# The linear codes of $t$-designs held in the Reed-Muller and Simplex codes

Cunsheng Ding
Chunming Tang

Hong Kong University of Science and Technology
and
China West Normal University, Nanchong, China

BFA 2020, Loen, Norway

# Contents

# Recall of $t$-designs

# $t$-designs

## Definition 1

Let $t$, $k$ and $v$ be integers with $1 \leq t \leq k \leq v$. Let $\mathcal{P} = \{p_1, \cdots, p_v\}$ be a set, and $\mathcal{B} = \{B_1, \cdots, B_b\}$, where each $B_i$ is a $k$-subset of $\mathcal{P}$. The pair $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ is called a $t$-$(v, k, \lambda)$ **design**, or simply a ***t*-design**, if every $t$-subset of $\mathcal{P}$ is contained in precisely $\lambda$ subsets $B_i$, where $\lambda$ is a positive integer.

A $t$-$(v, k, 1)$ design is called a **Steiner system**, and denoted by $S(t, k, v)$.

The elements in $\mathcal{P}$ are called **points**, and these $B_i$ are called **blocks** or **lines**.

## Example 2 (Fano plane in finite geometry)

Let $\mathcal{P} = \{1, 2, 3, 4, 5, 6, 7\}$ and

$$\mathcal{B} = \{\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,7\}, \{2,5,6\}, \{3,5,7\}, \{3,4,6\}\}.$$

Then $(\mathcal{P}, \mathcal{B})$ is a 2-$(7, 3, 1)$ design, i.e., Steiner triple system $S(2, 3, 7)$.

# Support $t$-designs from linear codes

# The support designs of linear codes

## The idea of construction

Let $\mathcal{C}$ be a code of length $v$ and let the coordinates of codewords in $\mathcal{C}$ be indexed by $\mathcal{P} := \{p_1, \ldots, p_v\}$. The *support* of $\mathbf{c} = (c_{p_1}, c_{p_2}, \ldots, c_{p_v}) \in \mathcal{C}$ is

$$\mathrm{Suppt}(\mathbf{c}) = \{p_i : 1 \le i \le v,\ c_{p_i} \neq 0\} \subseteq \mathcal{P}.$$

Let $\mathcal{B}_w(\mathcal{C})$ be the set of the supports of the codewords of weight $w$ in $\mathcal{C}$, where no repeated blocks are allowed.

Then it is possible that $\mathbb{D}_w(\mathcal{C}) := (\mathcal{P}, \mathcal{B}_w(\mathcal{C}))$ is a $t$-design for some $t$. In this case, we say that $\mathcal{C}$ holds or supports a $t$-design.

## Question

When is the pair $\mathbb{D}_w(\mathcal{C}) := (\mathcal{P}, \mathcal{B}_w(\mathcal{C}))$ from a code $\mathcal{C}$ a $t$-design for some $t$?

# The support designs of linear codes

## Example 3

Let $\mathcal{C}$ be the binary cyclic code of length 7 with generator polynomial $g(x) = x^3 + x + 1$. Then the Hamming code $\mathcal{C}$ has parameters $[7,4,3]$ and weight enumerator $1 + 7z^3 + 7z^4 + z^7$. The codewords of weight 3 are:

$$
\begin{array}{lll}
(0100011) & \{2,6,7\} & B_1 \\
(1010001) & \{1,3,7\} & B_2 \\
(1101000) & \{1,2,4\} & B_3 \\
(0110100) & \{2,3,5\} & B_4 \\
(0011010) & \{3,4,6\} & B_5 \\
(1000110) & \{1,5,6\} & B_6 \\
(0001101) & \{4,5,7\} & B_7
\end{array}
$$

Let $\mathcal{P} = \{1,2,3,4,5,6,7\}$. Then $(\mathcal{P}, \mathcal{B})$ is a 2-$(7,3,1)$ design, i.e., the Fano plane.

# The support designs of linear codes

**Question**

When is the pair $(\mathcal{P}, \mathcal{B}_w(\mathcal{C}))$ from a linear code $\mathcal{C}$ a $t$-design for some $t \geq 1$?

**Some sufficient conditions**

- The Assmus-Mattson theorem (1969).
- The generalised Assmus-Mattson theorem (Tang-Ding-Xiong 2020).
- When the automorphism group of $\mathcal{C}$ is $t$-homogeneous or $t$-transitive.

**A research direction for over 70 years**

- E. F. Assmus Jr., H. F. Mattson Jr., New 5-designs, J. Comb. Theory 6 (1969) 122–151.
- C. Tang, C. Ding, M. Xiong, Codes, differentially $\delta$-uniform functions and $t$-designs, IEEE Trans. Inf. Theory 66(6) (2020) 3691–3703.
- C. Ding, Designs from Linear Codes, World Scientific, Singapore, 2018.

# Classical linear codes of t-designs

# Linear codes of a $t$-design

## Incidence matrix of a $t$-design

Let $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ be a $t$-design with $v \geq 1$ points and $b \geq 1$ blocks. The points of $\mathcal{P}$ are usually indexed with $p_1, p_2, \ldots, p_v$, and the blocks of $\mathcal{B}$ are normally denoted by $B_1, B_2, \ldots, B_b$. The *incidence matrix* $M_{\mathbb{D}} = (m_{ij})$ of $\mathbb{D}$ is a $b \times v$ matrix where $m_{ij} = 1$ if $p_j$ is on $B_i$ and $m_{ij} = 0$ otherwise.

## Linear codes of a $t$-design

Let $M_{\mathbb{D}}$ be the incidence matrix of a $t$-design $\mathbb{D}$. When $M_{\mathbb{D}}$ is viewed as a matrix over $\mathrm{GF}(q)$, its rows span a linear code of length $v$ over $\mathrm{GF}(q)$, denoted by $\mathcal{C}_q(\mathbb{D})$.

## Another research direction with a long history

- E. F. Assmus and J. D. Key, Designs and Their Codes, Cambridge University Press, Cambridge, 1992.
- C. Ding, Codes from Difference Sets, World Scientific, Singapore, 2015.

# A research problem

# A research problem

**Choose a code $\mathcal{C}_1$ supporting a design, study the new code $\mathcal{C}_2$ below:**

Let $q = p^s$

$\mathcal{C}_1$ over $\mathrm{GF}(q) \Rightarrow$ a $t$-design $\mathbb{D}_k(\mathcal{C}_1)$ held in $\mathcal{C}_1 \Rightarrow \mathcal{C}_2 := \mathcal{C}_p(\mathbb{D}_k(\mathcal{C}_1))$.

**Remarks**

- $\mathcal{C}_q(\mathbb{D}_k(\mathcal{C}_1))$ and $\mathcal{C}_p(\mathbb{D}_k(\mathcal{C}_1))$ have the same length, dimension and minimum distance. Hence, we consider mainly $\mathcal{C}_p(\mathbb{D}_k(\mathcal{C}_1))$.
- Many infinite families of linear codes supporting $t$-designs are known.
- Not much work is done in this direction.
- In this talk, we consider the Reed-Muller codes and Simplex codes as the starting code $\mathcal{C}_1$.

# The codes of the designs held in the Simplex codes

# Simplex Codes

We view $\mathrm{GF}(q^m)$ as an $m$-dimensional vector space over $\mathrm{GF}(q)$. Let $\alpha$ be a generator of $\mathrm{GF}(q^m)^*$. Let $v = (q^m-1)/(q-1)$. Then

$$\mathcal{P} = \{1, \alpha, \alpha^2, \ldots, \alpha^{v-1}\} = \mathrm{GF}(q^m)^*/\mathrm{GF}(q)^*$$

is the set of points in the projective geometry $\mathrm{PG}(m-1, q)$.
By the definition $\alpha$ and $v$, it is easily seen that

$$\left\{(\mathrm{Tr}(a\alpha^i))_{i=0}^{v-1} : a \in \mathrm{GF}(q^m)\right\} \tag{1}$$

is the Simplex code with weight enumerator $1 + (q^m-1)z^{q^{m-1}}$.
The $[v, v-m, 3]$ Hamming code is the dual of the Simplex code.

# The design held in the Simplex code

## The design

By the Assmus-Mattson theorem, the codewords of weight $q^{m-1}$ in the Simplex code support a design $\mathbb{D}$ with the following parameters

$$2\text{-}\left(\frac{q^m-1}{q-1},\ q^{m-1},\ (q-1)q^{m-2}\right). \tag{2}$$

## Questions

- Let $q = p^s$. What are the parameters of the code $\mathcal{C}_p(\mathbb{D})$?
- Is $\mathcal{C}_p(\mathbb{D})$ a good code?

# The code of the design held in the Simplex code

## Theorem 4

*Let $q = p^s$. The code $\mathcal{C}_p(\mathbb{D})$ of the design $\mathbb{D}$ has parameters*

$$\left[\frac{q^m-1}{q-1}, \binom{p+m-2}{m-1}^s, d \geq 2q^{m-2}\right].$$

*Moreover, if $q = p$, $d = 2q^{m-2}$.*

## Conjecture 1

*Let $\mathbb{D}$ be defined as before and $q = p^s$. Then $d\left(\mathcal{C}_p(\mathbb{D})\right)$ equals $2q^{m-2}$.*

## The outline of proof of Theorem 4

- The designs $\mathbb{D}$ and $\mathrm{PG}_{m-2}(m-1, q)$ are the complement of each other.
- $\mathcal{C}_p(\mathbb{D})$ is a subcode of $\mathcal{C}_p(\mathrm{PG}_{m-2}(m-1, q))$ $(= \mathrm{PRM}(1, m-1, p))$ with dimension one less.

# The codes $\mathcal{C}_p(\mathbb{D})$ and $\mathcal{C}_p(\mathrm{PG}_{m-2}(m-1,q))$

- $\mathcal{C}_p(\mathbb{D})$ is a subcode of the geometry code $\mathcal{C}_p(\mathrm{PG}_{m-2}(m-1,q))$ with dimension one less.
- $\mathcal{C}_p(\mathbb{D})$ is much better than $\mathcal{C}_p(\mathrm{PG}_{m-2}(m-1,q))$.

| $(q,m)$ | $\mathcal{C}_p(\mathbb{D})$ | $\mathcal{C}_p(\mathrm{PG}_{m-2}(m-1,q))$ |
|---|---|---|
| $(3,2)$ | $[4,3,2]$ | $[4,4,1]$ |
| $(3,3)$ | $[13,6,6]$ | $[13,7,4]$ |
| $(3,4)$ | $[40,10,18]$ | $[40,11,13]$ |
| $(3,5)$ | $[121,15,54]$ | $[121,16,40]$ |
| $(4,2)$ | $[5,4,2]$ | $[5,5,1]$ |
| $(4,3)$ | $[21,9,8]$ | $[21,10,5]$ |
| $(4,4)$ | $[85,16,32]$ | $[85,17,21]$ |
| $(5,2)$ | $[6,5,2]$ | $[6,6,1]$ |
| $(5,3)$ | $[31,15,10]$ | $[31,16,6]$ |

# The dual of the code of the design held in the Simplex code

## Theorem 5

*Let $q = p^s$ and $\mathbb{D}$ be defined as before. The dual code $\mathcal{C}_p(\mathbb{D})^\perp$ has parameters*

$$\left[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - \binom{p+m-2}{m-1}^s, d^\perp\right],$$

*where $d^\perp \geq 3$. Moreover, if $q = p$, $d^\perp = p+1$.*

## Conjecture 2

*Let $\mathbb{D}$ be defined as before. The minimum distance of the code $\mathcal{C}_p(\mathbb{D})^\perp$ equals $q+1$.*

# The codes of the designs held in the Reed-Muller codes

# The punctured generalized Reed-Muller codes

## Definition 6

Let $\ell$ be a positive integer with $1 \leq \ell < (q-1)m$. The $\ell$-th order *punctured generalized Reed-Muller code* $\mathcal{R}_q(\ell, m)^*$ over $\mathrm{GF}(q)$ is the cyclic code of length $n = q^m - 1$ with generator polynomial

$$g(x) = \prod_{\substack{1 \leq j \leq n-1 \\ \mathrm{wt}_q(j) < (q-1)m-\ell}} (x - \alpha^j), \tag{3}$$

where $\alpha$ is a generator of $\mathrm{GF}(q^m)^*$ and $\mathrm{wt}_q(j)$ is the $q$-weight of $j$.
Since $\mathrm{wt}_q(j)$ is a constant function on each $q$-cyclotomic coset modulo $n = q^m - 1$, $g(x)$ is a polynomial over $\mathrm{GF}(q)$.

# The generalized Reed-Muller codes

The generalized Reed-Muller code $\mathcal{R}_q(\ell, m)$ is defined to be the extended code of $\mathcal{R}_q(\ell, m)^*$, and its parameters are given below.

## Theorem 7

*Let $0 \le \ell < q(m-1)$. Then the generalized Reed-Muller code $\mathcal{R}_q(\ell, m)$ has length $n = q^m$, dimension*

$$\kappa = \sum_{i=0}^{\ell} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{i - jq + m - 1}{i - jq},$$

*and minimum weight*

$$d = (q - \ell_0) q^{m - \ell_1 - 1},$$

*where $\ell = \ell_1(q-1) + \ell_0$ and $0 \le \ell_0 < q - 1$.*

**Remark**: $\mathcal{R}_q(\ell, m)^\perp = \mathcal{R}_q(m(q-1) - 1 - \ell, m)$.

# The generalized Reed-Muller codes

## Theorem 8

*Let* $0 \le \ell < q(m-1)$ *and* $\ell = \ell_1(q-1) + \ell_0$, *where* $0 \le \ell_0 < q-1$. *The total number* $A_{(q-\ell_0)q^{m-\ell_1-1}}$ *of minimum weight codewords in* $\mathcal{R}_q(\ell, m)$ *is given by*

$$A_{(q-\ell_0)q^{m-\ell_1-1}} = (q-1)\frac{q^{\ell_1}(q^m-1)(q^{m-1}-1)\cdots(q^{\ell_1+1}-1)}{(q^{m-\ell_1}-1)(q^{m-\ell_1-1}-1)\cdots(q-1)}N_{\ell_0},$$

*where*

$$N_{\ell_0} = \begin{cases} 1 & \text{if } \ell_0 = 0, \\ \binom{q}{\ell_0}\frac{q^{m-\ell_1}-1}{q-1} & \text{if } 0 < \ell_0 < q-1. \end{cases}$$

# Affine-invariant codes of length $r$

## Definition 9

The general affine group $\mathrm{GA}_1(\mathrm{GF}(r))$ is defined by

$$\mathrm{GA}_1(\mathrm{GF}(r)) = \{ax + b : a \in \mathrm{GF}(r)^*,\ b \in \mathrm{GF}(r)\},$$

which acts on $\mathrm{GF}(r)$ doubly transitively.

## The action of $\mathrm{GA}_1(\mathrm{GF}(r))$ on a code of length $r$

Let $\mathcal{C}$ be a code of length $r$. We index the coordinates of codewords in $\mathcal{C}$ with the elements in $\mathrm{GF}(r)$.
Any $\sigma$ in $\mathrm{GA}_1(\mathrm{GF}(r))$ acts on the coordinates of a codeword when it acts on the codeword.

## Definition 10

A linear code $\mathcal{C}$ of length $r$ is said to be affine-invariant if $\mathrm{GA}_1(\mathrm{GF}(r))$ fixes $\mathcal{C}$.

# The designs held in $\mathcal{R}_q(\ell, m)$

**Theorem 11**

*Let $\ell$ be a positive integer with $1 \leq \ell < (q-1)m$. Then the supports of the codewords of weight $i > 0$ in $\mathcal{R}_q(\ell, m)$ form a $2$-design, provided that $A_i \neq 0$.*

**Outline of proof.**

Note that $\mathcal{R}_q(\ell, m)$ is affine-invariant and $\mathrm{GA}_1(\mathrm{GF}(q^m))$ acts on $\mathrm{GF}(q^m)$ doubly transitively. $\square$

**Remark**

- The parameters of the 2-design supported by the minimum weight codewords in $\mathcal{R}_q(\ell, m)$ are known (due to Theorem 8.)

# The codes $\mathcal{C}_p(\mathbb{D}_w(\mathcal{R}_q(\ell, m)))$

## Question

Let $q = p^s$ and $A_w > 0$. What are the parameters of the code $\mathcal{C}_p(\mathbb{D}_w(\mathcal{R}_q(\ell, m)))$?

## Partial answers

- $\ell = 1$.
- $\ell = 2$ and $q = p = 3$.

# The code $\mathcal{C}_p(\mathbb{D}_{(q-1)q^{m-1}}(\mathcal{R}_q(1,m)))$

## Theorem 12

*$\mathcal{R}_q(1,m)$ has parameters $[q^m, 1+m, (q-1)q^{m-1}]$ and weight enumerator*

$$1 + q(q^m - 1)z^{(q-1)q^{m-1}} + (q-1)z^{q^m}. \tag{4}$$

*Furthermore, the supports of all minimum weight codewords in $\mathcal{R}_q(1,m)$ form a $2$-$(q^m, (q-1)q^{m-1}, (q-1)q^{m-1}-1)$ design*

## Question

What are the parameters of the code $\mathcal{C}_p(\mathbb{D}_{(q-1)q^{m-1}}(\mathcal{R}_q(1,m)))$?

# The code $\mathcal{C}_p(\mathbb{D}_{(q-1)q^{m-1}}(\mathcal{R}_q(1,m)))$

## Theorem 13

*Let* $\mathbb{D}_{(q-1)q^{m-1}}(\mathcal{R}_q(1,m))$ *denote the* 2*-design supported by the codewords of weight* $(q-1)q^{m-1}$ *in* $\mathcal{R}_q(1,m)$*. Then* $\mathcal{C}_p(\mathbb{D}_{(q-1)q^{m-1}}(\mathcal{R}_q(1,m)))$ *has parameters*

$$\left[q^m,\ \binom{p+m-1}{m}^s,\ q^{m-1}\right],$$

*where* $q = p^s$*.*

## The outline of the proof of Theorem 13

- The design $\mathbb{D}_{(q-1)q^{m-1}}(\mathcal{R}_q(1,m))$ and the geometry design $\mathrm{AG}_{m-1}(m,q)$ are the complement of each other.
- $\mathcal{C}_p(\mathbb{D}_{(q-1)q^{m-1}}(\mathcal{R}_q(1,m))) = \mathcal{C}_p(\mathrm{AG}_{m-1}(m,q))$.

# The dual code $\mathcal{C}_p(\mathbb{D}_{(q-1)q^{m-1}}(\mathcal{R}_q(1,m)))^\perp$

## Theorem 14

*The dual code* $\mathcal{C}_p(\mathbb{D}_{(q-1)q^{m-1}}(\mathcal{R}_q(1,m)))^\perp$ *has parameters*

$$\left[q^m,\ q^m - \binom{p+m-1}{m}^s,\ d^\perp\right],$$

*where* $q = p^s$, $d^\perp \geq q+2$ *if* $s > 1$ *and* $d^\perp = 2p$ *if* $s = 1$.

## Open problem

Determine $d^\perp$ for $s > 1$.

# The code $\mathcal{C}_3(\mathbb{D}_{3^{m-1}}(\mathcal{R}_3(2,m)))$

**Theorem 15**

*For $m \geq 2$ the two codes $\mathcal{R}_3(2,m)$ and $\mathcal{C}_3(\mathbb{D}_{3^{m-1}}(\mathcal{R}_3(2,m)))$ are identical.*

- This is the special case $q = p = 3$ and $\ell = 2$.
- This may be the first known non-binary code with this property.
- The proof of Theorem 15 is technical and omitted.

# Open problem

Determine the parameters of $\mathcal{C}_p(\mathbb{D}_i(\mathcal{R}_q(\ell, m)))$ for other designs $\mathbb{D}_i(\mathcal{R}_q(\ell, m))$ held in $\mathcal{R}_q(\ell, m)$ for $\ell \geq 2$, and study properties of $\mathcal{C}_p(\mathbb{D}_i(\mathcal{R}_q(\ell, m)))$.

## Remarks

- For $\ell = 2$, we have the answer only for the sub case $q = p = 3$ and $i = 3^{m-1}$. Other subcases are still open, but mat be workable.
- For $3 \leq \ell \leq m - 2$, the problem looks extremely difficult.

# Concluding remarks

# Concluding remarks

- This approach can give very good codes. In addition to the codes presented in this talk, very good codes were also obtained in:
  C. Ding, C. Tang, V. D. Tonchev, Linear codes of 2-designs associated with subcodes of the ternary generalized Reed-Muller codes, *Designs, Codes and Cryptography* 88(4) (2020) 625–641.
- Naturally, this approach may produce bad codes.
- Little work in this direction is done.
- Further work on this topic should be done.