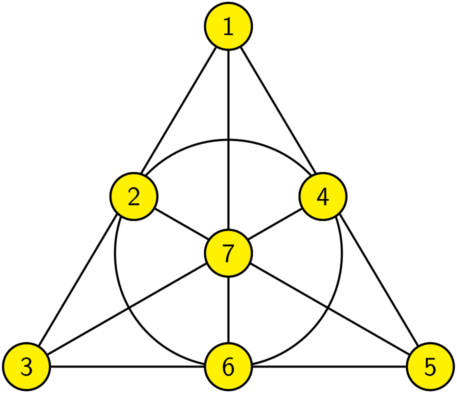
Codes and Designs Over GF(q)

Eimear Byrne
University College Dublin

ICERM, Nov 12-16 2018

A Design - the Fano Plane



$\{1,2,3\}$

$\{1,4,5\}$

$\{1,6,7\}$

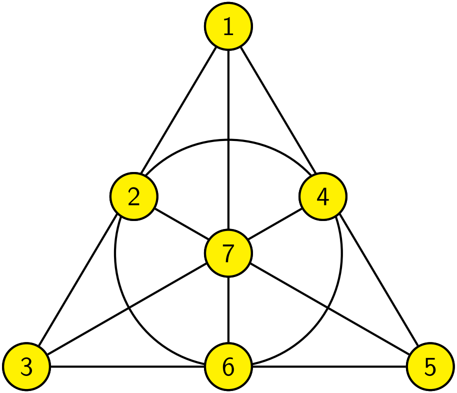
$\{2,4,6\}$

$\{2,5,7\}$

$\{3,4,7\}$

$\{3,5,6\}$

A Design - the Fano Plane



[1,1,1,0,0,0,0]

[1,0,0,1,1,0,0]

[1,0,0,0,0,1,1]

[0,1,0,1,0,1,0]

[0,1,0,0,1,0,1]

[0,0,1,1,0,0,1]

[0,0,1,0,1,1,0]

A Code That Holds a Design - the Hamming Code

$$\begin{array}{c}
[0,0,0,1,1,1,1] \\
[0,1,1,0,0,1,1] \\
[0,1,1,1,1,0,0] \\
[1,0,1,0,1,0,1] \\
[1,0,1,1,0,1,0] \\
[1,1,0,0,1,1,0] \\
[1,1,0,1,0,0,1] \\
\hline
[1,1,1,1,1,1,1]
\end{array}
\qquad
\begin{array}{c}
[1,1,1,0,0,0,0] \\
[1,0,0,1,1,0,0] \\
[1,0,0,0,0,1,1] \\
[0,1,0,1,0,1,0] \\
[0,1,0,0,1,0,1] \\
[0,0,1,1,0,0,1] \\
[0,0,1,0,1,1,0] \\
\hline
[0,0,0,0,0,0,0]
\end{array}$$

Codes and Designs

Definition

A t-(n, d, λ) design is a pair $\mathbf{D} = (\mathbf{P}, \mathbf{B})$, where $\mathbf{P}$ is an n-set (points) and $\mathbf{B}$ is a collection of d-subsets of $\mathbf{P}$ (blocks) such that every t-set of points of $\mathbf{P}$ is contained in exactly λ blocks of $\mathbf{B}$.

- The Fano plane is a 2-$(7, 3, 1)$ design (also called a Steiner system).

Definition

An $\mathbb{F}_q$-$[n, k, d]$ (Hamming metric) code is a k-dimensional subspace of $\mathbb{F}_q^n$, such that the minimum of the Hamming weights of its non-zero elements is d.

- The binary Hamming code shown before is an $\mathbb{F}_2$-$[7, 4, 3]$ code.

q-Analogues of Codes and Designs

Definition

A t-$(n, d, \lambda)_q$ design is a pair $\mathbf{D} = (V, \mathbf{B})$, where V is an n-dimensional $\mathbb{F}_q$-space and $\mathbf{B}$ is a collection of d-dimensional subspaces (blocks) of V, such that every t-dimensional subspace of V is contained in exactly λ blocks of $\mathbf{B}$.

- A q-analogue of the Fano plane would be an 2-$(7, 3, 1)_q$ design.

Definition

An $\mathbb{F}_q$-$[n \times m, k, d]$ rank metric code is a k-dimensional subspace of $\mathbb{F}_q^{n\times m}$, such that the minimum of the ranks of its non-zero elements is d.

- Any k-dimensional subspace of $\mathbb{F}_{q^m}^n$ is a km-dimensional rank metric code.

The Assmus-Mattson Theorem

Hamming Weight Distributions

The Hamming weight of $v \in \mathbb{F}_q^n$ is: $w_H(v) := |\{i : v_i \neq 0\}|$.

The support of v is: $\sigma_H(v) := \{i : v_i \neq 0\}$.

Definition

Let C be an $\mathbb{F}_q$-$[n,k]$ code. The Hamming weight distribution of C is $(A_i(C) : i \geq 0)$ where

$$A_i(C) := |\{c \in C : w_H(c) = i\}|.$$

If $A_i(C) \neq 0$ and $i \geq 1$, we say that i is a weight of C.

- The 3-supports of the Hamming code shown are the blocks of the Fano plane.
- An $\mathbb{F}_2$-$[7,4,3]$ code has weight distribution $(1,0,0,7,7,0,0,1)$.
- The weight distribution of an extremal code is often determined.

Duality

- $C^\perp = \{x \in \mathbb{F}_q^n : x \cdot y = 0 \, \forall y \in C\}$.
- The Assmus-Mattson theorem relies on the MacWilliams duality theorem:

$$(A_i(C) : 0 \leq i \leq n)P = (A_i(C^\perp) : 0 \leq i \leq n),$$

  for an invertible transform matrix P.

Example

If C is the $\mathbb{F}_2$-$[7,4,3]$ (Hamming) code, then $C^\perp$ is the $\mathbb{F}_2$-$[7,3,4]$ (Simplex) code

- C has weight distribution $(1,0,0,7,7,0,0,1)$,
- $C^\perp$ has weight distribution $(1,0,0,0,7,0,0,0)$.

The Assmus-Mattson Theorem

Theorem (Assmus-Mattson, 1969)

Let C be an $\mathbb{F}_q$-$[n,k,d]$ code. Let $t \leq d \leq n-t$. Suppose that $C^\perp$ has at most $d-t$ weights in $\{1,\dots,n-t\}$. Then the supports of the words of weight d in C form the blocks of a t-design.

Let w be the greatest integer such that for each $d \leq s \leq w$ and every s-support S of C

$$|\{c \in C : \sigma_H(c) = S\}| \text{ depends only on } s.$$

Let $w^\perp$ be defined similarly. Then the

1. *s-supports of C form the blocks of a t-design, $d \leq s \leq w$,*
2. *s-supports of $C^\perp$ form the blocks of a t-design, $d^\perp \leq s \leq \min\{w^\perp, n-t\}$.*

- The (Hamming) support of c is $\sigma_H(c) := \{i : c_i \neq 0\}$.

The Assmus-Mattson Theorem

Theorem

Let C be an $\mathbb{F}_q$-$[n,k,d]$ code. Let $t \leq d \leq n-t$. Suppose that $C^\perp$ has at most $d-t$ weights in $\{1,...,n-t\}$. Then the d-supports of C form the blocks of a t-(n,d,λ) design.

- The $\mathbb{F}_2$-$[7,4,3]$ code C has dual with weight distribution $(1,0,0,0,7,0,0,0)$. As $d-2=3-2=1$, the 3-supports of C form a 2-design.
- The $\mathbb{F}_2$-$[24,12,8]$ Golay code is self-dual with weights $\{8,12,16,24\}$. There are $8-5=3$ weights $\leq 25-5=19$.The 8-supports form a 5-$(24,8,1)$ design.
- The $\mathbb{F}_3$-$[12,6,6]$ Golay code is self-dual with weights $\{6,9,12\}$. There is $6-5=1$ weight $\leq 12-5=7$. The 6-supports form a 5-$(12,6,1)$ design.
- Many classes of BCH codes have dual codes with few weights & hold designs.

Subspace Designs

Subspace Designs

Theorem

Let $n \equiv 1 \mod 6, n \geq 7$. *Let* $\mathbf{P} = \mathbb{F}_{q^n}^{\times}$ *and let*

$$\mathbf{B} := \{\langle x^2, xy, y^2\rangle_{\mathbb{F}_q} : \langle x, y\rangle \subset \mathbb{F}_{q^n}^{\times}, \dim_{\mathbb{F}_q}\langle x, y\rangle = 2\}.$$

Then $(\mathbf{P}, \mathbf{B})$ *is a* $2\text{-}(n, 3, q^2+q+1)_q$ *design.*

- Thomas, 1987, $q = 2$, construction using orbits of planes under $\mathbb{F}_{2^n}^{\times}$
- Suzuki, 1990, $q = 2^m$; 1992 any prime power q.

Problem

If $(n, (2r)!) = 1$, *is this a design?*

$$\mathbf{B} := \{\langle x^r, x^{r-1}y, \ldots, xy^{r-1}, y^r\rangle_{\mathbb{F}_q} : \langle x, y\rangle \subset \mathbb{F}_{q^n}^{\times}, \dim_{\mathbb{F}_q}\langle x, y\rangle = 2\}.$$

Other Examples

- Most known examples of subspace designs were found by prescribing an automorphism group.
- $\tau \in \Gamma L(V)$ is an automophism of $(V, \mathbf{B})$ if $B \in \mathbf{B} \implies B^\tau \in \mathbf{B}$.
- The first t-subspace design with $t = 3$ was found with the normalizer of a Singer cycle as an automorphism group (Braun, Kerber, Laue, 2005).

If A is the $\begin{bmatrix} n \\ t \end{bmatrix}_q \times \begin{bmatrix} n \\ d \end{bmatrix}_q$ incidence matrix of t-subspaces and k-subspaces, then finding a t-(n, d, λ) designs amounts to solving the following equation for a $0-1$ vector x.

$$Ax = \lambda \mathbf{1}.$$

If we assume an automorphism group of the design, then A is replaced with a $T \times D$ matrix with T orbits of t-spaces and D orbits of d-spaces.

Subspace Designs - Steiner Systems

- A $(k-1)$-spread in $PG(n-1,q)$ is a 1-$(n,k,1)_q$ design.
- A 2-$(n,3,1)_q$ is called a q-Steiner triple system, $STS_q(n)$.
- An $STS_q(n)$ exists only if $n \equiv 1 \mod 6$ or $n \equiv 3 \mod 6$.
- It is not yet known if there exists an $STS_q(7)$, i.e. a 2-$(7,3,1)_q$ design, - the q-analogue of the Fano plane.

Theorem (Braun, Etzion, Östergard, Vardy, Wassermann, 2016)

2-$(13,3,1)_2$ *Steiner triple systems exist.*

Theorem (Braun, Wassermann, 2018)

There are 1316 mutually disjoint $2-(13,3,1)_2$ *designs, which implies the existence of a* 2-$(13,3,\lambda)$ *design for each* $\lambda \in \left\{1,\ldots,2047 = \begin{bmatrix} 13-2 \\ 3-2 \end{bmatrix}_2\right\}$.

Itoh's Construction

Theorem (Itoh, 1998)

Let $v, s, r, \ell \in \mathbb{N}_0$ such that $r \in \{0,1\}$, $r = 0$ if $3 \not| \ \ell$ and

$$\lambda = q(q+1)(q^3-1)s + q(q^2-1)r.$$

Let $S(\ell, q)$ be the conjugacy class of Singer cycle groups in $GL(\ell, q)$.

If there exists an $S(\ell, q)$-invariant 2-$(\ell, 3, \lambda)_q$ design then there exists an $SL(v, q^\ell)$-invariant 2-$(v\ell, 3, \lambda)_q$ design.

Itoh's result has been used to obtain many concrete examples of subspace designs.

Existence of Subspace Designs

Theorem (Fazeli, Lovett, Vardy, 2014)

Let q be a prime power and let n, d, t be positive integers with $d > 12(t+1)$.

If $n \geq cdt$ for a sufficiently large constant c, then there exists a non-trivial t-$(n, d, \lambda)_q$ design.

Moreover, these designs have at most $q^{12(t+1)n}$ blocks.

An existence result for q-Steiner systems is not known.

Known Infinite Families

t-(n,r,λ)	$\mathbb{F}_q$	Constraints	
2-$(n,3,7)$	$\mathbb{F}_2$	$(n,6)=1,\ n\geq 7$	1987
2-$\left(n,3,\begin{bmatrix}3\\1\end{bmatrix}_q\right)$	$\mathbb{F}_q$	$(n,6)=1,\ n\geq 7$	1992
2-$\left(\ell s,3,q^3\begin{bmatrix}s-5\\1\end{bmatrix}_q\right)$	$\mathbb{F}_q$	if $\exists$ 2-$\left(s,3,q^3\begin{bmatrix}s-5\\1\end{bmatrix}_q\right)$ design over $\mathbb{F}_q$ that is invariant under a Singer cycle	1999
2-$\left(n,r,\frac{1}{2}\begin{bmatrix}n-2\\r-2\end{bmatrix}_q\right)$	$\mathbb{F}_3,\mathbb{F}_5$	$n\geq 6,\ n\equiv 2 \mod 4$, $3\leq r\leq n-3,\ r\equiv 3 \mod 4$	2017

Table: Known infinite families of subspace designs.

Some Remarks

- Up to now, there are no other methods known to produce subspace designs.
- Actions of t-transitive groups yield only trivial subspace designs.
- Prescribing an automorphism group still requires parameters to be not too big.
- A new approach is required if there is any hope to find infinite families.

This motivates using ideas from coding theory to construct new subspace designs.

Matrix Codes and Designs

Supports in Matrix Codes

- For any $X \in \mathbb{F}_q^{n\times m}$, define $\sigma(X) := \mathrm{colspace}(X)$.
- For any $x \in \mathbb{F}_{q^m}^n$, define $\sigma(x) := \mathrm{colspace}(\Gamma(x))$, where $\Gamma(x) \in \mathbb{F}_q^{m\times n}$ is the expression of x wrt an $\mathbb{F}_q$-basis Γ of $\mathbb{F}_{q^m}$.
- An r-support of a rank metric code is an r-dimensional subspace U of $\mathbb{F}_q^n$ that is the support of a codeword.

Question

When do the r-supports of a rank metric code form a subspace design?

An Assmus-Mattson Theorem for Rank Metric Codes

Theorem (B., Ravagnani, 2018)

Let C be an $\mathbb{F}_q$-$[n \times m, k, d]$ rank metric code. Let $t \leq d \leq n-t$. Suppose that $C^\perp$ has at most $d-t$ ranks in $\{1, ..., n-t\}$.

Let w be the greatest integer such that for each $d \leq s \leq w$ and every s-support $S \subset \mathbb{F}_q^n$ of C

$$|\{c \in C : \sigma(c) = S\}| \text{ depends only on } s.$$

Let $w^\perp$ be defined similarly. Then the

1. *s-supports of C form a t-subspace design, $d \leq s \leq w$.*
2. *s-supports of $C^\perp$ form a t-subspace design, $d^\perp \leq s \leq \min\{w^\perp, n-t\}$.*

An Assmus-Mattson Theorem for Rank Metric Codes

1. MacWilliams duality theorem holds for rank metric codes.
2. There exist dual operations of puncturing and shortening.
3. Compatibility of these operations with supports of matrices.
4. Invariance of matrix rank under $\mathbb{F}_q$-isomorphisms.

Basic Idea

- If $C^\perp$ has $d-t$ ranks, the weight distribution of any punctured code of C in $\mathbb{F}_q^{(n-t)\times m}$ is determined.
- The words of rank $d-t$ in a punctured code in $\mathbb{F}_q^{(n-t)\times m}$ correspond to words of rank d whose d-supports contain a t-dimensional space.
- This number is invariant of the choice of subspace.

An Assmus-Mattson Theorem for Rank Metric Codes

Corollary (B., Ravagnani, 2018)

Let C be an $\mathbb{F}_{q^m}$-$[n,k,d]$ code. Let $1 \leq t < d$ be an integer, and assume that

$$|\{1 \leq i \leq n-t \ : \ W_i(C^\perp) \neq 0\}| \leq d-t.$$

Let $d^\perp$ be the minimum distance of $C^\perp$. Then

1. *the d-supports of C form the blocks of a t-design over $\mathbb{F}_q$,*
2. *the $d^\perp$-supports of $C^\perp$ form the blocks of a t-design over $\mathbb{F}_q$.*

A Subspace Design from a Rank Metric Code

Example

Let s be a positive integer and let $m = 2s$. Let $\{\alpha_1, \ldots \alpha_m\}$ be an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. Let C be the $\mathbb{F}_{q^m}$-$[m, m-2, 2]$ vector rank metric code with parity check matrix

$$H = \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^{q^s} & \alpha_2^{q^s} & \cdots & \alpha_m^{q^s} \end{bmatrix}.$$

Then $C^\perp$ has $\mathbb{F}_q$-ranks $\{s, 2s\}$.

Set $t = 1$. $C^\perp$ has exactly $d - t = 1$ weight, s, in $\{1, \ldots, 2s-1\}$.

The supports of the codewords of C of rank 2 form a 1-design over $\mathbb{F}_q$ and the words of rank s in $C^\perp$ form a 1-$(m, s, 1)$ subspace design (a spread).

A Subspace Design from a Rank Metric Code

Example

Let $n \leq m$ and let $\{\alpha_1, ..., \alpha_n\} \subset \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$.
Let C be the $\mathbb{F}_{q^m}$-$[n, k, n-k+1]$ rank metric code generated by the rows of

$$G = \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_n^q \\ \alpha_1^{q^2} & \alpha_2^{q^2} & \cdots & \alpha_n^{q^2} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{q^{k-1}} & \alpha_2^{q^{k-1}} & \cdots & \alpha_n^{q^{k-1}} \end{bmatrix}.$$

$C^\perp$ has ranks $\{d^\perp = k+1, k+2, ..., n\}$. For $1 \leq t \leq d$, $C^\perp$ has

$$n - t - d^\perp + 1 = n - t - k < d - t = n - k + 1 - t$$

ranks in $\{1, ..., n-t\}$. So the minimum rank vectors of C and $C^\perp$ hold t-designs..

MRD Codes

An $\mathbb{F}_q$-$[n \times m, k, d]$ code is called MRD if $k = \max\{m, n\}(\min\{m, n\} - d + 1)$.

- The minimum rank words of any MRD code hold t-designs, but they are trivial! Every d-dimensional space of $\mathbb{F}_q^n$ is a d-support of the code.
- If an $\mathbb{F}_{q^m}$-$[n, k, d]$ rank metric code holds a trivial design, it must be MRD.
- The last statement is false for rank metric codes that are not $\mathbb{F}_{q^m}$-linear.

Other Examples?

No constructions of codes that hold non-trivial designs for $t \geq 2$ are known yet.

- Not many classes of rank-metric codes are known.
- Known families of rank metric codes are all MRD.
- Subspace designs from MRD codes are trivial.

Problem

Construct a family of $\mathbb{F}_{q^m}$-linear rank metric codes with a small number of ranks.

Problem

Construct $\mathbb{F}_q$-linear matrix codes where the number of codewords with a given d-support is invariant.

Existence Results

Lemma (B. Ravagnani, 2018)

Let C is an $\mathbb{F}_q$-$[n \times m, k, d]$ code satisfying the hypothesis of of the rank-metric Assmus-Mattson theorem. If $m \geq \log_q(4) + n^2/4$, then $C^\perp$ has either d or $d+1$ ranks.

Theorem (B. Ravagnani, 2018)

Let C be an $\mathbb{F}_{q^m}$-$[n, k, d]$ code if $m \geq n$ is sufficiently large then $C^\perp$ has at least $n-k$ ranks.

Corollary (B. Ravagnani, 2018)

Let C be an $\mathbb{F}_{q^m}$-$[n, k, d]$ code and let $1 \leq t \leq d-1$. If $m \geq n$ is sufficiently large and if C satisfies the hypothesis of the rank-metric Assmus-Mattson theorem then $d \geq n-k$.

Existence Questions

Problem

Are any of the known subspace designs realizable as d-supports of $\mathbb{F}_{q^m}$-$[n,k,d]$ *rank metric codes?*

Problem

Does there exist an $\mathbb{F}_{q^m}$-$[7,k,3]$ *rank metric code whose* 3*-supports form the Fano plane?*

Problem

Do there exist q-BCH codes with minimum rank distance ≥ 5 *whose dual codes have few ranks?*

Problem

What can we say in general about existence of codes satisfying the rank Assmus-Mattson theorem?

References

- E. F. Assmus, Jr., H. F. Mattson, Jr., New 5-Designs, Jour. Comb. Thy, **6** 1969.
- M. Braun, M. Kiermaier, A. Kohnert, R. Laue, Large Sets of Subspace Designs, Jour. Comb. Thy (A), **147**, 2017.
- M. Braun, M. Kiermaier, A. Wassermann, q-Analogs of Designs: Subspace Designs, in Network Coding and Subspace Designs, Eds. M. Greferath, M. Pavcevic, A. Vazquez-Castro, N. Silberstein, Springer-Verlag Berlin, 2018.
- M. Braun, M. Kiermaier, A. Wassermann, Computational Methods in Subspace Designs, in Network Coding and Subspace Designs, Eds. M. Greferath, M. Pavcevic, A. Vazquez-Castro, N. Silberstein, Springer-Verlag Berlin, 2018.
- A. Fazeli, S. Lovett, A. Vardy, Nontrivial t-Designs Over Finite Fields Exist For All t, J. Combin. Theory Ser. A 127, 2014.
- T. Itoh, A New Family of 2-designs over $GF(q)$ Admitting $\mathrm{SL}_m(q^\ell)$, Geom. Dedicata 69(3), 1998.
- H. Suzuki, 2-Designs over $GF(q)$ Graphs Comb. **8** (4), 1992.
- H. Suzuki, On the Inequalities of t-Designs Over a Finite Field, European J. Combin., **11**, 6, 1990.