An infinite family of linear codes supporting 4-designs

Chunming Tang, Cunsheng Ding

***Abstract*—The question as to whether there exists an infinite family of near MDS codes holding an infinite family of t-designs for $t \geq 2$ was answered in the recent paper [Infinite families of near MDS codes holding t-designs, IEEE Trans. Inf. Theory 66(9) (2020)], where an infinite family of near MDS codes holding an infinite family of 3-designs and an infinite family of near MDS codes holding an infinite family of 2-designs were presented, but no infinite family of linear codes holding an infinite family of 4-designs was presented. Hence, the question as to whether there is an infinite family of linear codes holding an infinite family of 4-designs remains open for 71 years. This paper settles this long-standing problem by presenting an infinite family of BCH codes of length $2^{2m+1}+1$ over $\mathrm{GF}(2^{2m+1})$ holding an infinite family of 4-$(2^{2m+1}+1, 6, 2^{2m}-4)$ designs. This paper also provides another solution to the first question, as some of the BCH codes presented in this paper are also near MDS. Moreover, an infinite family of linear codes holding the spherical geometry design $S(3, 5, 4^m+1)$ is presented. The new direction of searching for t-designs with elementary symmetric polynomials will be further advanced.**

***Index Terms*—BCH code, cyclic code, linear code, near MDS code, t-design.**

I. Introduction

Let $\mathcal{P}$ be a set of $v \geq 1$ elements, where v is an integer, and let $\mathcal{B}$ be a set of k-subsets of $\mathcal{P}$, where k is a positive integer with $1 \leq k \leq v$. Let t be a positive integer with $t \leq k$. The pair $\mathbb{D} := (\mathcal{P}, \mathcal{B})$ becomes an incidence structure when the incidence relation is the set membership. The incidence structure $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ is called a t-(v, k, λ) *design*, or simply t-*design*, if every t-subset of $\mathcal{P}$ is contained in exactly λ elements of $\mathcal{B}$. The elements of $\mathcal{P}$ are called points, and those of $\mathcal{B}$ are referred to as blocks. The set $\mathcal{B}$ is called the block set. The number of blocks in $\mathcal{B}$ is usually denoted by b. Let $\binom{\mathcal{P}}{k}$ denote the set of all k-subsets of $\mathcal{P}$. Then $\left(\mathcal{P}, \binom{\mathcal{P}}{k}\right)$ is a k-$(v, k, 1)$ design, which is called a *complete design*. A t-design is called *simple* if $\mathcal{B}$ does not contain any repeated blocks. This paper considers only simple t-designs with $v > k > t$. A t-(v, k, λ) design is referred to as a *Steiner system* if $t \geq 2$ and $\lambda = 1$, and is denoted by $S(t, k, v)$. From the definition, it follows that the parameters of a t-(ν, k, λ) design have the following relation:

$$\binom{\nu}{t}\lambda = \binom{k}{t}b.$$

Let C be a $[v, \kappa, d]$ linear code over $\mathrm{GF}(q)$, where κ and d denote the dimension and minimum distance of C. Let A_i denote the number of codewords with Hamming weight i in C for $0 \leq i \leq v$. The sequence $(A_0, A_1, \cdots, A_v)$ of integers is called the *weight distribution* of C, and the polynomial $\sum_{i=0}^{v} A_i z^i$ is referred to as the *weight enumerator* of C. In this paper, $\mathsf{C}^\perp$ denotes the dual code of a linear code C, $d^\perp$ denotes the minimum distance of $\mathsf{C}^\perp$, and $(A_0^\perp, A_1^\perp, \cdots, A_v^\perp)$ denotes the weight distribution of $\mathsf{C}^\perp$.

There are different approaches to constructing t-designs. A coding-theoretic construction of t-designs is as follows. For each k with $A_k \neq 0$, let $\mathcal{B}_k(\mathsf{C})$ denote the set of the supports of all codewords with Hamming weight k in C, where the coordinates of a codeword are indexed by $(p_1, \ldots, p_v)$. Let $\mathcal{P}(\mathsf{C}) = \{p_1, \ldots, p_v\}$. The incidence structure $(\mathcal{P}(\mathsf{C}), \mathcal{B}_k(\mathsf{C}))$ may be a t-(v, k, λ) design for some positive integers t and λ, which is called a *support design* of the code C, and is denoted by $\mathbb{D}_k(\mathsf{C})$. In such a case, we say that the codewords of weight k in C support or hold a t-(v, k, λ) design, and for simplicity, we say that C supports or holds a t-(v, k, λ) design.

There are three sets of sufficient conditions under which the incidence structure $(\mathcal{P}(\mathsf{C}), \mathcal{B}_k(\mathsf{C}))$ is a t-design for some positive integer t. The first set of conditions is described in the Assmus-Mattson Theorem [1]. The second set of conditions is documented in a generalised Assmus-Mattson Theorem [20]. The third set of conditions is in terms of the automorphism group of the code C [12, p. 308].

A number of infinite families of t-designs with $t \in \{2, 3\}$ have been constructed from this coding-theoretic approach [4]. In [6], the authors solved the 70-year-old open problem as to whether there exists an infinite family of near MDS codes supporting an infinite family of t-designs for $t \geq 2$ by presenting an infinite family of near MDS codes over $\mathrm{GF}(3^s)$ supporting an infinite family of 3-designs and an infinite family of near MDS codes over $\mathrm{GF}(2^{2s})$ supporting an infinite family of 2-designs. However, no infinite family of 4-designs has been produced with this coding approach, though sporadic t-designs with $t = 4$ and $t = 5$ have been obtained from some sporadic linear codes. The first linear code supporting t-design with $t \geq 4$ was the $[11, 6, 5]$ ternary Golay code discovered in 1949 by Golay [11]. This ternary code holds 4-designs, and its extended code holds a Steiner system $S(5, 6, 12)$ having the largest strength known. In the past 71 years, some sporadic linear codes holding 4-designs and 5-

C. Tang was supported by The National Natural Science Foundation of China (Grant No. 11871058) and China West Normal University (14E013, CXTD2014-4 and the Meritocracy Research Funds). C. Ding's research was supported by the Hong Kong Research Grants Council, Proj. No. 16300418.

C. Tang is with the School of Mathematics and Information, China West Normal University, Nanchong 637002, China (e-mail: tangchunming-math@163.com).

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (email: cding@ust.hk).

designs were discovered and many infinite families of linear codes supporting 3-designs were constructed. However, the question as to whether there is an infinite family of liner codes holding an infinite family of 4-designs remains open for 71 years, in spite of the recent breakthrough in [6]. The objective of this paper is to settle this 71-year-old problem by presenting an infinite family of near MDS codes over $\mathrm{GF}(2^{2m+1})$ holding an infinite family of 4-$(2^{2m+1}+1, 6, 2^{2m}-4)$ designs. In addition, this paper presents an infinite family of linear codes holding the spherical geometry design $S(3, 5, 1+4^m)$. The new direction of searching for t-designs with elementary symmetric polynomials will be further advanced.

Since a number of infinite families of linear codes supporting an infinite family of 2-designs and 3-designs are known in the literature [4] and the codes presented in [6] support only 2-designs and 3-designs, the breakthrough made in [6] is limited to an open question regarding near MDS codes. The work of this paper is not incremental, as it presents the first and unique infinite family of linear codes supporting an infinite family of 4-designs in the literature. This paper also gives another solution to the problem solved in [6], as the codes presented in this paper are also near MDS. Both [6] and this paper consider BCH codes and near MDS codes and make use of elementary symmetric polynomials.

II. Cyclic codes, BCH codes, AMDS codes and NMDS codes

In this section, we recall cyclic codes, BCH codes, almost MDS codes and near MDS codes, as they will be used later for constructing a family of 4-designs.

A. Cyclic codes and BCH codes

An $[n, k, d]$ code C over $\mathrm{GF}(q)$ is said to be *cyclic* if the condition $(c_0, c_1, \cdots, c_{n-1}) \in \mathsf{C}$ implies $(c_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in \mathsf{C}$. In this paper we identify a vector $(c_0, c_1, \cdots, c_{n-1}) \in \mathrm{GF}(q)^n$ with the polynomial

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \mathrm{GF}(q)[x]/(x^n - 1).$$

In this way, any code C of length n over $\mathrm{GF}(q)$ corresponds to a subset of the quotient ring $\mathrm{GF}(q)[x]/(x^n-1)$. A linear code C is then cyclic if and only if the corresponding subset in $\mathrm{GF}(q)[x]/(x^n-1)$ is an ideal of the ring $\mathrm{GF}(q)[x]/(x^n-1)$.

It is well known that every ideal of $\mathrm{GF}(q)[x]/(x^n-1)$ is principal. Let $\mathsf{C} = \langle g(x) \rangle$ be a cyclic code, where $g(x)$ is monic and has the smallest degree among all the generators of C. Then this $g(x)$ is unique and called the *generator polynomial* of C, and $h(x) = (x^n-1)/g(x)$ is called the *parity-check* polynomial of C.

We are now ready to recall BCH codes over finite fields. Let $\gcd(n, q) = 1$. Let $m := \mathrm{ord}_n(q)$, which is the order of q modulo n, and let α be a generator of the group $\mathrm{GF}(q^m)^*$. Define $\beta = \alpha^{(q^m-1)/n}$. Then β is a primitive n-th root of unity in $\mathrm{GF}(q^m)$. The minimal polynomial $\mathbb{M}_{\beta^s}(x)$ of β^s over $\mathrm{GF}(q)$ is defined to be the monic polynomial of the smallest degree over $\mathrm{GF}(q)$ with β^s as a root. It is easy to verify that this minimal polynomial is given by

$$\mathbb{M}_{\beta^s}(x) = \prod_{i \in C_s} (x - \beta^i) \in \mathrm{GF}(q)[x], \tag{1}$$

which is clearly irreducible over $\mathrm{GF}(q)$.

Let δ be an integer with $2 \le \delta \le n$ and let h be an integer. A *BCH code* over $\mathrm{GF}(q)$ with length n and *designed distance* δ, denoted by $\mathsf{C}_{(q,n,\delta,h)}$, is the cyclic code of length n over $\mathrm{GF}(q)$ with generator polynomial

$$g_{(q,n,\delta,h)} = \mathrm{lcm}(\mathbb{M}_{\beta^h}(x), \mathbb{M}_{\beta^{h+1}}(x), \cdots, \mathbb{M}_{\beta^{h+\delta-2}}(x)), \tag{2}$$

where the least common multiple is computed over $\mathrm{GF}(q)$.

When $h = 1$, the code $\mathsf{C}_{(q,n,\delta,h)}$ with the generator polynomial in (2) is called a *narrow-sense* BCH code. If $n = q^m - 1$, then $\mathsf{C}_{(q,n,\delta,h)}$ is referred to as a *primitive* BCH code.

BCH codes form a subclass of cyclic codes and have nice properties. It is known that BCH codes are asymptotically bad. However, in many cases BCH codes are the best linear codes. For instance, among all binary cyclic codes of odd length at most 125 the best cyclic code is always a BCH code except for two special cases [3, Appendix A]. Some BCH codes are very popular in engineering. As a subclass of BCH codes, Reed-Solomon codes have been widely used in communication devices and consumer electronics. In the past ten years, a lot of progress on the study of BCH codes has been made (see, for example, [16], [17], [18], [19], [25]). In this paper, we will investigate an important application of BCH codes in combinatorial designs.

It is well known that the extended code $\overline{\mathsf{C}_{(q,q^m-1,\delta,1)}}$ of the narrow-sense primitive BCH code $\mathsf{C}_{(q,q^m-1,\delta,1)}$ holds 2-designs, as the permutation automorphism group of the extended code contains the general affine group as a subgroup (see, for example, [7] and [4, Chapter 8]). However, it is very rare that an infinite family of cyclic codes hold an infinite family of 3-designs. In this paper, we will present an infinite family of BCH codes holding an infinite family of 4-designs, which makes a breakthrough in 71 years and shows the beauty of BCH codes in theory.

B. AMDS codes and NMDS codes

An $[n, k, n-k+1]$ linear code is called an MDS code. An $[n, k, n-k]$ linear code is said to be almost maximum distance separable (almost MDS or AMDS for short). A code is said to be near maximum distance separable (near MDS or NMDS for short) if the code and its dual code both are almost maximum distance separable. MDS codes do hold t-designs with very large t. Unfortunately, all t-designs held in MDS codes are complete and thus trivial. The first NMDS code was the $[11, 6, 5]$ ternary Golay code discovered in 1949 by Golay [11]. This ternary code holds 4-designs, and its extended code holds a Steiner system $S(5, 6, 12)$ with the largest strength known. The authors of this paper very recently presented an infinite family of NMDS codes over $\mathrm{GF}(3^m)$ holding an infinite family of 3-designs and an infinite family of NMDS codes over $\mathrm{GF}(2^{2m})$ holding an infinite family of 2-designs [6]. In this paper, we will present a family of NMDS codes over $\mathrm{GF}(2^{2m+1})$ holding an infinite family of 4-designs, and a family of NMDS codes over $\mathrm{GF}(2^{2m})$ holding an infinite family of 3-designs.

NMDS codes have nice properties [8], [9], [10], [23]. In particular, up to a multiple, there is a natural correspondence

between the minimum weight codewords of an NMDS code C and its dual $\mathsf{C}^\perp$, which follows from the next result [10].

Theorem 1. *Let C be an NMDS code. Then for every minimum weight codeword $\mathbf{c}$ in C, there exists, up to a multiple, a unique minimum weight codeword $\mathbf{c}^\perp$ in $\mathsf{C}^\perp$ such that $\mathrm{suppt}(\mathbf{c}) \cap \mathrm{suppt}(\mathbf{c}^\perp) = \emptyset$. In particular, C and $\mathsf{C}^\perp$ have the same number of minimum weight codewords.*

By Theorem 1, if the minimum weight codewords of an NMDS code support a t-design, so do the minimum weight codewords of its dual, and the two t-designs are complementary of each other.

III. Combinatorial t-designs from elementary symmetric polynomials

The objective of this section is to construct 3-designs and 4-designs from elementary symmetric polynomials. These results would play a crucial role in proving that the codes constructed in the next section support 3-designs or 4-designs.

We define $[k] := \{1, 2, \cdots, k\}$. The *elementary symmetric polynomial* (*ESP*) of degree ℓ in k variables $u_1, u_2, \cdots, u_k$, written $\sigma_{k,\ell}$, is defined by

$$\sigma_{k,\ell}(u_1, \cdots, u_k) = \sum_{I \subseteq [k], |I| = \ell} \prod_{j \in I} u_j. \tag{3}$$

In commutative algebra, the elementary symmetric polynomials are a type of basic building blocks for symmetric polynomials, in the sense that any symmetric polynomial can be expressed as a polynomial in elementary symmetric polynomials. Throughout this section, we use $\sigma_{k,\ell}$ to abbreviate $\sigma_{k,\ell}(u_1, \cdots, u_k)$ when $u_1, \ldots, u_k$ are clear from the context.

Let $q = 2^m$ throughout this section. Let U_{q+1} be the subgroup of $\mathrm{GF}(q^2)^*$ of order $q+1$, that is, $U_{q+1} = \{u \in \mathrm{GF}(q^2)^* : u^{q+1} = 1\}$. For any integer k with $1 \le k \le q+1$, let $\binom{U_{q+1}}{k}$ denote the set of all k-subsets of U_{q+1}. Define

$$\mathcal{B}_{\sigma_{k,\ell},q+1} = \left\{ \{u_1, \cdots, u_k\} \in \binom{U_{q+1}}{k} : \sigma_{k,\ell}(u_1, \cdots, u_k) = 0 \right\}. \tag{4}$$

The incidence structure $\mathbb{D}_{\sigma_{k,\ell},q+1} = (U_{q+1}, \mathcal{B}_{\sigma_{k,\ell},q+1})$ may be a t-$(q+1, k, \lambda)$ design for some λ, where U_{q+1} is the point set, and the incidence relation is the set membership. In this case, we say that the ESP $\sigma_{k,\ell}$ supports a t-$(q+1, k, \lambda)$ design. The ESP $\sigma_{k,\ell}$ always supports a 1-design, but may not support 2-designs. Define the block sets $\mathcal{B}^0_{\sigma_{6,3},q+1}$ and $\mathcal{B}^1_{\sigma_{6,3},q+1}$ by

$$\mathcal{B}^0_{\sigma_{6,3},q+1} = \left\{ \begin{array}{c} \{u_1, u_2, u_3, u_4, u_5, u_6\} \in \mathcal{B}_{\sigma_{6,3},q+1} : \\ \{u_{i_1}, u_{i_2}, u_{i_3}, u_{i_4}, u_{i_5}\} \in \mathcal{B}_{\sigma_{5,2},q+1} \\ \text{for some } \{i_1, i_2, \cdots, i_5\} \text{ with} \\ 1 \le i_1 < i_2 < i_3 < i_4 < i_5 \le 6 \end{array} \right\}, \tag{5}$$

and

$$\mathcal{B}^1_{\sigma_{6,3},q+1} = \mathcal{B}_{\sigma_{6,3},q+1} \setminus \mathcal{B}^0_{\sigma_{6,3},q+1}. \tag{6}$$

The following three theorems and corollary are the main results of this section. They show an interesting application of ESPs in the theory of combinatorial designs.

Theorem 2. *Let $m \ge 5$ be odd. Then the incidence structure $(U_{q+1}, \mathcal{B}_{\sigma_{6,3},q+1})$ is a 4-$\left(q+1, 6, \frac{q-8}{2}\right)$ design, where the block set $\mathcal{B}_{\sigma_{6,3},q+1}$ is given by (4).*

Theorem 3. *Let $m \ge 4$ be even. Then the incidence structure $(U_{q+1}, \mathcal{B}_{\sigma_{5,2},q+1})$ is a Steiner system $S(3, 5, q+1)$, where the block set $\mathcal{B}_{\sigma_{5,2},q+1}$ is given by (4).*

Theorem 4. *Let $m \ge 4$ be even. Then the incidence structure $(U_{q+1}, \mathcal{B}^0_{\sigma_{6,3},q+1})$ is a 3-$(q+1, 6, 2(q-4))$ design, and the incidence structure $(U_{q+1}, \mathcal{B}_{\sigma_{6,3},q+1})$ is a 3-$\left(q+1, 6, \frac{(q-4)^2}{6}\right)$ design.*

The following corollary follows immediately from the previous theorem.

Corollary 5. *Let $m \ge 4$ be even. Then the incidence structure $(U_{q+1}, \mathcal{B}^1_{\sigma_{6,3},q+1})$ is a 3-$\left(q+1, 6, \frac{(q-4)(q-16)}{6}\right)$ design.*

From Theorems 2, 3 and 4, one gets

$$\left|\mathcal{B}_{\sigma_{5,2},q+1}\right| = \begin{cases} \frac{1}{10}\binom{q+1}{3}, & \text{if } m \text{ is even,} \\ 0, & \text{if } m \text{ is odd,} \end{cases}$$

and

$$\left|\mathcal{B}_{\sigma_{6,3},q+1}\right| = \begin{cases} \frac{(q-4)^2}{120}\binom{q+1}{3}, & \text{if } m \text{ is even,} \\ \frac{q-8}{30}\binom{q+1}{4}, & \text{if } m \text{ is odd.} \end{cases}$$

In general, it is difficult to determine $\left|\mathcal{B}_{\sigma_{k,\ell},q+1}\right|$. It would be interesting to settle the following problem.

Open Problem 6. *Let k, ℓ be two positive integers with $\ell \le \frac{k}{2}$. Determine the cardinality of the block set $\mathcal{B}_{\sigma_{k,\ell},q+1}$ given by (4) for $(k, \ell) \ne (6, 3)$ and $(5, 2)$.*

To prove Theorems 2, 3, and 4, we need the following lemmas. The first one is on quadratic equations over finite fields of characteristic 2 [15], and is documented below.

Lemma 7. *Let $f(T) = T^2 + aT + b \in \mathrm{GF}(q)[T]$ be a polynomial of degree 2. Then*

1) *f has exactly one root in $\mathrm{GF}(q)$ if and only if $a = 0$;*
2) *f has exactly two roots in $\mathrm{GF}(q)$ if and only if $a \ne 0$ and $\mathrm{Tr}_{q/2}\left(\frac{b}{a^2}\right) = 0$; and*
3) *f has exactly two roots in $\mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$ if and only if $a \ne 0$ and $\mathrm{Tr}_{q/2}\left(\frac{b}{a^2}\right) = 1$.*

Lemma 8. *Let $\{u_1, u_2\} \in \binom{U_{q+1}}{2}$. Then $\frac{u_1 u_2}{u_1^2 + u_2^2} \in \mathrm{GF}(q)$ and $\mathrm{Tr}_{q/2}\left(\frac{u_1 u_2}{u_1^2 + u_2^2}\right) = 1$.*

Proof. Let $a = \frac{u_1 u_2}{u_1^2 + u_2^2}$. Then $a^q = \frac{u_1^{-1} u_2^{-1}}{u_1^{-2} + u_2^{-2}} = a$. Thus $a \in \mathrm{GF}(q)$. Note that $\frac{1}{a} = u + \frac{1}{u}$, where $u = \frac{u_1}{u_2} \in U_{q+1}$. One has

$$(au)^2 + (au) + a^2 = 0, \tag{7}$$

where $au \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$. Hence, the equation $T^2 + T + a^2 = 0$ has two roots in $\mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$. It then follows from Lemma 7 that $\mathrm{Tr}_{q/2}(a) = \mathrm{Tr}_{q/2}(a^2) = 1$. This completes the proof. □

Lemma 9. *Let $\{u_1, u_2, u_3, u_4\} \in \binom{U_{q+1}}{4}$. Then we have the following.*

1) *$u_1 + u_2 + u_3 + u_4 \ne 0$.*

2) *If m is even, then $u_1+u_2+u_3\neq 0$.*

Proof. Suppose that $u_1+u_2+u_3+u_4=0$. We have then

$$\frac{1}{u_1}+\frac{1}{u_2}+\frac{1}{u_3}+\frac{1}{u_4}=(u_1+u_2+u_3+u_4)^q=0.$$

It follows from $u_4=u_1+u_2+u_3$ that

$$\frac{1}{u_1}+\frac{1}{u_2}+\frac{1}{u_3}+\frac{1}{u_1+u_2+u_3}=0.$$

Multiplying both sides of the previous equation by $u_1u_2u_3(u_1+u_2+u_3)$ yields

$$(u_1+u_2+u_3)(u_1u_2+u_2u_3+u_3u_1)+u_1u_2u_3=0,$$

which is the same as

$$(u_1+u_2)(u_2+u_3)(u_3+u_1)=0,$$

which is contrary to our assumption that u_1,u_2,u_3 are pairwise distinct. Thus, $u_1+u_2+u_3+u_4\neq 0$.

Let m be even. Suppose that $u_1+u_2+u_3=0$. Then $\frac{1}{u_1+u_2}=\frac{1}{u_3}=\frac{1}{u_1}+\frac{1}{u_2}=\frac{u_1+u_2}{u_1u_2}$. We then have $u_1^2+u_1u_2+u_2^2=0$. Thus, $u_1^3=u_2^3$. Since m is even , $\gcd(3,q+1)=1$. It then follows from $u_1^3=u_2^3$ that $u_1=u_2$, which is contrary to our assumption that $u_1\neq u_2$. This completes the proof. □

Lemma 10. *Let $\sigma_{3,1},\sigma_{3,2},\sigma_{3,3}$ be the ESPs given by (3) with $\{u_1,u_2,u_3\}\in\binom{U_{q+1}}{3}$. Then*

1) $\sigma_{3,1}\sigma_{3,2}+\sigma_{3,3}=(u_1+u_2)(u_2+u_3)(u_3+u_1)$.
2) $\sigma_{3,1}\sigma_{3,2}+\sigma_{3,3}\neq 0$.
3) $\sigma_{3,2}^2+\sigma_{3,1}\sigma_{3,3}=\sigma_{3,3}^2\left(\sigma_{3,1}^2+\sigma_{3,2}\right)^q$.

Proof. The proofs are straightforward and omitted. □

Lemma 11. *Let m be even. Let $\sigma_{3,1},\sigma_{3,2},\sigma_{3,3}$ be the ESPs given by (3) with $\{u_1,u_2,u_3\}\in\binom{U_{q+1}}{3}$. Then*

1) $\sigma_{3,1}^2+\sigma_{3,2}\neq 0$*; and*
2) $\sigma_{3,2}^2+\sigma_{3,1}\sigma_{3,3}\neq 0$.

Proof. Suppose that $\sigma_{3,1}^2+\sigma_{3,2}=0$, that is

$$u_1^2+u_2^2+u_3^2+u_1u_2+u_2u_3+u_3u_1=0.$$

Multiplying both sides of the previous equation by $u_1+u_2+u_3$ yields

$$u_1^3+u_2^3+u_3^3+u_1u_2u_3=0.$$

It then follows that $|\{u_1^3,u_2^3,u_3^3,u_1u_2u_3\}|=3$ from Lemma 9, which is contrary to the assumption that m is even. Combining Part 1 and Lemma 10 gives Part 2. This completes the proof. □

Lemma 12. *Let $u_j\in U_{q+1}$ such that $\sigma_{5,2}=0$, where $j\in\{1,2,3,4,5\}$. Then*

$$\begin{cases}(\sigma_{3,1}^2+\sigma_{3,2})(u_4+u_5) &= \sigma_{3,1}\sigma_{3,2}+\sigma_{3,3},\\ (\sigma_{3,1}^2+\sigma_{3,2})u_4u_5 &= \sigma_{3,2}^2+\sigma_{3,1}\sigma_{3,3},\end{cases}$$

where $\sigma_{3,1},\sigma_{3,2},\sigma_{3,3}$ and $\sigma_{5,2}$ are the ESPs given by (3).

Proof. Observe first that

$$u_4u_5+\sigma_{3,1}(u_4+u_5)+\sigma_{3,2}=0. \tag{8}$$

Raising to the q-th power both sides of Equation (8) yields

$$u_4^{-1}u_5^{-1}+\sigma_{3,1}^q(u_4^{-1}+u_5^{-1})+\sigma_{3,2}^q=0,$$

which is the same as

$$\sigma_{3,1}u_4u_5+\sigma_{3,2}(u_4+u_5)+\sigma_{3,3}=0. \tag{9}$$

The desired conclusion then follows from Equations (8) and (9). This completes the proof. □

Lemma 13. *Let m be even and $\{u_1,u_2,u_3,u_4,u_5,u_6\}\in\mathcal{B}^0_{\sigma_{6,3},q+1}$. Let A and A' be two 5-subsets of $\{u_1,u_2,u_3,u_4,u_5,u_6\}$ such that $A,A'\in\mathcal{B}_{\sigma_{5,2},q+1}$. Then $A=A'$.*

Proof. Suppose that $A\neq A'$. Due to symmetry, let $A=\{u_1,u_2,u_3,u_4,u_5\}\in\mathcal{B}_{\sigma_{5,2},q+1}$ and $A'=\{u_1,u_2,u_3,u_4,u_6\}\in\mathcal{B}_{\sigma_{5,2},q+1}$. It then follows from Lemma 12 that

$$(\sigma_{3,1}^2+\sigma_{3,2})(u_4+u_5)=\sigma_{3,1}\sigma_{3,2}+\sigma_{3,3}=(\sigma_{3,1}^2+\sigma_{3,2})(u_4+u_6),$$

which gives

$$(\sigma_{3,1}^2+\sigma_{3,2})(u_5+u_6)=0.$$

It then follows from Lemma 11 that $u_5+u_6=0$, which is contrary to the assumption that $u_5\neq u_6$. □

The following result is an immediate consequence of Lemmas 10, 11 and 12.

Lemma 14. *Let $\{u_1,u_2,u_3\}\in\binom{U_{q+1}}{3}$ and $u_4,u_5\in U_{q+1}$ such that $\sigma_{5,2}=0$. Then none of $\sigma_{3,1}^2+\sigma_{3,2},\sigma_{3,1}\sigma_{3,2}+\sigma_{3,3}$ and $\sigma_{3,2}^2+\sigma_{3,1}\sigma_{3,3}$ equals zero, and $u_4\neq u_5$.*

Lemma 15. *Let $\{u_1,u_2,u_3\}\in\binom{U_{q+1}}{3}$ such that $(\sigma_{3,1}^2+\sigma_{3,2})(\sigma_{3,1}\sigma_{3,2}+\sigma_{3,3})(\sigma_{3,2}^2+\sigma_{3,1}\sigma_{3,3})\neq 0$. Put $a=\frac{\sigma_{3,1}\sigma_{3,2}+\sigma_{3,3}}{\sigma_{3,1}^2+\sigma_{3,2}}$ and $b=\frac{\sigma_{3,2}^2+\sigma_{3,1}\sigma_{3,3}}{\sigma_{3,1}^2+\sigma_{3,2}}$. Then $b\in U_{q+1}$, $\frac{b}{a^2}\in\mathrm{GF}(q)$ and $\mathrm{Tr}_{q/2}\left(\frac{b}{a^2}\right)\equiv 1+m\pmod 2$.*

Proof. First, it follows from Part 3 of Lemma 10 that $b\in U_{q+1}$. Next, observe that

$$\frac{b}{a^2}=\frac{u_1u_2}{(u_1+u_2)^2}+\frac{u_2u_3}{(u_2+u_3)^2}+\frac{u_3u_1}{(u_3+u_1)^2}+1. \tag{10}$$

The desired conclusion then follows from Lemma 8 and Equation (10). This completes the proof. □

Lemma 16. *Let the notation and assumption be the same as in Lemma 15. Let $f(u)$ be the quadratic polynomial $u^2+au+b\in\mathrm{GF}(q)[u]$. Then we have the following.*

1) *If m is odd, then f has no root in $U_{q+1}\setminus\left\{\sqrt{b}\right\}$.*
2) *If m is even, then f has exactly two roots in U_{q+1}.*

Proof. Let m be odd. Suppose that there exists an $u\in U_{q+1}\setminus\left\{\sqrt{b}\right\}$ such that $f(u)=0$. Then

$$\left(\frac{u}{\sqrt{b}}\right)^2+\frac{a}{\sqrt{b}}\left(\frac{u}{\sqrt{b}}\right)+1=0.$$

From Lemma 7 and $\frac{u}{\sqrt{b}}\in U_{q+1}\setminus\{1\}\subseteq\mathrm{GF}(q^2)\setminus\mathrm{GF}(q)$, we have that $\mathrm{Tr}_{q/2}\left(\frac{b}{a^2}\right)=1$, which is contrary to the result of Lemma 15.

Let m be even. By Lemmas 7 and 15, there exists $u' \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$ such that u', u'^q are exactly the two solutions of the quadratic equation $T^2+\frac{a}{\sqrt{b}}T+1=0$. It's easily checked that $u_4 = \sqrt{b}u'$ and $u_5 = \sqrt{b}u'^q$ are the two roots of f. Then the result follows from $u'^{q+1} = 1$. This completes the proof. □

Combining Lemmas 14, 12, and 16 gives the following.

Lemma 17. *Let m be odd and $\{u_1, u_2, u_3, u_4, u_5\} \in \binom{U_{q+1}}{5}$. Then $\sigma_{5,2} \neq 0$.*

Lemma 18. *Let m be even and $\{u_1, u_2, u_3\} \in \binom{U_{q+1}}{3}$. Let u_4, u_5 be the two solutions of the quadratic equation $u^2 + au + b = 0$, where $a = \frac{\sigma_{3,1}\sigma_{3,2}+\sigma_{3,3}}{\sigma_{3,1}^2+\sigma_{3,2}}$ and $b = \frac{\sigma_{3,2}^2+\sigma_{3,1}\sigma_{3,3}}{\sigma_{3,1}^2+\sigma_{3,2}}$. Then*

$$\{u_1, u_2, u_3, u_4, u_5\} \in \mathcal{B}_{\sigma_{5,2},q+1}.$$

Proof. First, employing Lemmas 10, 11, and 16, we have that $u_4, u_5 \in U_{q+1}$ and $u_4 \neq u_5$. Using $\sigma_{5,2} = u_4u_5 + (u_4 + u_5)\sigma_{3,1} + \sigma_{3,2}$ and Vieta's formulas yields

$$\sigma_{5,2} = \frac{\sigma_{3,2}^2 + \sigma_{3,1}\sigma_{3,3}}{\sigma_{3,1}^2 + \sigma_{3,2}} + \frac{\sigma_{3,1}\sigma_{3,2} + \sigma_{3,3}}{\sigma_{3,1}^2 + \sigma_{3,2}}\sigma_{3,1} + \sigma_{3,2} = 0.$$

Suppose that $u_4 = u_i$ and $u_5 = u_j$ for some $i, j \in \{1, 2, 3\}$. By symmetry, let $(i, j) = (3, 2)$. Then

$$\sigma_{5,2} = u_3u_4 + u_2u_5 = u_2^2 + u_3^2 = 0,$$

which is contrary to the condition $u_2 \neq u_3$. Thus, $|\{u_1, u_2, u_3\} \cap \{u_4, u_5\}| \neq 2$.

Suppose that $|\{u_1, u_2, u_3\} \cap \{u_4, u_5\}| = 1$. By the symmetry of u_1, u_2, u_3, let $u_5 = u_3$ and $u_4 \notin \{u_1, u_2, u_3\}$. Then $\sigma_{5,2}(u_1, u_2, u_4, u_5, u_3) = 0$. Note that $\{u_1, u_2, u_4\} \in \binom{U_{q+1}}{3}$ and $u_5 = u_3$, which is contrary to Lemma 14. Thus, $|\{u_1, u_2, u_3\} \cap \{u_4, u_5\}| \neq 1$. Hence, $\{u_1, u_2, u_3, u_4, u_5\} \in \binom{U_{q+1}}{5}$. This completes the proof. □

Lemma 19. *Let $\{u_1, u_2, u_3, u_4\} \in \binom{U_{q+1}}{4}$. Then $\sigma_{4,3}\sigma_{4,1} \neq 0$ and $(\sigma_{4,3} + u_i\sigma_{4,2})(\sigma_{4,2} + u_i\sigma_{4,1}) \neq 0$, where $i \in \{1, 2, 3, 4\}$.*

Proof. Note that

$$\sigma_{4,3}\sigma_{4,1} = \sigma_{4,4}\sigma_{4,1}^{q+1}.$$

By Part 1 of Lemma 9, we have $\sigma_{4,3}\sigma_{4,1} \neq 0$.

Note that $(\sigma_{4,3} + u_i\sigma_{4,2})(\sigma_{4,2} + u_i\sigma_{4,1}) = u_i\sigma_{4,4}(\sigma_{4,2} + u_i\sigma_{4,1})^{q+1}$. We only need to prove that $\sigma_{4,2} + u_i\sigma_{4,1} \neq 0$. On the contrary, suppose that $\sigma_{4,2} + u_i\sigma_{4,1} = 0$. Using the symmetry of u_1, u_2, u_3, u_4, choose $u_i = u_4$. Then $\sigma_{3,2} + u_4^2 = u_1u_2 + u_2u_3 + u_3u_1 + u_4^2 = 0$, which is contrary to Part 1 of Lemma 9 if $u_4^2 \notin \{u_1u_2, u_2u_3, u_3u_1\}$. If $u_4^2 \in \{u_1u_2, u_2u_3, u_3u_1\}$, due to symmetry suppose that $u_4^2 = u_1u_2$. It then follows from $u_1u_2 + u_2u_3 + u_3u_1 + u_4^2 = 0$ that $u_1 = u_2$, which contradicts the assumption that $u_1 \neq u_2$. This completes the proof. □

The following result is a direct consequence of Lemma 19.

Lemma 20. *Let $\{u_1, u_2, u_3, u_4\} \in \binom{U_{q+1}}{4}$. Then $\sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}, \frac{\sigma_{4,3}+u_i\sigma_{4,2}}{\sigma_{4,2}+u_i\sigma_{4,1}} \in U_{q+1}$, where $i \in \{1, 2, 3, 4\}$.*

Lemma 21. *Let $\{u_1, u_2, u_3, u_4\} \in \binom{U_{q+1}}{4}$. Then $\sigma_{6,3}\left(u_1, u_2, u_3, u_4, \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}, \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}\right) = 0$ and*

$$\sigma_{6,3}\left(u_1, u_2, u_3, u_4, \frac{\sigma_{4,3} + u_i\sigma_{4,2}}{\sigma_{4,2} + u_i\sigma_{4,1}}, u_i\right) = 0,$$

where $i \in \{1, 2, 3, 4\}$.

Proof. Set $u_5 = u_6 = \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}$. Then

$$\begin{aligned}
&\sigma_{6,3}(u_1, u_2, u_3, u_4, u_5, u_6)\\
&= \sigma_{4,3} + (u_5 + u_6)\sigma_{4,2} + u_5u_6\sigma_{4,1}\\
&= \sigma_{4,3} + u_5^2\sigma_{4,1}\\
&= 0.
\end{aligned}$$

Thus, $\sigma_{6,3}\left(u_1, u_2, u_3, u_4, \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}, \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}\right) = 0$.

Choose $\sigma_5 = \frac{\sigma_{4,3}+u_i\sigma_{4,2}}{\sigma_{4,2}+u_i\sigma_{4,1}}$ and $\sigma_6 = u_i$. Then

$$\begin{aligned}
&\sigma_{6,3}\\
&= \sigma_{4,3} + (u_5 + u_6)\sigma_{4,2} + u_5u_6\sigma_{4,1}\\
&= \sigma_{4,3} + \left(\frac{\sigma_{4,3} + u_i\sigma_{4,2}}{\sigma_{4,2} + u_i\sigma_{4,1}} + u_i\right)\sigma_{4,2} + \frac{\sigma_{4,3} + u_i\sigma_{4,2}}{\sigma_{4,2} + u_i\sigma_{4,1}}u_i\sigma_{4,1}\\
&= 0.
\end{aligned}$$

This completes the proof. □

Lemma 22. *Let $\{u_1, u_2, u_3, u_4\} \in \binom{U_{q+1}}{4}$ such that $\sigma_{5,2}(u_1, u_2, u_3, u_4, u_5) \neq 0$ for any $u_5 \in U_{q+1} \setminus \{u_1, u_2, u_3, u_4\}$. Let S be the subset of U_{q+1} given by*

$$\left\{\frac{\sigma_{4,3} + u_i\sigma_{4,2}}{\sigma_{4,2} + u_i\sigma_{4,1}} : i = 1, 2, 3, 4\right\} \bigcup \{u_i : i = 1, 2, 3, 4\} \bigcup \left\{\sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}\right\}.$$

Then $|S| = 9$.

Proof. First, we prove that $\sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}} \neq u_4$. On the contrary, suppose that $\sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}} = u_4$. Then

$$\sigma_{4,1}u_4^2 + \sigma_{4,3} = 0,$$

which is the same as

$$u_4^3 + \sigma_{3,1}u_4^2 + \sigma_{3,2}u_4 + \sigma_{3,3} = 0.$$

Then,

$$(u_4 + u_1)(u_4 + u_2)(u_4 + u_3) = 0,$$

which is contrary to the assumption that $\{u_1, u_2, u_3, u_4\} \in \binom{U_{q+1}}{4}$. Thus $\sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}} \neq u_4$. By the symmetry of u_1, u_2, u_3, u_4,

$$\sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}} \neq u_i \text{ for all } i. \tag{11}$$

Suppose that $\frac{\sigma_{4,3}+u_4\sigma_{4,2}}{\sigma_{4,2}+u_4\sigma_{4,1}} = u_4$. Then $u_4 = \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}$, which is contrary to Inequality (11). Thus, $\frac{\sigma_{4,3}+u_4\sigma_{4,2}}{\sigma_{4,2}+u_4\sigma_{4,1}} \neq u_4$. By the symmetry of u_1, u_2, u_3, u_4,

$$\frac{\sigma_{4,3} + u_i\sigma_{4,2}}{\sigma_{4,2} + u_i\sigma_{4,1}} \neq u_i \text{ for all } i. \tag{12}$$

Suppose that $\frac{\sigma_{4,3}+u_4\sigma_{4,2}}{\sigma_{4,2}+u_4\sigma_{4,1}} = u_3$. Then $\sigma_{4,3} + u_4\sigma_{4,2} + u_3(\sigma_{4,2} + u_4\sigma_{4,1}) = 0$, which is the same as $(u_3 + u_4)^2(u_1 + u_2) = 0$. This is contrary to our assumption that $\{u_1, u_2, u_3, u_4\} \in \binom{U_{q+1}}{4}$. Thus, $\frac{\sigma_{4,3}+u_4\sigma_{4,2}}{\sigma_{4,2}+u_4\sigma_{4,1}} \neq u_3$. By the symmetry of u_1, u_2, u_3, u_4,

$$\frac{\sigma_{4,3} + u_i\sigma_{4,2}}{\sigma_{4,2} + u_i\sigma_{4,1}} \neq u_j \text{ for all } i \neq j. \tag{13}$$

Suppose that $\frac{\sigma_{4,3}+u_i\sigma_{4,2}}{\sigma_{4,2}+u_i\sigma_{4,1}} = \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}$ for some $i \in \{1, 2, 3, 4\}$. Put $u_5 = \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}$. It follows from Inequality (11) that $u_5 \notin \{u_1, u_2, u_3, u_4\}$. By Lemma 21, we have

$$\begin{cases} \sigma_{6,3}(u_1, u_2, u_3, u_4, u_5, u_i) & = 0, \\ \sigma_{6,3}\left(u_1, u_2, u_3, u_4, u_5, \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}\right) & = 0. \end{cases}$$

By the assumption of this lemma, $\sigma_{5,2}(u_1, u_2, u_3, u_4, u_5) \neq 0$. Thus,

$$\begin{cases} u_i & = \frac{\sigma_{5,3}}{\sigma_{5,2}}, \\ \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}} & = \frac{\sigma_{5,3}}{\sigma_{5,2}}, \end{cases}$$

which is contrary to Inequality (11). Hence,

$$\frac{\sigma_{4,3} + u_i\sigma_{4,2}}{\sigma_{4,2} + u_i\sigma_{4,1}} \neq \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}. \tag{14}$$

Assume that $\frac{\sigma_{4,3}+u_i\sigma_{4,2}}{\sigma_{4,2}+u_i\sigma_{4,1}} = \frac{\sigma_{4,3}+u_j\sigma_{4,2}}{\sigma_{4,2}+u_j\sigma_{4,1}}$ for some $i, j \in \{1, 2, 3, 4\}$. Put $u_5 = \frac{\sigma_{4,3}+u_i\sigma_{4,2}}{\sigma_{4,2}+u_i\sigma_{4,1}}$. It follows from Inequalities (12) and (13) that $u_5 \notin \{u_1, u_2, u_3, u_4\}$. By Lemma 21, we have

$$\begin{cases} \sigma_{6,3}(u_1, u_2, u_3, u_4, u_5, u_i) & = 0, \\ \sigma_{6,3}(u_1, u_2, u_3, u_4, u_5, u_j) & = 0. \end{cases}$$

By the assumption of this lemma, $\sigma_{5,2}(u_1, u_2, u_3, u_4, u_5) \neq 0$. Thus,

$$\begin{cases} u_i & = \frac{\sigma_{5,3}}{\sigma_{5,2}}, \\ u_j & = \frac{\sigma_{5,3}}{\sigma_{5,2}}. \end{cases}$$

Then $i = j$. Hence,

$$\frac{\sigma_{4,3} + u_i\sigma_{4,2}}{\sigma_{4,2} + u_i\sigma_{4,1}} \neq \frac{\sigma_{4,3} + u_j\sigma_{4,2}}{\sigma_{4,2} + u_j\sigma_{4,1}}, \text{ for } i \neq j. \tag{15}$$

The desired conclusion then follows from Inequalities (11), (12), (13), (14) and (15). This completes the proof. □

Lemma 23. *Let m be even, and let $\{u'_1, u'_2, u'_3, u'_4, u'_5\} \in \mathcal{B}_{\sigma_{5,2},q+1}$ and $u_5, u_6 \in U_{q+1}$ such that $\sigma_{6,3}(u'_1, u'_2, u'_3, u'_4, u_5, u_6) = 0$. Then $u'_5 \in \{u_5, u_6\}$.*

Proof. Suppose that $u'_5 \notin \{u_5, u_6\}$. By Lemmas 11 and 12, $\sigma_{5,2}(u'_1, u'_2, u'_3, u'_4, u_5) \neq 0$. One has

$$\begin{cases} \sigma_{6,3}(u'_1, u'_2, u'_3, u'_4, u_5, u'_5) & = 0, \\ \sigma_{6,3}(u'_1, u'_2, u'_3, u'_4, u_5, u_6) & = 0, \end{cases}$$

which is the same as

$$\begin{cases} u'_5 & = \frac{\sigma_{5,3}(u'_1,u'_2,u'_3,u'_4,u_5)}{\sigma_{5,2}(u'_1,u'_2,u'_3,u'_4,u_5)}, \\ u_6 & = \frac{\sigma_{5,3}(u_1,u_2,u_3,u_4,u_5)}{\sigma_{5,2}(u'_1,u'_2,u'_3,u'_4,u_5)}. \end{cases}$$

This is contrary to our assumption that $u'_5 \notin \{u_5, u_6\}$. This completes the proof. □

Lemma 24. *Let $\{u_1, u_2, u_3, u_4\} \in \binom{U_{q+1}}{4}$ such that $\sigma_{5,2}(u_1, u_2, u_3, u_4, u_5) \neq 0$ for any $u_5 \in U_{q+1} \setminus \{u_1, u_2, u_3, u_4\}$. Then*

$$\frac{\sigma_{5,3}\left(u_1, u_2, u_3, u_4, \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}\right)}{\sigma_{5,2}\left(u_1, u_2, u_3, u_4, \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}\right)} = \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}},$$

and

$$\frac{\sigma_{5,3}\left(u_1, u_2, u_3, u_4, \frac{\sigma_{4,3}+u_i\sigma_{4,2}}{\sigma_{4,2}+u_i\sigma_{4,1}}\right)}{\sigma_{5,2}\left(u_1, u_2, u_3, u_4, \frac{\sigma_{4,3}+u_i\sigma_{4,2}}{\sigma_{4,2}+u_i\sigma_{4,1}}\right)} = u_i,$$

where $i \in \{1, 2, 3, 4\}$.

Proof. The claim follows from Lemma 21. □

We will need the following lemma whose proof is straightforward.

Lemma 25. *Let $\{u_1, u_2, u_3, u_4\} \in \binom{U_{q+1}}{4}$ and $u_5 \in U_{q+1}$ such that $\sigma_{5,2}(u_1, u_2, u_3, u_4, u_5) \neq 0$. Let $u_6 = \frac{\sigma_{5,3}(u_1,u_2,u_3,u_4,u_5)}{\sigma_{5,2}(u_1,u_2,u_3,u_4,u_5)}$. Then we have the following.*

1) *If $u_6 = u_5$, then $u_5 = \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}$.*
2) *If $u_6 = u_i$, then $u_5 = \frac{\sigma_{4,3}+u_i\sigma_{4,2}}{\sigma_{4,2}+u_i\sigma_{4,1}}$, where $i \in \{1, 2, 3, 4\}$.*

Lemma 26. *Let m be even and $\{u_1, u_2, u_3, u_4\} \in \binom{U_{q+1}}{4}$ such that $\sigma_{5,2}(u_1, u_2, u_3, u_4, u_5) \neq 0$ for any $u_5 \in U_{q+1} \setminus \{u_1, u_2, u_3, u_4\}$. Let S be the subset of U_{q+1} given by*

$$\left\{\frac{\sigma_{4,3} + u_i\sigma_{4,2}}{\sigma_{4,2} + u_i\sigma_{4,1}} : i = 1, 2, 3, 4\right\} \bigcup \{u_i : i = 1, 2, 3, 4\} \bigcup \left\{\sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}\right\}.$$

Let $\tilde{u}_4$ and $\tilde{u}_5$ be the two solutions of the quadratic equation $u^2+au+b = 0$, where $a = \frac{\sigma_{3,1}\sigma_{3,2}+\sigma_{3,3}}{\sigma_{3,1}^2+\sigma_{3,2}}$ and $b = \frac{\sigma_{3,2}^2+\sigma_{3,1}\sigma_{3,3}}{\sigma_{3,1}^2+\sigma_{3,2}}$. Then $\tilde{u}_4 \notin S$ and $\tilde{u}_5 \notin S$.

Proof. By the definition of $\tilde{u}_4, \tilde{u}_5$ and Lemma 12, $u_4 \notin \{\tilde{u}_4, \tilde{u}_5\}$. Suppose that $\tilde{u}_4 = \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}$. From Lemma 21 or 24, one gets

$$\sigma_{6,3}\left(u_1, u_2, u_3, u_4, \tilde{u}_4, \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}\right) = 0.$$

From Lemma 23 and $\tilde{u}_5 \neq u_4$, it follows that $\tilde{u}_5 = \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}} = \tilde{u}_4$, which is contrary to $a \neq 0$. Thus, $\tilde{u}_4 \neq \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}$. By the symmetry of $\tilde{u}_4$ and $\tilde{u}_5$, $\tilde{u}_5 \neq \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}}$.

Suppose that $\tilde{u}_4 = \frac{\sigma_{4,3}+u_i\sigma_{4,2}}{\sigma_{4,2}+u_i\sigma_{4,1}}$. From Lemma 21 or 24, one gets

$$\sigma_{6,3}(u_1, u_2, u_3, u_4, u_i, \tilde{u}_4) = 0.$$

From Lemma 23 and $\tilde{u}_5 \neq u_4$, it follows that $\tilde{u}_5 = u_i$, which is contrary to the definition of $\tilde{u}_5$. Thus, $\tilde{u}_4 \neq \frac{\sigma_{4,3}+u_i\sigma_{4,2}}{\sigma_{4,2}+u_i\sigma_{4,1}}$. By the symmetry of $\tilde{u}_4$ and $\tilde{u}_5$, $\tilde{u}_5 \neq \frac{\sigma_{4,3}+u_i\sigma_{4,2}}{\sigma_{4,2}+u_i\sigma_{4,1}}$. This completes the proof. □

Proof of Theorem 2. Recall Theorem 2 first. Let $\{u_1, u_2, u_3, u_4\}$ be a fixed 4-subset of U_{q+1}. Set

$$S = \left\{ \frac{\sigma_{4,3} + u_i\sigma_{4,2}}{\sigma_{4,2} + u_i\sigma_{4,1}} : i = 1, 2, 3, 4 \right\} \bigcup \{u_i : i = 1, 2, 3, 4\} \bigcup \left\{ \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}} \right\}.$$

For any $u_5 \notin \{u_i : i = 1, 2, 3, 4\}$, $\sigma_{5,2}(u_1, u_2, u_3, u_4, u_5) \neq 0$ from Lemma 17. Define

$$\mathcal{T} = \left\{ \left\{ u_5, \frac{\sigma_{5,3}(u_1, u_2, u_3, u_4, u_5)}{\sigma_{5,2}(u_1, u_2, u_3, u_4, u_5)} \right\} : u_5 \in U_{q+1} \setminus S \right\}.$$

From Lemmas 24 and 25, it follows that $\frac{\sigma_{5,3}(u_1,u_2,u_3,u_4,u_5)}{\sigma_{5,2}(u_1,u_2,u_3,u_4,u_5)} \notin S$ if $u_5 \notin S$. By Lemma 22, $|\mathcal{T}| = \frac{(q+1-9)}{2}$. From Lemma 25 and $\frac{\sigma_{5,3}(u_1,u_2,u_3,u_4,u_5)}{\sigma_{5,2}(u_1,u_2,u_3,u_4,u_5)} \in U_{q+1}$, we deduce that $\{u_1, u_2, u_3, u_4, u_5, u_6\} \in \mathcal{B}_{\sigma_{6,3},q+1}$ for any $\{u_5, u_6\} \in \mathcal{T}$.

On the other hand, let $\{u_1, u_2, u_3, u_4, u_5, u_6\} \in \mathcal{B}_{\sigma_{6,3},q+1}$. Employing Lemma 24, $\{u_5, u_6\} \in \mathcal{T}$. Thus, $\{u_1, u_2, u_3, u_4, u_5, u_6\} \in \mathcal{B}_{\sigma_{6,3},q+1}$ if and only if $\{u_5, u_6\} \in \mathcal{T}$. Hence, $(U_{q+1}, \mathcal{B}_{\sigma_{6,3},q+1})$ is a 4-$\left(q+1, 6, \frac{q-8}{2}\right)$ design. This completes the proof. □

Proof of Theorem 3. Recall Theorem 3 first. Let $\{u_1, u_2, u_3\}$ be a fixed 3-subset of U_{q+1}. By Lemmas 12 and 18, $\{u_1, u_2, u_3, u_4, u_5\} \in \mathcal{B}_{\sigma_{6,3},q+1}$ if and only if u_4 and u_5 are the two solutions of the quadratic equation $u^2 + au + b = 0$ in U_{q+1}, where $a = \frac{\sigma_{3,1}\sigma_{3,2}+\sigma_{3,3}}{\sigma_{3,1}^2+\sigma_{3,2}}$ and $b = \frac{\sigma_{3,2}^2+\sigma_{3,1}\sigma_{3,3}}{\sigma_{3,1}^2+\sigma_{3,2}}$. Hence, $(U_{q+1}, \mathcal{B}_{\sigma_{5,2},q+1})$ is a Steiner System $S(3, 5, q+1)$. This completes the proof. □

Proof of Theorem 4. Recall Theorem 4 first. For any 3-subset $\{u_1, u_2, u_3\}$ of U_{q+1}, let $Q(u_1, u_2, u_3)$ denote the 2-subset $\left\{u \in U_{q+1} : u^2 + au + b = 0\right\}$, where $a = \frac{\sigma_{3,1}\sigma_{3,2}+\sigma_{3,3}}{\sigma_{3,1}^2+\sigma_{3,2}}$ and $b = \frac{\sigma_{3,2}^2+\sigma_{3,1}\sigma_{3,3}}{\sigma_{3,1}^2+\sigma_{3,2}}$. Next, let $\{u_1, u_2, u_3\}$ be fixed. Set

$$\mathcal{T}_1^0 = \left\{ S^0 \cup \{u_6\} : u_6 \in U_{q+1} \setminus S^0 \right\},$$

and

$$\mathcal{T}_{i,j}^0 = \left\{ \{u_1, u_2, u_3, u_4\} \cup Q(u_i, u_j, u_4) : u_4 \in U_{q+1} \setminus S^0 \right\},$$

where $1 \leq i < j \leq 3$ and $S^0 = \{u_1, u_2, u_3\} \cup Q(u_1, u_2, u_3)$. Let $\mathcal{T}^0 = \mathcal{T}_1^0 \cup \mathcal{T}_{1,2}^0 \cup \mathcal{T}_{1,3}^0 \cup \mathcal{T}_{2,3}^0$. It is easily checked that $\{u_1, u_2, u_3, u_4, u_5, u_6\} \in \mathcal{B}_{\sigma_{6,3},q+1}^0$ if and only if $\{u_1, u_2, u_3, u_4, u_5, u_6\} \in \mathcal{T}^0$. Note that $|\mathcal{T}_1^0| = q - 4$ and $|\mathcal{T}_{i,i}^0| = \frac{q-4}{3}$, where $1 \leq i < j \leq 3$. From Lemma 13, it follows that $\mathcal{T}_1^0$, $\mathcal{T}_{1,2}^0$, $\mathcal{T}_{1,3}^0$ and $\mathcal{T}_{2,3}^0$ are pairwise disjoint. Then $(U_{q+1}, \mathcal{B}_{\sigma_{6,3},q+1}^0)$ is a 3-$(q+1, 6, 2(q-4))$ design.

Let $\{u_1, u_2, u_3\}$ be a fixed 3-subset of U_{q+1}. Define

$$\mathcal{T}^1 = \left\{ \begin{array}{l} \{u_1, u_2, u_3, u_4, u_5, u_6\} : \\ u_4 \in U_{q+1} \setminus S^0, u_5 \in U_{q+1} \setminus (S^0 \cup S^1) \end{array} \right\},$$

where $S^0 = \{u_1, u_2, u_3\} \cup Q(u_1, u_2, u_3)$, $S^1 = \left\{ \frac{\sigma_{4,3}+u_i\sigma_{4,2}}{\sigma_{4,2}+u_i\sigma_{4,1}} : 1 \leq i \leq 4 \right\} \bigcup \left\{ \sqrt{\frac{\sigma_{4,3}}{\sigma_{4,1}}} \right\}$, and

$$u_6 = \frac{\sigma_{5,3}(u_1, u_2, u_3, u_4, u_5)}{\sigma_{5,2}(u_1, u_2, u_3, u_4, u_5)}.$$

Let $\mathcal{T} = \mathcal{T}_1^0 \cup \mathcal{T}^1$. It is easily checked that $B \in \mathcal{B}_{\sigma_{6,3},q+1}$ if and only if $B \in \mathcal{T}$. Note that $|\mathcal{T}_1^0| = q - 4$ and $|\mathcal{T}^1| = \frac{(q+1-|S^0|)(q+1-|S^0 \cup S^1|)}{6}$. By Lemmas 22 and 26, $|S^0 \cup S^1| = 11$. From Lemma 13, $\mathcal{T}_1^0$ and $\mathcal{T}^1$ are disjoint. Then $(U_{q+1}, \mathcal{B}_{\sigma_{6,3},q+1})$ is a 3-$\left(q+1, 6, \frac{(q-4)^2}{6}\right)$ design. This completes the proof. □

IV. Infinite families of BCH codes supporting t-designs for $t = 3, 4$

Throughout this section, let $q = 2^m$, where m is a positive integer. We consider the narrow-sense BCH code $\mathsf{C}_{(q,q+1,4,1)}$ over $\mathrm{GF}(q)$ and its dual, and prove that they are almost MDS, and support 4-designs when $m \geq 5$ is odd and 3-designs when $m \geq 4$ is even.

For a positive integer ℓ, define a $6 \times \ell$ matrix M_ℓ by

$$\begin{bmatrix} u_1^{-3} & u_2^{-3} & \cdots & u_\ell^{-3} \\ u_1^{-2} & u_2^{-2} & \cdots & u_\ell^{-2} \\ u_1^{-1} & u_2^{-1} & \cdots & u_\ell^{-1} \\ u_1^{+1} & u_2^{+1} & \cdots & u_\ell^{+1} \\ u_1^{+2} & u_2^{+2} & \cdots & u_\ell^{+2} \\ u_1^{+3} & u_2^{+3} & \cdots & u_\ell^{+3} \end{bmatrix}, \tag{16}$$

where $u_1, \cdots, u_\ell \in U_{q+1}$. For $r_1, \cdots, r_i \in \{\pm 1, \pm 2, \pm 3\}$, let $M_\ell[r_1, \cdots, r_i]$ denote the submatrix of M_ℓ obtained by deleting the rows $(u_1^{r_1}, u_2^{r_1}, \cdots, u_\ell^{r_1}), \cdots, (u_1^{r_i}, u_2^{r_i}, \cdots, u_\ell^{r_i})$ of the matrix M_ℓ.

Lemma 27. *Let M_ℓ be the matrix given by (16) with $\{u_1, \cdots, u_\ell\} \in \binom{U_{q+1}}{\ell}$. Consider the system of homogeneous linear equations defined by*

$$M_\ell(x_1, \cdots, x_\ell)^T = 0. \tag{17}$$

Then (17) has a nonzero solution $(x_1, \cdots, x_\ell)$ in $\mathrm{GF}(q)^\ell$ if and only if $\mathrm{rank}(M_\ell) < \ell$, where $\mathrm{rank}(M_\ell)$ denotes the rank of the matrix M_ℓ.

Proof. It is obvious that $\mathrm{rank}(M_\ell) < \ell$ if (17) has a nonzero solution $(x_1, \cdots, x_\ell)$ in $\mathrm{GF}(q)^\ell$.

Conversely, assume that $\mathrm{rank}(M_\ell) < \ell$. Then there exists a nonzero vector $\mathbf{x}' = (x_1', \cdots, x_\ell') \in \mathrm{GF}(q^2)^\ell$ such that $M_\ell \mathbf{x}'^T = 0$. Choose an $i_0 \in \{1, \cdots, \ell\}$ such that $x_{i_0}' \neq 0$. Put

$$\mathbf{x} = (x_1'' + x_1''^q, \cdots, x_{i_0}'' + x_{i_0}''^q, \cdots, x_\ell'' + x_\ell''^q),$$

where $(x_1'', \cdots, x_\ell'') = \frac{\alpha}{x_{i_0}'}\mathbf{x}'$ and α is a primitive element of $\mathrm{GF}(q^2)$. It is easily checked that $M_\ell \mathbf{x}^T = 0$ and $\mathbf{x} \in \mathrm{GF}(q)^\ell \setminus \{\mathbf{0}\}$. This completes the proof. □

Lemma 28. *Let M_4 be the matrix given by (16) with $\{u_1, u_2, u_3, u_4\} \in \binom{U_{q+1}}{4}$. Then $\mathrm{rank}(M_4) = 4$.*

Proof. Suppose that $\mathrm{rank}(M_4) < 4$. Then $\det(M_4[2, 3]) = \frac{\prod_{1 \leq i < j \leq 4}(u_i + u_j)}{\sigma_{4,4}^3}(u_1 + u_2 + u_3 + u_4)$=0, which is contrary to Lemma 9. This completes the proof. □

Lemma 29. *Let M_5 be the matrix given by (16) with $\{u_1, \cdots, u_5\} \in \binom{U_{q+1}}{5}$. Then $\mathrm{rank}(M_5) = 4$ if and only if $\sigma_{5,2}(u_1, \cdots, u_5) = 0$.*

Proof. First, note that

$$\begin{cases} \det(M_5[3]) &= \frac{\prod_{1\le i<j\le 5}(u_i+u_j)}{\sigma_{5,5}^3}\sigma_{5,2}, \\ \det(M_5[2]) &= \frac{\prod_{1\le i<j\le 5}(u_i+u_j)}{\sigma_{5,5}^3}\left(\sigma_{5,1}\sigma_{5,2}+\sigma_{5,5}\sigma_{5,2}^q\right), \\ \det(M_5[1]) &= \frac{\prod_{1\le i<j\le 5}(u_i+u_j)}{\sigma_{5,5}^3}\left(\sigma_{5,1}\sigma_{5,5}\sigma_{5,2}^q+\sigma_{5,2}^2\right), \\ \det(M_5[-3]) &= \frac{\prod_{1\le i<j\le 5}(u_i+u_j)}{\sigma_{5,5}}\sigma_{5,2}^q, \\ \det(M_5[-2]) &= \frac{\prod_{1\le i<j\le 5}(u_i+u_j)}{\sigma_{5,5}}\left(\sigma_{5,1}^q\sigma_{5,2}^q+\sigma_{5,5}^q\sigma_{5,2}\right), \\ \det(M_5[-1]) &= \frac{\prod_{1\le i<j\le 5}(u_i+u_j)}{\sigma_{5,5}}\left(\sigma_{5,1}^q\sigma_{5,5}^q\sigma_{5,2}+\sigma_{5,2}^{2q}\right). \end{cases}$$

The desired conclusion then follows from Lemma 28. This completes the proof. □

Lemma 30. *Let M_6 be the matrix given by (16) with $\{u_1,\cdots,u_6\}\in\binom{U_{q+1}}{6}$. Then $\mathrm{rank}(M_6)<6$ if and only if $\sigma_{6,3}(u_1,\cdots,u_6)=0$.*

Proof. Note that

$$\det(M_6)=\frac{\prod_{1\le i<j\le 6}(u_i+u_j)}{\sigma_{6,6}^3}\sigma_{6,3},$$

which completes the proof. □

Lemma 31. *Let m be even and M_6 be the matrix given by (16) with $\{u_1,\cdots,u_6\}\in\binom{U_{q+1}}{6}$. Let $\{u_1,\cdots,u_6\}\in\mathcal{B}^1_{\sigma_{6,3},q+1}$, where $\mathcal{B}^1_{\sigma_{6,3},q+1}$ was defined by (6). Then the set of all solutions of the system $M_6(x_1,\cdots,x_6)^T=0$ over $\mathrm{GF}(q)^6$ is*

$$\{(ax_1,\cdots,ax_6):a\in\mathrm{GF}(q)\},$$

where $(x_1,\cdots,x_6)$ is a vector in $(\mathrm{GF}(q)^*)^6$.

Proof. Let $\{u_1,\cdots,u_6\}\in\mathcal{B}^1_{\sigma_{6,3},q+1}$. By Lemma 30, $\mathrm{rank}(M_6)<6$. By Lemma 27, there exists a nonzero $(x_1,\cdots,x_6)\in\mathrm{GF}(q)^6$ such that $M_6(x_1,\cdots,x_6)^T=0$. Suppose that there is an i ($1\le i\le 6$) such that $x_i=0$. Then the submatrix of the matrix M_6 obtained by deleting the i-th column has rank less than 5, which is contrary to Lemma 29 and the definition of $\mathcal{B}^1_{\sigma_{6,3},q+1}$. Thus, for any nonzero solution $(x_1,\cdots,x_6)\in\mathrm{GF}(q)^6$, we have $x_i\neq 0$, where $1\le i\le 6$. The desired conclusion then follows. This completes the proof. □

Lemma 32. *Let m be even and M_6 be the matrix given by (16) with $\{u_1,\cdots,u_6\}\in\binom{U_{q+1}}{6}$. If there exists a vector $(x_1,\cdots,x_6)\in(\mathrm{GF}(q)^*)^6$ such that $M_6(x_1,\cdots,x_6)^T=0$, then $\{u_1,\cdots,u_6\}\in\mathcal{B}^1_{\sigma_{6,3},q+1}$, where $\mathcal{B}^1_{\sigma_{6,3},q+1}$ was defined by (6).*

Proof. By Lemma 30, $\{u_1,\cdots,u_6\}\in\mathcal{B}_{\sigma_{6,3},q+1}$. Suppose that $\{u_1,\cdots,u_6\}\in\mathcal{B}^0_{\sigma_{6,3},q+1}$. Without loss of generality, let $\sigma_{5,2}(u_1,\cdots,u_5)=0$. By Lemmas 27 and 29, there exists a nonzero $(x_1',\cdots,x_5')\in\mathrm{GF}(q)^5$ such that $M_5(x_1',\cdots,x_5')^T=0$, that is, $M_6(x_1',\cdots,x_5',0)^T=0$. Note that

$$M_6\left(x_1+\frac{x_1}{x_1'}x_1',\cdots,x_5+\frac{x_1}{x_1'}x_5',x_6+\frac{x_1}{x_1'}0\right)^T=0.$$

Applying Lemma 29, $\sigma_{5,2}(u_2,\cdots,u_6)=0$, which is contrary to Lemma 13 and $\sigma_{5,2}(u_1,\cdots,u_5)=0$. This completes the proof. □

Lemma 33. *Let $f(u)=\mathrm{Tr}_{q^2/q}\left(au^3+bu^2+cu\right)$ where $(a,b,c)\in\mathrm{GF}(q^2)^3\setminus\{\mathbf{0}\}$. Define $\mathrm{zero}(f)=\{u\in U_{q+1}:f(u)=0\}$. Then $|\mathrm{zero}(f)|\le 6$. Moreover, $|\mathrm{zero}(f)|=6$ if and only if $a=\frac{\tau}{\sqrt{\sigma_{6,6}}}$, $b=\frac{\tau\sigma_{6,1}}{\sqrt{\sigma_{6,6}}}$ and $c=\frac{\tau\sigma_{6,2}}{\sqrt{\sigma_{6,6}}}$, where $\{u_1,\cdots,u_6\}\in\mathcal{B}_{\sigma_{6,3},q+1}$ and $\tau\in\mathrm{GF}(q)^*$.*

Proof. When $u\in U_{q+1}$, one has

$$f(u)=\frac{1}{u^3}\left(au^6+bu^5+cu^4+c^qu^2+b^qu+a^q\right). \quad (18)$$

Thus, $|\mathrm{zero}(f)|\le 6$.

Assume that $|\mathrm{zero}(f)|=6$. From (18), there exists $\{u_1,\cdots,u_6\}\in U_{q+1}$ such that $f(u)=\frac{a\prod_{i=1}^6(u+u_i)}{u^3}$. By Vieta's formula, $b=a\sigma_{6,1}$, $c=a\sigma_{6,2}$, $0=\sigma_{6,3}$, $c^q=a\sigma_{6,6}\sigma_{6,2}^q$, $b^q=a\sigma_{6,6}\sigma_{6,1}^q$ and $a^q=a\sigma_{6,6}$. One obtains $a=\frac{\tau}{\sqrt{\sigma_{6,6}}}$ from $a^{q-1}=\sigma_{6,6}$, where $\tau\in\mathrm{GF}(q)^*$. Then $b=\frac{\tau\sigma_{6,1}}{\sqrt{\sigma_{6,6}}}$ and $c=\frac{\tau\sigma_{6,2}}{\sqrt{\sigma_{6,6}}}$.

Conversely, assume that $a=\frac{\tau}{\sqrt{\sigma_{6,6}}}$, $b=\frac{\tau\sigma_{6,1}}{\sqrt{\sigma_{6,6}}}$ and $c=\frac{\tau\sigma_{6,2}}{\sqrt{\sigma_{6,6}}}$, where $\{u_1,\cdots,u_6\}\in\mathcal{B}_{\sigma_{6,3},q+1}$ and $\tau\in\mathrm{GF}(q)^*$. Then $f(u)=\frac{a\prod_{i=1}^6(u+u_i)}{u^3}$. Thus, $\mathrm{zero}(f)=\{u_1,\cdots,u_6\}$ and $|\mathrm{zero}(f)|=6$. □

A. A class of narrow-sense BCH codes with length 2^m+1

We are now ready to prove the following result about the code $\mathsf{C}_{(q,q+1,4,1)}$.

Theorem 34. *Let $m\ge 4$ be an integer. Then the narrow-sense BCH code $\mathsf{C}_{(q,q+1,4,1)}$ over $\mathrm{GF}(q)$ has parameters $[q+1,q-5,d]$, where $d=6$ if m is odd and $d=5$ if m is even.*

Proof. Put $n=q+1$. Let α be a generator of $\mathrm{GF}(q^2)^*$ and $\beta=\alpha^{q-1}$. Then β is a primitive n-th root of unity in $\mathrm{GF}(q^2)$, that is, β is a generator of the cyclic group U_{q+1}. Let $g_i(x)$ denote the minimal polynomial of β^i over $\mathrm{GF}(q)$, where $i\in\{1,2,3\}$. Note that $g_i(x)$ has only the roots β^i and β^{-i}. One deduces that $g_1(x)$, $g_2(x)$ and $g_3(x)$ are pairwise distinct irreducible polynomials of degree 2. By definition, $g(x):=g_1(x)g_2(x)g_3(x)$ is the generator polynomial of $\mathsf{C}_{(q,q+1,4,1)}$. Therefore, the dimension of $\mathsf{C}_{(q,q+1,4,1)}$ is $q+1-6$. Note that $g(x)$ has only the roots $\beta^{-3},\beta^{-2},\beta^{-1},\beta,\beta^2$ and β^3. By the BCH bound, the minimum weight of $\mathsf{C}_{(q,q+1,4,1)}$ is at least 4. Put $\gamma=\beta^{-1}$. Then $\gamma^{q+1}=\beta^{-(q+1)}=1$. It then follows from Delsarte's theorem that the trace expression of $\mathsf{C}^{\perp}_{(q,q+1,4,1)}$ is given by

$$\mathsf{C}^{\perp}_{(q,q+1,4,1)}=\{\mathbf{c}_{(a,b,c)}:a,b,c\in\mathrm{GF}(q^2)\}, \quad (19)$$

where $\mathbf{c}_{(a,b,c)}=(\mathrm{Tr}_{q^2/q}(a\gamma^i+b\gamma^{2i}+c\gamma^{3i}))_{i=0}^{q}$.

Define

$$H=\begin{bmatrix} 1 & \gamma^{-3} & \gamma^{-6} & \gamma^{-9} & \cdots & \gamma^{-3q} \\ 1 & \gamma^{-2} & \gamma^{-4} & \gamma^{-6} & \cdots & \gamma^{-2q} \\ 1 & \gamma^{-1} & \gamma^{-2} & \gamma^{-3} & \cdots & \gamma^{-q} \\ 1 & \gamma^{+1} & \gamma^{+2} & \gamma^{+3} & \cdots & \gamma^{+q} \\ 1 & \gamma^{+2} & \gamma^{+4} & \gamma^{+6} & \cdots & \gamma^{+2q} \\ 1 & \gamma^{+3} & \gamma^{+6} & \gamma^{+9} & \cdots & \gamma^{+3q} \end{bmatrix}. \quad (20)$$

It is easily seen that H is a parity-check matrix of $\mathsf{C}_{(q,q+1,4,1)}$, i.e.,

$$\mathsf{C}_{(q,q+1,4,1)} = \{\mathbf{c} \in \mathrm{GF}(q)^{q+1} : \mathbf{c}H^T = \mathbf{0}\}. \quad (21)$$

Let m be odd. Note that $d \geq 4$. Suppose that $d = 4$. Then there exist $\{u_1, \cdots, u_4\} \in \binom{U_{q+1}}{4}$ and $(x_1, \cdots, x_4) \in (\mathrm{GF}(q)^*)^4$ such that $M_4(x_1, \cdots, x_4)^T = 0$. Thus $\mathrm{rank}(M_4) < 4$, which is contrary to Lemma 28. Suppose that $d = 5$. Then there exist $\{u_1, \cdots, u_5\} \in \binom{U_{q+1}}{5}$ and $(x_1, \cdots, x_5) \in (\mathrm{GF}(q)^*)^5$ such that $M_5(x_1, \cdots, x_5)^T = 0$. By Lemma 29, $\mathrm{rank}(M_5) < 5$ and $\sigma_{5,2} = 0$, which is contrary to Lemma 17. Thus, $d \geq 6$. By Theorem 2, $\mathcal{B}_{\sigma_{6,3},q+1} \neq \emptyset$. Choose $\{u_1, \cdots, u_6\} \in \mathcal{B}_{\sigma_{6,3},q+1}$. By Lemma 27, there exists $(x_1, \cdots, x_6) \in (\mathrm{GF}(q)^*)^6$ such that $M_6(x_1, \cdots, x_6)^T = 0$. Set $\mathbf{c} = (c_1, \cdots, c_{q+1})$ where

$$c_i = \begin{cases} x_j, & \text{if } i = i_j, \\ 0, & \text{otherwise}, \end{cases} \quad (22)$$

where γ_{i_j} is given by $u_j = \gamma^{i_j}$ ($j \in \{1, \cdots, 6\}$). By (21), $\mathbf{c} \in \mathsf{C}_{(q,q+1,4,1)}$ and $\mathtt{wt}(\mathbf{c}) = 6$. Thus, $d = 6$.

The proof for the even m case is similar to that for the odd m case and the detail is omitted. This completes the proof. □

Theorem 35. *Let $m \geq 4$ and $\mathsf{C}^{\perp}_{(q,q+1,4,1)}$ be the dual of the narrow-sense BCH code $\mathsf{C}_{(q,q+1,4,1)}$ over $\mathrm{GF}(q)$. Then $\mathsf{C}^{\perp}_{(q,q+1,4,1)}$ has parameters $[q+1, 6, q-5]$. In particular, $\mathsf{C}_{(q,q+1,4,1)}$ is a near MDS code if m is odd.*

Proof. From Theorems 2 and 4, $\mathcal{B}_{\sigma_{6,3},q+1} \neq \emptyset$. The desired conclusion then follows from Lemma 33 and Equation (19). This completes the proof. □

B. An infinite class of near MDS codes supporting 4-designs

Theorem 36. *Let $m \geq 5$ be odd. Then the incidence structure*

$$\left(\mathcal{P}\left(\mathsf{C}_{(q,q+1,4,1)}\right), \mathcal{B}_6\left(\mathsf{C}_{(q,q+1,4,1)}\right)\right)$$

of the minimum weight codewords in $\mathsf{C}_{(q,q+1,4,1)}$ is isomorphic to $(U_{q+1}, \mathcal{B}_{\sigma_{6,3},q+1})$.

Proof. Using Lemma 30, the desired conclusion then follows by a similar discussion as in the proof of Theorem 34. This completes the proof. □

The theorem below makes a breakthrough in 71 years in the sense that it presents the first family of linear codes supporting an infinite family of 4-designs since the first linear code holding a 4-design was discovered 71 years ago by Golay [11].

Theorem 37. *Let $m \geq 5$ be odd. Then the minimum weight codewords in $\mathsf{C}_{(q,q+1,4,1)}$ support a 4-$(q+1, 6, (q-8)/2)$ design and the minimum weight codewords in $\mathsf{C}^{\perp}_{(q,q+1,4,1)}$ support a 4-$(q+1, q-5, \lambda)$ design with*

$$\lambda = \frac{q-8}{30}\binom{q-5}{4}.$$

Proof. The desired conclusion follows from Theorems 36, 2 and 1. This completes the proof. □

Example 38. *Let $m = 5$. Then $\mathsf{C}_{(q,q+1,4,1)}$ has parameters $[33, 27, 6]$. The dual $\mathsf{C}^{\perp}_{(q,q+1,4,1)}$ has parameters $[33, 6, 27]$ and weight distribution*

$$1 + 1014816z^{27} + 1268520z^{28} + 20296320z^{29} + 64609952z^{30} + 210132384z^{31} + 399584823z^{32} + 376835008z^{33}.$$

The codewords of weight 6 in $\mathsf{C}_{(q,q+1,4,1)}$ supports a 4-$(33, 6, 12)$ design, and the codewords of weight 27 in $\mathsf{C}^{\perp}_{(q,q+1,4,1)}$ support a 4-$(33, 27, 14040)$ design.

In Example 38, the code $\mathsf{C}_{(q,q+1,4,1)}$ has a codeword of weight i for all i with $6 \leq i \leq 33$. Hence, the Assmus-Mattson Theorem cannot prove that the codes in Theorem 37 support 4-designs. It is an open problem whether the generalised Assmus-Mattson theorem in [20] can prove that the codes in Theorem 37 support 4-designs. It looks impossible to prove that the codes in Theorem 37 support 4-designs with the automorphism groups of the codes due to the following:

1) Except the Mathieu groups M11, M12, M23, M24, the alternating group A_n and the symmetric group S_n, no finite permutation groups are more than 3-transitive [2].
2) No infinite family of 4-homogeneous permutation groups is known.

It would be a very interesting problem to determine the automorphism groups of the codes in Theorem 37.

C. An infinite class of linear codes supporting Steiner systems $S(3, 5, 4^m + 1)$

Theorem 39. *Let $m \geq 4$ be even. Then the incidence structure*

$$\left(\mathcal{P}\left(\mathsf{C}_{(q,q+1,4,1)}\right), \mathcal{B}_5\left(\mathsf{C}_{(q,q+1,4,1)}\right)\right)$$

of the minimum weight codewords in $\mathsf{C}_{(q,q+1,4,1)}$ is isomorphic to $(U_{q+1}, \mathcal{B}_{\sigma_{5,2},q+1})$, and the incidence structure

$$\left(\mathcal{P}\left(\mathsf{C}_{(q,q+1,4,1)}\right), \mathcal{B}_6\left(\mathsf{C}_{(q,q+1,4,1)}\right)\right)$$

is isomorphic to $(U_{q+1}, \mathcal{B}^1_{\sigma_{6,3},q+1})$. Moreover, the incidence structure

$$\left(\mathcal{P}\left(\mathsf{C}^{\perp}_{(q,q+1,4,1)}\right), \mathcal{B}_{q-5}\left(\mathsf{C}^{\perp}_{(q,q+1,4,1)}\right)\right)$$

is isomorphic to the complementary incidence structure of $(U_{q+1}, \mathcal{B}_{\sigma_{6,3},q+1})$.

Proof. Using Lemma 29, by a similar discussion as in the proof of Theorem 34, we can prove that the incidence structure

$$\left(\mathcal{P}\left(\mathsf{C}_{(q,q+1,4,1)}\right), \mathcal{B}_5\left(\mathsf{C}_{(q,q+1,4,1)}\right)\right)$$

is isomorphic to $(U_{q+1}, \mathcal{B}_{\sigma_{5,2},q+1})$. Employing Lemma 32, we can prove that

$$\left(\mathcal{P}\left(\mathsf{C}_{(q,q+1,4,1)}\right), \mathcal{B}_6\left(\mathsf{C}_{(q,q+1,4,1)}\right)\right)$$

is isomorphic to $(U_{q+1}, \mathcal{B}^1_{\sigma_{6,3},q+1})$. The last statement then follows from Equation (19) and Lemma 33. This completes the proof. □

Theorem 40. *Let $m \geq 4$ be even. Then the minimum weight codewords in $\mathsf{C}_{(q,q+1,4,1)}$ support a 3-$(q+1, 5, 1)$ design, i.e., a Steiner system $S(3, 5, q+1)$, and the minimum weight*

codewords in $\mathsf{C}_{(q,q+1,4,1)}^{\perp}$ *support a* 3-$(q+1, q-5, \lambda)$ *design with*

$$\lambda = \frac{(q-4)^2}{120}\binom{q-5}{3}.$$

Furthermore, the codewords of weight 6 *in* $\mathsf{C}_{(q,q+1,4,1)}$ *support a* 3-$\left(q+1, 6, \frac{(q-4)(q-16)}{6}\right)$ *design if* $m \geq 6$.

Proof. The desired conclusion follows from Theorems 39, 3, 4 and Corollary 5. This completes the proof. □

There are two different constructions of an infinite family of Steiner systems $S(3, r+1, r^m+1)$ for r being a prime power and $m \geq 2$. The first produces the spherical geometry designs due to [24], which is based on the action of $\mathrm{PGL}_2(\mathrm{GF}(r^m))$ on the base block $\mathrm{GF}(r) \cup \{\infty\}$. The automorphism group of the spherical geometry design contains the group $\mathrm{P\Gamma L}_2(\mathrm{GF}(r^m))$. The second construction was proposed in [13], and is based on affine spaces. The Steiner systems $S(3, r+1, r^m+1)$ from the two constructions are not isomorphic [13].

When $m \in \{2, 3\}$, the Steiner system $S(3, 5, 4^m+1)$ of Theorem 40 is isomorphic to the spherical geometry design with the same parameters. We conjecture that they are isomorphic in general, but do not have a proof. The contribution of Theorem 40 is a coding-theoretic construction of the spherical geometry design $S(3, 5, 4^m+1)$ if this conjecture is true. .

Example 41. *Let* $m = 4$. *Then* $\mathsf{C}_{(q,q+1,4,1)}$ *has parameters* $[17, 11, 5]$ *and weight distribution*

$$\begin{aligned}1 &+ 1020z^5 + 224400z^7 + 3730650z^8 + 55370700z^9 \\ &+ 669519840z^{10} + 6378704640z^{11} + 47857084200z^{12} \\ &+ 276083558100z^{13} + 1183224112800z^{14} \\ &+ 3549668972400z^{15} + 6655630071165z^{16} \\ &+ 5872614694500z^{17}.\end{aligned}$$

The codewords of weight 5 *in* $\mathsf{C}_{(q,q+1,4,1)}$ *support a Steiner system* $S(3, 5, 17)$.

The dual $\mathsf{C}_{(q,q+1,4,1)}^{\perp}$ *has parameters* $[17, 6, 11]$ *and weight distribution*

$$\begin{aligned}1 &+ 12240z^{11} + 35700z^{12} + 244800z^{13} + 1203600z^{14} \\ &+ 3292560z^{15} + 6398715z^{16} + 5589600z^{17}.\end{aligned}$$

The codewords of weight 11 *in* $\mathsf{C}_{(q,q+1,4,1)}^{\perp}$ *support a* 3-$(17, 11, 198)$ *design.*

This example shows that the Assmus-Mattson Theorem cannot prove that the codes $\mathsf{C}_{(q,q+1,4,1)}$ and $\mathsf{C}_{(q,q+1,4,1)}^{\perp}$ support 3-designs. It is an open question if the generalised Assmus-Mattson theorem in [20] can prove that the codes in Theorem 40 support 4-designs. It is also an open question if the automorphism groups of the codes can prove that the codes support 3-designs.

V. Summary and concluding remarks

This paper settled the 71-year-old open problem by presenting an infinite family of near MDS codes of length $2^{2m+1}+1$ over $\mathrm{GF}(2^{2m+1})$ holding an infinite family of 4-$(2^{2m+1}+1, 6, 2^{2m}-4)$ designs [14, Table 4.37]. Hence, these codes have nice applications in combinatorics. It would be nice if the automorphism groups of the linear codes could be determined. It is noticed that the novelty of this paper and [6] is that elementary symmetric polynomials and their properties were used to prove the design property of the incidence structures from special near MDS codes. This opens a new direction of searching for t-designs from elementary symmetric polynomials.

A coding-theoretic construction of a Steiner system $S(3, r+1, r^m+1)$ was given in [6] for $r = 3$ and in this paper for $r = 4$. Whether there exists an infinite family of linear codes holding a Steiner system $S(3, r+1, r^m+1)$ for $r \geq 5$ being a prime power is yet unknown.

An interesting open problem is whether there exists an infinite family of linear codes holding an infinite family of t-designs for $t \geq 5$. Another open problem is whether there is a specific linear code supporting a nontrivial 6-design.

Acknowledgements

The authors are very grateful to the anonymous reviewers and the associate editor, Prof. Sudhir Ghorpade, for their comments and suggestions that much improved the presentation of this paper.

References

[1] E. F. Assmus Jr., H. F. Mattson Jr., "New 5-designs," *J. Comb. Theory*, vol. 6, pp. 122–151, 1969
[2] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 1999.
[3] C. Ding, *Codes from Difference Sets*, World Scientific, Singapore, 2015.
[4] C. Ding, *Designs from Linear Codes*, World Scientific, Singapore, 2019.
[5] C. Ding, C. Li, "Infinite families of 2-designs and 3-designs from linear codes," *Discrete Math.*, vol. 340, no. 10, pp. 2415–2431, 2017.
[6] C. Ding, C. Tang, "Infinite families of near MDS codes holding t-designs," *IEEE Trans. Inf. Theory*, vol. 66, no. 9, pp. 5419–5428, 2020.
[7] C. Ding, Z. Zhou, "Parameters of 2-designs from some BCH codes," Codes, Cryptography and Information Security, Lecture Notes in Computer Science, S. El Hajji, A. Nitaj and E. M. Souidi (Editors), Springer, Heidelberg, Vol. 10194, pp. 110–127, 2017.
[8] S. Dodunekov, I. Landgev, "On near-MDS codes," *J. Geometry*, vol. 54, pp. 30–43, 1995.
[9] S. M. Dodunekov, I. N. Landjev, "Near-MDS codes over some small fields," *Discrete Math.*, vol. 213, pp. 55–65, 2000.
[10] A. Faldum, W. Willems, "Codes of small defect," *Des. Codes Cryptogr.*, vol. 10, pp. 341–350, 1997.
[11] M. J. E. Golay, "Notes on digital coding," *Proceedings of the I.R.E.*, vol. 37, p. 657, 1949.
[12] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
[13] J. D. Key, A. Wagner, "On an infinite class of Steiner systems constructed from affine spaces," *Arch. Math.*, vol. 47, pp. 376–378, 1986.
[14] G. B. Khosrovshahi, R. Laue, "t-designs with $t \geq 3$," in: Handbook of Combinatorial Designs, 2nd Edition, C. J. Colbourn, and J. H. Dinitz, (Editors), CRC Press, New York, pp.79–101, 2007.
[15] R. Lidl, H. Niederreiter, *Finite fields*, vol. 20, Cambridge University Press, 1997.
[16] C. Li, P. Wu, F. Liu, "On two classes of primitive BCH codes and some related codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3830–3840, 2019.
[17] S. Li, "The minimum distance of some narrow-sense primitive BCH codes," *SIAM J. Discrete Math.*, vol. 31, no. 4, pp. 2530–2569, 2017.
[18] Y. Liu, R. Li, Q. Fu, L. Lu, Y. Rao, "Some binary BCH codes with length $n = 2^m + 1$," *Finite Fields and Their Applications*, vol. 55, pp. 109–133, 2019.
[19] X. Shi, Q. Yue, Y. Wu, "The dual-containing primitive BCH codes with the maximum designed distance and their applications to quantum codes," *Des. Codes Cryptogr.*, vol. 87, no. 9, pp. 2165–2183, 2019.

[20] C. Tang, C. Ding, M. Xiong, Codes, "differentially δ-uniform functions and t-designs," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3691–3703, 2020.
[21] V. D. Tonchev, "Codes and designs," in: Handbook of Coding Theory, Vol. II, V. S. Pless, and W. C. Huffman, (Editors), Elsevier, Amsterdam, pp. 1229–1268, 1998.
[22] V. D. Tonchev, "Codes," in: Handbook of Combinatorial Designs, 2nd Edition, C. J. Colbourn, and J. H. Dinitz, (Editors), CRC Press, New York, pp.677–701, 2007.
[23] H. Tong, Y. Ding, "Quasi-cyclic NMDS codes," *Finite Fields and Their Applications*, vol. 24, pp. 45–54, 2013.
[24] E. Witt, " Über Steinersche Systeme," *Abh. Math. Sem. Hamburg*, vol. 12, pp. 265–275, 1938.
[25] H. Yan, H. Liu, C. Li, S. Yang, "Parameters of LCD BCH codes with two lengths," *Adv. in Math. of Comm.*, vol. 12, no. 3, pp. 579–594, 2018.

Chunming Tang was born in Sichuan, China, in 1982. He received the B.S. degree from Sichuan Normal University, Sichuan, China, in 2004, the M.S. degree and Ph. D. degree from Peking University, Beijing, China, in 2012. From 2017 to 2018, he was a postdoctoral member in the Department of Mathematics, the Universities of Paris VIII. He is now a professor in the School of Mathematics and Information, China West Normal University, Nanchong, Sichuan, China. His research fields are cryptography, coding theory, and information security.

Cunsheng Ding (M'98–SM'05) was born in 1962 in Shaanxi, China. He received the M.Sc. degree in 1988 from the Northwestern Telecommunications Engineering Institute, Xian, China; and the Ph.D. in 1997 from the University of Turku, Turku, Finland.

From 1988 to 1992 he was a Lecturer of Mathematics at Xidian University, China. Before joining the Hong Kong University of Science and Technology in 2000, where he is currently a Professor of Computer Science and Engineering, he was an Assistant Professor of Computer Science at the National University of Singapore.

His research fields are combinatorial designs, cryptography and coding theory. He has coauthored five research monographs, and served as a guest editor or editor for ten journals. Dr. Ding co-received the State Natural Science Award of China in 1989.