Shortened Linear Codes Over Finite Fields

Yang Liu, Cunsheng Ding, *Senior Member, IEEE*, and Chunming Tang

***Abstract*— The puncturing and shortening techniques are two important approaches to constructing new linear codes from old ones. In the past 70 years, a lot of progress on the puncturing technique has been made, and many works on punctured linear codes have been done. Many families of linear codes with interesting parameters have been obtained with the puncturing technique. However, little research on the shortening technique has been done and there are only a handful references on shortened linear codes. The first objective of this paper is to prove some general theory for shortened linear codes. The second objective is to study some shortened codes of the Hamming codes, Simplex codes, some Reed-Muller codes, and ovoid codes. Eleven families of optimal shortened codes over finite fields are presented in this paper. As a byproduct, five infinite families of 2-designs are also constructed from some of the shortened codes presented in this paper.**

***Index Terms*— Linear code, cyclic code, punctured code, shortened code, t-design.**

I. Introduction

LET $\mathrm{GF}(q)$ denote the finite field with q elements, where q is a prime power. An $[n, \kappa, d]$ code over $\mathrm{GF}(q)$ is a κ-dimensional linear subspace of $\mathrm{GF}(q)^n$ with minimum Hamming distance d. Throughout the whole paper, let $\mathcal{C}$ be an $[n, \kappa, d]$ code over $\mathrm{GF}(q)$, unless the length, dimension and minimum distance of $\mathcal{C}$ and q are otherwise stated. By the parameters of a linear code, we refer to its length, dimension and minimum distance. Let $A_i(\mathcal{C})$ denote the number of codewords with Hamming weight i in $\mathcal{C}$, where $0 \leq i \leq n$. The sequence $(A_0(\mathcal{C}), A_1(\mathcal{C}), \cdots, A_n(\mathcal{C}))$ is called the *weight distribution* of $\mathcal{C}$, and $\sum_{i=0}^{n} A_i(\mathcal{C}) z^i$ is referred to as the *weight enumerator* of $\mathcal{C}$.

Manuscript received July 5, 2020; revised May 30, 2021; accepted June 2, 2021. Date of publication June 7, 2021; date of current version July 14, 2021. The work of Yang Liu was supported in part by NSFC under Project 11801414 and Project 11701140 and in part by the Natural Science Foundation of Hebei Province of China under Project A2019210223. The work of Cunsheng Ding was supported by the Hong Kong Research Grants Council under Project 16301020. The work of Chunming Tang was supported in part by the National Natural Science Foundation of China under Grant 11871058 and in part by the China West Normal University (Meritocracy Research Funds) under Grant 14E013 and Grant CXTD2014-4. *(Corresponding author: Chunming Tang.)*

Yang Liu is with the College of Mathematics and Information Science, Tianjin University of Commerce, Tianjin 300384, China (e-mail: yangshaohua120@163.com).

Cunsheng Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong, SAR, China (e-mail: cding@ust.hk).

Chunming Tang is with the School of Mathematics and Information, China West Normal University, Nanchong 637002, China, and also with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong, SAR, China (e-mail: tangchunmingmath@163.com).

Communicated by V. Sidorenko, Associate Editor for Coding Techniques.
Digital Object Identifier 10.1109/TIT.2021.3087082

The code $\mathcal{C}$ is called *distance-optimal* (respectively, *dimension-optimal* and *length-optimal*) if there is no $[n, \kappa, d' \geq d+1]$ (respectively, $[n, \kappa' \geq \kappa+1, d]$ and $[n' \leq n-1, \kappa, d]$) linear code over $\mathrm{GF}(q)$. An optimal code is a code that is length-optimal, or dimension-optimal, or distance-optimal, or meets a bound for linear codes. If the code $\mathcal{C}$ is distance-optimal, then any linear code over $\mathrm{GF}(q)$ with parameters $[n, \kappa, d-1]$ is called *distance-almost-optimal*. If the code $\mathcal{C}$ is dimension-optimal, then any linear code over $\mathrm{GF}(q)$ with parameters $[n, \kappa-1, d]$ is called *dimension-almost-optimal*. If the code $\mathcal{C}$ is length-optimal, then any linear code over $\mathrm{GF}(q)$ with parameters $[n+1, \kappa, d]$ is called *length-almost-optimal*.

Two linear codes of the same length over $\mathrm{GF}(q)$ are said to be *permutation-equivalent* if one can be transformed into the other by a permutation of the coordinates of codewords, and *monomially-equivalent* if one can be transformed into the other by a permutation of the coordinates of codewords and the multiplication of each coordinate of all codewords with a nonzero element in $\mathrm{GF}(q)$.

An important problem in the theory and practice of coding theory is the construction of linear codes with good error-correcting capability or desirable parameters. To this end, one may construct a linear code with good or desirable parameters from a known linear code with optimal or good parameters. There are several standard ways of obtaining linear codes from a known one. The most famous methods are the puncturing and shortening techniques. Since extending a linear code increases the code length by one and does not change the code dimension, the extending method is less interesting in constructing new codes.

Let T be a set of t coordinate positions in $\mathcal{C}$. We puncture $\mathcal{C}$ by deleting all the coordinates in T in each codeword of $\mathcal{C}$. The resulting code is still linear and has length $n-t$, where $t = |T|$. We denote the punctured code by $\mathcal{C}^T$. Let $\mathcal{C}(T)$ be the set of codewords which are 0 on T. Then $\mathcal{C}(T)$ is a subcode of $\mathcal{C}$. We now puncture $\mathcal{C}(T)$ on T, and obtain a linear code over $\mathrm{GF}(q)$ with length $n-t$, which is called a *shortened code* of $\mathcal{C}$, and is denoted by $\mathcal{C}_T$.

To explain the motivations of this paper, we recall a general construction of linear codes. Let $D = \{d_1, d_2, \ldots, d_n\} \subseteq \mathrm{GF}(r)$, where $r = q^m$. Let $\mathrm{Tr}_{r/q}$ be the trace function from $\mathrm{GF}(r)$ to $\mathrm{GF}(q)$. Define a linear code of length n over $\mathrm{GF}(q)$ by

$$\mathcal{C}_D = \{(\mathrm{Tr}_{r/q}(xd_1), \ldots, \mathrm{Tr}_{r/q}(xd_n)) : x \in \mathrm{GF}(r)\}. \quad (1)$$

The set D is called the defining set of $\mathcal{C}_D$. The next theorem says that the defining-set construction in (1) is fundamental [17], and is a refinement of the work in [28].

Theorem 1 [17, Theorem 1]: Any linear code of length n over $\mathrm{GF}(q)$ can be expressed as the code $\mathcal{C}_D$ in (1), where $D = \{d_1, d_2, \ldots, d_n\} \subseteq \mathrm{GF}(q^m)$ is a multiset and m is some positive integer.

Let α be a primitive element of $\mathrm{GF}(q^m)$. The following code

$$\mathcal{C}(m, q, \alpha) = \{(\mathrm{Tr}_{q^m/q}(a\alpha^0), \ldots, \mathrm{Tr}_{q^m/q}(a\alpha^{q^m-2})) : a \in \mathrm{GF}(q^m)\} \quad (2)$$

is a $[q^m - 1, m, (q-1)q^{m-1}]$ cyclic code with check polynomial $M_{\alpha^{-1}}(x)$, which is the minimal polynomial of α^{-1} over $\mathrm{GF}(q)$ and is irreducible over $\mathrm{GF}(q)$. The code $\mathcal{C}(m, q, \alpha)$ is said to be *irreducible*. It is easily seen that the weight enumerator of $\mathcal{C}(m, q, \alpha)$ is $1 + (q^m - 1)z^{q^m - q^{m-1}}$ [13].

The next theorem was proved in [16, Theorem 3].

Theorem 2 [16, Theorem 3]: Every linear code of length n over $\mathrm{GF}(q)$ with dual distance at least 3 is permutation-equivalent to a punctured code of an irreducible cyclic code $\mathcal{C}(m, q, \alpha)$ in (2) for some integer m and primitive element $\alpha \in \mathrm{GF}(q^m)$.

While cyclic codes form a subclass of linear codes, every linear code with minimum distance at least 3 can be punctured from a special irreducible cyclic code $\mathcal{C}(m, q, \alpha)$. This demonstrates the importance of the very special subclass of irreducible cyclic codes $\mathcal{C}(m, q, \alpha)$ and the puncturing technique.

In the past ten years, a lot of research on the defining-set construction of linear codes has been done, and many families of linear codes with various parameters have been obtained (see, for example, [8], [11], [12], [17], [27]). Recall that the defining-set construction is in fact to puncture a code $\mathcal{C}(m, q, \alpha)$. Hence, the puncturing technique was extensively studied in the past ten years and proved to be an effective approach to obtaining linear codes with good or desirable parameters. However, every approach has limitations and there is no exception for the puncturing technique.

Motivated by the success of the puncturing technique, we ask the following questions on the shortening technique:

1) Is there a family of cyclic codes such that every linear code with minimum distance at least 3 is a shortened code of a cyclic code in this family?
2) Can we obtain optimal linear codes or linear codes with desirable parameters by shortening certain known families of linear codes or cyclic codes? If the answer is positive, which known families of linear codes can be shortened for obtaining good linear codes, and which set T of coordinate positions leads to a shortened linear code $\mathcal{C}_T$ with good or desirable parameters?
3) Can we develop some general theory for shortened linear codes?

The basic questions above are the major motivations of studying the shortening technique. In addition to obtaining new linear codes with desirable parameters from old ones, one may have to study some shortened codes of certain families of linear codes in particular applications. For instance, in order to obtain 2-designs and Steiner systems, certain shortened codes of a family of ternary codes were investigated in [25], where two families of shortened ternary codes with the best-known parameters were obtained. The study of shortened linear codes in [26] led to a generalization of the Assmus-Mattson theorem. Shortened and punctured codes were used to prove a generalized MacWilliams identity in [14]. These important applications of shortened linear codes are additional motivations of this paper.

The last motivation of this paper is that there are only several papers on shortened linear codes in the literature (see [2], [7], [15], [21], [22], [24], [29]). This is quite amazing, as the defining-set construction of linear codes is a puncturing technique and there are over a hundred papers on the defining-set construction. This fact shows that the shortening technique was overlooked by the coding theory community for 70 years.

It is known that $\mathcal{C}_T = ((\mathcal{C}^\perp)^T)^\perp$ (see Theorem 8 below). This means that in theory a shortened linear code can be obtained by first performing the dual operation, then the puncturing operation, and finally the dual operation. But this involves the study of three codes in the sequence $\left(\mathcal{C}^\perp, (\mathcal{C}^\perp)^T, ((\mathcal{C}^\perp)^T)^\perp\right)$, and is usually much more complicated. In addition, the puncturing technique also has a limitation in obtaining linear codes with good parameters in practice. Consequently, it is still necessary to study the shortening technique.

The objectives of this paper are the following:

1) Develop some general theory for shortened linear codes.
2) Construct linear codes over $\mathrm{GF}(q)$ with various and good parameters by shortening some known families of linear codes over $\mathrm{GF}(q)$.

In this paper, we present eleven families of optimal shortened codes and five families of 2-designs from some of the shortened codes.

II. General Results About Shortened Linear Codes

The objective of this paper is to study shortened linear codes. The theory of shortened codes is related to orthogonal arrays and t-designs. In this section, we first introduce some fundamental results of orthogonal arrays and t-designs, as they will be used as basic tools for studying shortened linear codes shortly. We then briefly recall known general results and prove new ones about shortened linear codes.

A. Orthogonal Arrays From Linear Codes

The objective of this subsection is to introduce a basic result about orthogonal arrays from linear codes. Let N, n, s, t be positive integers with $1 \leq t \leq n$. Let S be a set with s elements. An $N \times n$ array A with entries from S is said to be an orthogonal array with s levels, strength t and index λ if every $N \times t$ subarray of A contains each t-tuple based on S exactly λ times as a row. Such an array is denoted by $\mathrm{OA}(N, n, s, t)$ [5, p. 2].

Lemma 3 [5, p. 2]: Consider an $[n, \kappa, d]$ code $\mathcal{C}$ over $\mathrm{GF}(q)$ with dual distance $d^\perp$. Let A be a $q^\kappa \times n$ matrix whose rows are all the codewords in $\mathcal{C}$. Then A is an $\mathrm{OA}(q^\kappa, n, q, d^\perp - 1)$

A proof of Lemma 3 can be found in [5, p. 66]. Conversely, some orthogonal arrays can be used to construct linear codes.

B. Auxiliary Results About t-Designs

Since t-designs will be used as basic tools for studying shortened codes in this paper, we have to introduce the basics of t-designs [9, Chapter 4]. Let $\mathcal{P}$ be a set of n elements and $\mathcal{B}$ a multiset of b k-subsets of $\mathcal{P}$, where $n \geq 1$, $b \geq 0$ and $1 \leq k \leq n$. Let t be a positive integer satisfying $1 \leq t \leq n$. The ordered pair $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ is called an *incidence structure*, where the incidence relation is the set membership, i.e., an element $P \in \mathcal{P}$ is incident with an element $B \in \mathcal{B}$ if and only if $P \in B$. The ordered pair $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ is called a t-(n, 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*.

When $\mathcal{B} = \emptyset$, i.e., $b = 0$, we put $\lambda = 0$ and call $(\mathcal{P}, \emptyset)$ a t-$(n, k, 0)$ design for any t and k with $1 \leq t \leq n$ and $0 \leq k \leq n$. A t-(n, k, λ) design with $t > k$ must have $\lambda = 0$ and must be the design $(\mathcal{P}, \emptyset)$. These designs are called trivial designs. We will use the following conventions for the ease of description in the sequel. A t-(n, k, λ) design $(\mathcal{P}, \mathcal{B})$ is also said to be trivial if every k-subset of $\mathcal{P}$ is a block.

A t-design is called *simple* if $\mathcal{B}$ does not contain repeated blocks. A t-(n, k, λ) design is called a *Steiner system* and denoted by $S(t, k, n)$ if $t \geq 2$ and $\lambda = 1$. The parameters of a t-(n, k, λ) design satisfy:

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

Consider an $[n, \kappa, d]$ code over $\mathrm{GF}(q)$ with dual distance $d^\perp$. Then $\mathcal{C}$ may induce a t-design under certain conditions, which is formed by the supports of codewords of a fixed Hamming weight in $\mathcal{C}$. Let $\mathcal{P}(\mathcal{C}) = \{0, 1, \ldots, n-1\}$ be the set of the coordinate positions of $\mathcal{C}$, where n is the length of $\mathcal{C}$. For a codeword $\mathbf{c} = (c_0, \ldots, c_{n-1})$ in $\mathcal{C}$, the *support* of $\mathbf{c}$ is denoted by $\mathrm{Supp}(\mathbf{c})$. Let $\mathcal{B}_w(\mathcal{C}) = \frac{1}{q-1}\{\{\mathrm{Supp}(\mathbf{c}) : \mathtt{wt}(\mathbf{c}) = w \text{ and } \mathbf{c} \in \mathcal{C}\}\}$, here and hereafter $\mathtt{wt}(\mathbf{c})$ denotes the Hamming weight of the codeword $\mathbf{c}$, $\{\{\}\}$ is the multiset notation and $\frac{1}{q-1}S$ denotes the multiset obtained after dividing the multiplicity of each element in the multiset S by $q-1$. For some special $\mathcal{C}$, $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ is a t-(n, w, λ) design with b blocks, where

$$b = \frac{1}{q-1}A_w(\mathcal{C}),\ \lambda = \frac{\binom{w}{t}}{(q-1)\binom{n}{t}}A_w(\mathcal{C}). \tag{3}$$

If $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ is a t-design for any $0 \leq w \leq n$, we say that the code $\mathcal{C}$ *supports* t-*designs*. Notice that such a design $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ may have repeated blocks or may be simple or trivial.

The following lemma provides a criterion for guaranteeing a simple block set $\mathcal{B}_k(\mathcal{C})$ [9, Lemma 4.1].

Lemma 4 [9, Lemma 4.1]: Consider an $[n, \kappa, d]$ code over $\mathrm{GF}(q)$ with dual distance $d^\perp$. Let w be the largest integer with $w \leq n$ satisfying

$$w - \left\lfloor \frac{w+q-2}{q-1} \right\rfloor < d.$$

Then there are no repeated blocks in $\mathcal{B}_k(\mathcal{C})$ for any $d \leq k \leq w$. Such a block set is said to be simple.

The following theorem gives a characterization of codes supporting t-designs via the weight distributions of their shortened and punctured codes [26].

Theorem 5 [26, p. 3694]: Consider an $[n, \kappa, d]$ code over $\mathrm{GF}(q)$ with dual distance $d^\perp$. Let t be a positive integer with $0 < t < \min\{d, d^\perp\}$. Then the following statements are equivalent.

(1) $(\mathcal{P}(\mathcal{C}), \mathcal{B}_k(\mathcal{C}))$ is a t-design for any $0 \leq k \leq n$.

(2) $\big(\mathcal{P}(\mathcal{C}^\perp), \mathcal{B}_k(\mathcal{C}^\perp)\big)$ is a t-design for any $0 \leq k \leq n$.

(3) For any $1 \leq t' \leq t$, the weight distribution $(A_k(\mathcal{C}_T))_{k=0}^{n-t'}$ of the shortened code $\mathcal{C}_T$ is independent of the specific choice of the elements in T, where T is any set of t' coordinate positions in $\mathcal{P}(\mathcal{C})$.

(4) For any $1 \leq t' \leq t$, the weight distribution $\big(A_k(\mathcal{C}^T)\big)_{k=0}^{n-t'}$ of the punctured code $\mathcal{C}^T$ is independent of the specific choice of the elements in T, where T is any set of t' coordinate positions in $\mathcal{P}(\mathcal{C})$.

The original Assmus-Mattson theorem was developed in [1]. It can be stated in the following way [26].

Theorem 6 [26, p. 3699]: Consider an $[n, \kappa, d]$ code over $\mathrm{GF}(q)$ with dual distance $d^\perp$. Let t $(1 \leq t < \min\{d, d^\perp\})$ be an integer such that there are at most $d^\perp - t$ weights of $\mathcal{C}$ in the range $\{1, 2, \ldots, n-t\}$. Then the following holds:

- $(\mathcal{P}(\mathcal{C}), \mathcal{B}_k(\mathcal{C}))$ is a simple t-design provided that $A_k(\mathcal{C}) \neq 0$ and $d \leq k \leq w$, where w is defined to be the largest integer satisfying $w \leq n$ and
$$w - \left\lfloor \frac{w+q-2}{q-1} \right\rfloor < d.$$
- $(\mathcal{P}(\mathcal{C}^\perp), \mathcal{B}_k(\mathcal{C}^\perp))$ is a simple t-design provided that $A_k(\mathcal{C}^\perp) \neq 0$ and $d^\perp \leq k \leq w^\perp$, where $w^\perp$ is defined to be the largest integer satisfying $w^\perp \leq n$ and
$$w^\perp - \left\lfloor \frac{w^\perp+q-2}{q-1} \right\rfloor < d^\perp.$$

We will use the Assmus-Mattson theorem to construct several families of 2-designs with some shortened linear codes at the end of this paper. To study some shortened linear codes later, we will use the results about t-designs above as tools.

C. The Trace Representation of Hamming and Simplex Codes

There are different ways to define the Hamming and Simplex codes. We now give a trace construction of the Hamming and Simplex codes. Let α be a primitive element of $\mathrm{GF}(q^m)$ and let ν denote $(q^m - 1)/(q-1)$. Define

$$\Delta_i := \alpha^i \mathrm{GF}(q)^* = \{\alpha^i a : a \in \mathrm{GF}(q)^*\}$$

for all i with $0 \leq i \leq \nu - 1$. By definition, $\{\Delta_i : 0 \leq i \leq \nu - 1\}$ is a partition of $\mathrm{GF}(q^m)^*$. Let i and j be any pair of distinct

elements in the set $\{0, 1, \ldots, \nu-1\}$. Then any $a \in \Delta_i$ and $b \in \Delta_j$ must be linearly independent over $\mathrm{GF}(q)$.

Let $b_i \in \Delta_i$ for each i with $0 \le i \le \nu-1$. Define

$$\mathcal{S}_{(q,m)}(b_0, \ldots, b_{\nu-1}) = \left\{ \left(\mathrm{Tr}_{q^m/q}(ab_i) \right)_{i=0}^{\nu-1} : a \in \mathrm{GF}(q^m) \right\}. \quad (4)$$

Then the set $\mathcal{S}_{(q,m)}(b_0, \ldots, b_{\nu-1})$ defined above is a Simplex code over $\mathrm{GF}(q)$ with parameters $[(q^m-1)/(q-1), m, q^{m-1}]$ and weight enumerator $1 + (q^m-1)z^{q^{m-1}}$. By definition, different choices of the vector $(b_0, \ldots, b_{\nu-1})$ in the set $\Delta_0 \times \cdots \times \Delta_{\nu-1}$ result in monomially-equivalent Simplex codes. Monomially-equivalent codes have the same parameters and same weight enumerator. Hence, up to monomial equivalence, Simplex codes are unique, and are denoted by $\mathcal{S}_{(q,m)}$.

The dual of any Simplex code $\mathcal{S}_{(q,m)}(b_0, \ldots, b_{\nu-1})$ is called a Hamming code, denoted by $\mathcal{H}_{(q,m)}(b_0, \ldots, b_{\nu-1})$. Hence, all the Hamming codes $\mathcal{H}_{(q,m)}(b_0, \ldots, b_{\nu-1})$ are monomially-equivalent and unique up to monomial equivalence. Hence, we denote them by $\mathcal{H}_{(q,m)}$. It is well known that $\mathcal{H}_{(q,m)}$ has parameters $[(q^m-1)/(q-1), (q^m-1)/(q-1)-m, 3]$ (see Section III for a simple proof).

A linear code is called a *s-weight code* if it has s nonzero weights. Some of the shortened codes presented in this paper are one-weight codes. We will need the following lemma later.

Lemma 7 [4, p. 181]: Let $\mathcal{C}'$ be a one-weight linear code over $\mathrm{GF}(q)$ with dual distance at least 2. Then there exists a positive integer t and there exist t Simplex codes $\mathcal{S}_{(q,m)}(b_0^{(i)}, \ldots, b_{\nu-1}^{(i)})$, $1 \le i \le t$, such that $\mathcal{C}'$ is permutation-equivalent to a linear code $\mathcal{C}''$ whose generator matrix is

$$|G_1|G_2|\cdots|G_t|$$

where G_i is a generator matrix $\mathcal{S}_{(q,m)}(b_0^{(i)}, \ldots, b_{\nu-1}^{(i)})$, and $|$ denotes the concatenation of matrices. Furthermore, $d(\mathcal{C}') = 3$ if $t = 1$ and $d(\mathcal{C}') = 2$ if $t \ge 2$.

D. Known General Results About Shortened Linear Codes

The objective of this section is to summarize known general results about shortened linear codes. Some of them will be used to prove new results for shortened linear codes. Under certain conditions, the dimension of a shortened code $\mathcal{C}_T$ is known and is given in the next theorem [19, Theorem 1.5.7].

Theorem 8 [19, Theorem 1.5.7]: Consider an $[n, \kappa, d]$ code over $\mathrm{GF}(q)$ with dual distance $d^\perp$. Let T be any set of t coordinate positions. Let $\mathcal{C}^T$ denote the punctured code of $\mathcal{C}$ in all coordinates on T. Then the following hold.

1) $(\mathcal{C}^\perp)_T = (\mathcal{C}^T)^\perp$ and $(\mathcal{C}^\perp)^T = (\mathcal{C}_T)^\perp$.
2) If $t < d$, then $\mathcal{C}^T$ and $(\mathcal{C}^\perp)_T$ have dimensions κ and $n-t-\kappa$, respectively.
3) If $t = d$ and T is the set of coordinates where a minimum weight codeword is nonzero, then $\mathcal{C}^T$ and $(\mathcal{C}^\perp)_T$ have dimensions $\kappa - 1$ and $n-t-\kappa+1$, respectively.

We will use this theorem to settle the dimension for the case $t < d^\perp$, and will develop a case-specific method to determine the dimension of $\mathcal{C}_T$ for the case $t > d^\perp$ according to the specific design of the original code $\mathcal{C}$. The most difficult task is to determine the minimum distance $d(\mathcal{C}_T)$ of a shortened code $\mathcal{C}_T$.

Let M be a $q^\kappa \times n$ matrix whose rows are all codewords in $\mathcal{C}$, and let M_i be the submatrix of M consisting of the codewords of weight i. A code is *homogeneous* provided that for $0 \le i \le n$, each column of M_i has the same weight. Prange proved the following result [19, p. 271].

Theorem 9 [19, p. 271]: Let $\mathcal{C}$ be a homogeneous code with $d > 1$, and let t_1 be a coordinate position in $\mathcal{C}$. Then for $0 \le i \le n-1$, we have

$$A_i(\mathcal{C}^{\{t_1\}}) = \frac{n-i}{n} A_i(\mathcal{C}) + \frac{i+1}{n} A_{i+1}(\mathcal{C})$$

and

$$A_i(\mathcal{C}_{\{t_1\}}) = \frac{n-i}{n} A_i(\mathcal{C}).$$

It is known that $\mathcal{C}$ is homogeneous if $\mathcal{C}$ has a transitive automorphism group [19, p. 271]. This may be the only known way to decide if a code is homogeneous. Hence, Theorem 9 has very limited applicability. Recently, better results regarding the weight distribution of a shortened code $\mathcal{C}_T$ of special linear codes were developed in [26] and documented below. Recall that the binomial coefficient $\binom{a}{b}$ equals 0 when $a < b$ or $b < 0$.

Theorem 10 [26, p. 3494]: Consider an $[n, \kappa, d]$ code over $\mathrm{GF}(q)$ with dual distance $d^\perp$. Let t be a positive integer with $0 < t < \min\{d, d^\perp\}$. Let T be a set of t coordinate positions in $\mathcal{P}(\mathcal{C})$. Suppose that $(\mathcal{P}(\mathcal{C}), \mathcal{B}_i(\mathcal{C}))$ is a t-design for any i with $d \le i \le n-t$. Then the shortened code $\mathcal{C}_T$ is a linear code of length $n-t$ and dimension $\kappa - t$. The weight distribution $(A_k(\mathcal{C}_T))_{k=0}^{n-t}$ of $\mathcal{C}_T$ is independent of the specific choice of the elements in T. Specifically,

$$A_k(\mathcal{C}_T) = \frac{\binom{k}{t}\binom{n-t}{k}}{\binom{n}{t}\binom{n-t}{k-t}} A_k(\mathcal{C}).$$

Theorem 11 [26, p. 3494]: Consider an $[n, \kappa, d]$ code over $\mathrm{GF}(q)$ with dual distance $d^\perp$. Let t be a positive integer with $0 < t < d^\perp$. Let T be a set of t coordinate positions in $\mathcal{P}(\mathcal{C})$. Suppose that $(\mathcal{P}(\mathcal{C}), \mathcal{B}_i(\mathcal{C}))$ is a t-design for any i with $d \le i \le n$. Then the punctured code $\mathcal{C}^T$ is a linear code of length $n-t$ and dimension κ. The weight distribution $\left(A_k(\mathcal{C}^T)\right)_{k=0}^{n-t}$ of $\mathcal{C}^T$ is independent of the specific choice of the elements in T. Specifically,

$$A_k(\mathcal{C}^T) = \sum_{i=0}^{t} \frac{\binom{n-t}{k}\binom{k+i}{t}\binom{t}{i}}{\binom{n-t}{k-t+i}\binom{n}{t}} A_{k+i}(\mathcal{C}).$$

Theorems 10 and 11 were used as tools to settle the weight distributions of some shortened and punctured codes of two families of binary codes and very good shortened and punctured codes were obtained in [26]. In this paper, we will make use of Theorems 10 and 11 further and settle the parameters and weight distributions of some shortened codes of several families of linear codes. Note that the conditions in Theorems 10 and 11 are very demanding. It is thus not easy to use these two theorems to study shortened and punctured codes.

E. Some New General Results

In this section, we prove two general results. The first one is the following.

Theorem 12: Every linear code $\mathcal{C}$ with minimum distance $d \geq 3$ is a shortened code of $\mathcal{C}(m,q,\alpha)^{\perp}$ for some m, q and α, where α is a generator of $\mathrm{GF}(q)^*$ and $\mathcal{C}(m,q,\alpha)$ was defined in (2).

Proof: By assumption $d \geq 3$. It follows from Theorem 2 that there are m, q and a generator α of $\mathrm{GF}(q)^*$ such that

$$\mathcal{C}^{\perp} = \mathcal{C}(m,q,\alpha)^T,$$

where T is a set of coordinate positions in $\mathcal{C}(m,q,\alpha)$. It then follows from Theorem 8 that

$$\begin{aligned}\mathcal{C}^{\perp} = \mathcal{C}(m,q,\alpha)^T &= ((\mathcal{C}(m,q,\alpha)^{\perp})^{\perp})^T \\ &= ((\mathcal{C}(m,q,\alpha)^{\perp})_T)^{\perp}.\end{aligned}$$

Hence, $\mathcal{C} = (\mathcal{C}(m,q,\alpha)^{\perp})_T$. This completes the proof. □

Corollary 13: Every linear code over $\mathrm{GF}(q)$ with dual distance at least 3 is a punctured code of a Simplex code over $\mathrm{GF}(q)$.

Proof: Let $\mathcal{C}$ be any linear code of length n over $\mathrm{GF}(q)$ with dual distance at least 3. By Theorem 2, there are a positive integer m and a set of integers $\{i_0, i_1, \ldots, i_{n-1}\}$ such that $0 \leq i_0 < i_1 < \ldots < i_{n-1} \leq q^m - 2$ and

$$\mathcal{C} = \{(\mathrm{Tr}_{q^m/q}(a\alpha^{i_j}))_{j=0}^{n-1} : a \in \mathrm{GF}(q^m)\}. \tag{5}$$

Since we assumed that the dual of $\mathcal{C}$ has minimal distance at least 3, $i_{j_1} \bmod (q^m-1)/(q-1)$ and $i_{j_2} \bmod (q^m-1)/(q-1)$ must be different for any pair of distinct j_1 and j_2 in the set $\{0,1,\ldots,n-1\}$. Note that $\alpha^{i_j} \in \Delta_{i_j \bmod q^m-1/(q-1)}$ for each $j \in \{0,1,\ldots,n-1\}$. We then deduce that $\mathcal{C}$ is a punctured code of a Simplex code $\mathcal{S}_{(q,m)}(b_0,\ldots,b_{\nu-1})$ for some $b_i \in \Delta_i$, where each α^{i_j} equals some b_h for each $j \in \{0,1,\ldots,n-1\}$. □

A Direct Proof of Corollary 13: Let $\mathcal{C}$ be any linear code over $\mathrm{GF}(q)$ with length n, dimension m and dual distance at least 3. Since the dual distance of $\mathcal{C}$ is at least 3, we must have $n \leq (q^m-1)/(q-1)$. Let $[\mathbf{g}_1,\ldots,\mathbf{g}_n]$ be a generator matrix of $\mathcal{C}$, where $\mathbf{g}_i$ is a column vector of $\mathrm{GF}(q)^m$. Since the dual distance of $\mathcal{C}$ is at least 3, any two $\mathbf{g}_i$ and $\mathbf{g}_j$ are linearly independent over $\mathrm{GF}(q)$ for $i \neq j$. Consequently, the set $\{\mathbf{g}_1,\ldots,\mathbf{g}_n\}$ can be extended into a set $\{\mathbf{g}_1,\ldots,\mathbf{g}_n,\ldots,\mathbf{g}_{(q^m-1)/(q-1)}\}$, in which any two distinct elements are linearly independent over $\mathrm{GF}(q)$, i.e., it is the point set of the projective space $\mathrm{PG}(m-1,\mathrm{GF}(q))$. Hence, the matrix $[\mathbf{g}_1 \cdots \mathbf{g}_{(q^m-1)/(q-1)}]$ generates a Simplex code $\mathcal{S}_{(q,m)}$. Clearly, $C = (\mathcal{S}_{(q,m)})^T$, where $T = \{n+1,\ldots,(q^m-1)/(q-1)\}$. This completes the proof. □

Corollary 13 shows the importance of the Simplex codes and the puncturing technique.

Theorem 14: Every linear code with minimum distance at least 3 is a shortened code of a Hamming code.

Proof: We follow the notation in the proof of Corollary 13. Let $\mathcal{C}$ be any linear code of length n over $\mathrm{GF}(q)$ with minimum distance at least 3. By Corollary 13, $\mathcal{C}^{\perp}$ is equal to $\big(\mathcal{S}_{(q,m)}(b_0,b_1,\ldots,b_{\nu-1})\big)^T$, where T is a set of some coordinate positions in the Simplex code $\mathcal{S}_{(q,m)}(b_0,b_1,\ldots,b_{\nu-1})$, m is a positive integer, $b_i \in \Delta_i$ for each i with $0 \leq i \leq \nu-1$. By Theorem 8,

$$\begin{aligned}&\big(\mathcal{S}_{(q,m)}(b_0,b_1,\ldots,b_{\nu-1})\big)^T \\ &\quad= \big((\mathcal{H}_{(q,m)}(b_0,b_1,\ldots,b_{\nu-1}))^{\perp}\big)^T \\ &\quad= \big((\mathcal{H}_{(q,m)}(b_0,b_1,\ldots,b_{\nu-1}))_T\big)^{\perp}.\end{aligned}$$

As a result, $\mathcal{C}^{\perp} = \big((\mathcal{H}_{(q,m)}(b_0,b_1,\ldots,b_{\nu-1}))_T\big)^{\perp}$. Their duals are equal. This completes the proof. □

Similar to the direct proof of Corollary 13, one can prove Theorem 14 without using Theorem 8. We omit the details of such a direct proof here. Theorem 14 shows the importance of the Hamming codes and the shortening technique.

Theorem 15: Consider an $[n,\kappa,d]$ code over $\mathrm{GF}(q)$ with dual distance $d^{\perp}$. Let t be an integer with $1 \leq t < \min\{d,d^{\perp}\}$.

(1) For any set $T = \{i_1,i_2,\ldots,i_t\}$ of t coordinate positions, $\mathcal{C}^T$ has length $n-t$, dimension κ and minimum distance at least $d-t$. Furthermore, if $A_d(\mathcal{C}) > q^{\kappa} - q^{\kappa-t}(q-1)^t - 1$ and $t \leq \kappa$, then the minimum distance of $\mathcal{C}^T$ equals $d-t$.

(2) For any set $T = \{i_1,i_2,\ldots,i_t\}$ of t coordinate positions, $(\mathcal{C}_T)^{\perp}$ has length $n-t$, dimension $n-\kappa$ and minimum distance at least $d^{\perp}-t$. Furthermore, if $A_{d^{\perp}}(\mathcal{C}^{\perp}) > q^{n-\kappa} - q^{n-\kappa-t}(q-1)^t - 1$ and $t \leq n-\kappa$, then the minimum distance of $(\mathcal{C}_T)^{\perp}$ equals $d^{\perp}-t$.

Proof: Since $t < d$, the punctured versions of any two distinct codewords in $\mathcal{C}$ are distinct. It then follows that the dimension of $\mathcal{C}^T$ is κ. Clearly, the minimum distance of $\mathcal{C}^T$ is at least $d-t$.

Let M be a $q^{\kappa} \times n$ matrix whose rows are all codewords of $\mathcal{C}$. Since $t < d^{\perp}$, it follows from Lemma 3 that M is an orthogonal array of strength t. Let $S_1(T)$ denote the set of all codewords in $\mathcal{C}$ whose coordinates in T are all nonzero, and define $S_2(T) = \mathcal{C} \setminus S_1(T)$. By definition, $S_1(T)$ and $S_2(T)$ partition $\mathcal{C}$. Since M is an orthogonal array of strength t, $|S_1(T)| = q^{\kappa-t}(q-1)^t$. Consequently, $|S_2(T)| = q^{\kappa} - q^{\kappa-t}(q-1)^t$. Let C_d denote the set of all codewords of weight d in $\mathcal{C}$. Then $S_1(T) \cap C_d$ and $S_2(T) \cap C_d$ partition C_d. Note that $d \geq 1$ and

$$|S_2(T) \cap C_d| \leq |S_2(T)| - 1 = q^{\kappa} - q^{\kappa-t}(q-1)^t - 1.$$

If $A_d(\mathcal{C}) > q^{\kappa} - q^{\kappa-t}(q-1)^t - 1$ and $t \leq \kappa$, then $|S_1(T) \cap C_d| \geq 1$. This means that there is at least one codeword in $\mathcal{C}$ whose coordinates in T are all nonzero. As a result, the punctured version of this codeword has Hamming weight $d-t$. Hence, the minimum distance of $\mathcal{C}^T$ equals $d-t$. This completes the proof of Part (1).

By Theorem 8, we have $(\mathcal{C}_T)^{\perp} = (\mathcal{C}^{\perp})^T$. The desired conclusions in Part (2) then follow from those in Part (1). □

The only new result in Part (1) of Theorem 15 is the last conclusion on the minimum distance of the punctured code $\mathcal{C}^T$. Theorem 15 will be used to determine the parameters of some shortened codes and their duals later.

III. Some Shortened Codes of the Hamming Codes

The trace definition of the Simplex code $\mathcal{S}_{(q,m)}$ and the Hamming code $\mathcal{H}_{(q,m)}$ was given in Section II-C. We now give

the matrix definition of them. A parity check matrix $H_{(q,m)}$ of the *Hamming code* $\mathcal{H}_{(q,m)}$ over $\mathrm{GF}(q)$ is defined by choosing for its columns a nonzero vector from each one-dimensional subspace of $\mathrm{GF}(q)^m$. In terms of finite geometry, the columns of $H_{(q,m)}$ are the points of the projective geometry $\mathrm{PG}(m-1,\mathrm{GF}(q))$ [9, Section 1.8]. Hence $\mathcal{H}_{(q,m)}$ has length $n=(q^m-1)/(q-1)$ and dimension $n-m$. Note that no two columns of $H_{(q,m)}$ are linearly dependent over $\mathrm{GF}(q)$. The minimum weight of $\mathcal{H}_{(q,m)}$ is at least 3. Adding two nonzero vectors from two different one-dimensional subspaces gives a nonzero vector from a third one-dimensional space. Therefore, $\mathcal{H}_{(q,m)}$ has minimum weight 3. It is also well known that any $[(q^m-1)/(q-1),(q^m-1)/(q-1)-m,3]$ code over $\mathrm{GF}(q)$ is monomially equivalent to the Hamming code $\mathcal{H}_{(q,m)}$ [19, Theorem 1.8.2]. The weight distribution of $\mathcal{H}_{(q,m)}$ is given in the following lemma [10].

Lemma 16 [10, p. 2418]: The weight distribution of $\mathcal{H}_{(q,m)}$ is given by

$$q^m A_k(\mathcal{H}_{(q,m)}) = \sum_{\substack{0\le i\le \frac{q^{m-1}-1}{q-1}\\ 0\le j\le q^{m-1}\\ i+j=k}} \left[\binom{\frac{q^{m-1}-1}{q-1}}{i}\binom{q^{m-1}}{j}\Big((q-1)^k + (-1)^j(q-1)^i(q^m-1)\Big)\right]$$

for $0\le k\le (q^m-1)/(q-1)$.

The following lemma was proved in [10] and will be needed later.

Lemma 17 [10, p. 2418]: Let $m\ge 2$. Then $(\mathcal{P}(\mathcal{H}^{\perp}_{(q,m)}),\mathcal{B}_{q^{m-1}}(\mathcal{H}^{\perp}_{(q,m)}))$ is a 2-$((q^m-1)/(q-1),q^{m-1},(q-1)q^{m-2})$ simple design.

Theorem 18: Let $n=(q^m-1)/(q-1)\ge 4$, and let t_1 be any coordinate position in $\mathcal{H}_{(q,m)}$. Then the following hold:

- $(\mathcal{H}_{(q,m)})_{\{t_1\}}$ is an $[n-1,n-m-1,3]$ code over $\mathrm{GF}(q)$ with
$$A_k((\mathcal{H}_{(q,m)})_{\{t_1\}}) = \frac{n-k}{n}A_k(\mathcal{H}_{(q,m)})$$
for $0\le k\le n-1$, where $A_k(\mathcal{H}_{(q,m)})$ was given in Lemma 16.
- $(\mathcal{H}^{\perp}_{(q,m)})_{\{t_1\}}$ is an $[n-1,m-1,q^{m-1}]$ code over $\mathrm{GF}(q)$ with weight enumerator $1+(q^{m-1}-1)z^{q^{m-1}}$.
- $((\mathcal{H}_{(q,m)})_{\{t_1\}})^{\perp}$ is an $[n-1,m,q^{m-1}-1]$ code over $\mathrm{GF}(q)$ with weight enumerator
$$1+(q-1)q^{m-1}z^{q^{m-1}-1}+(q^{m-1}-1)z^{q^{m-1}}.$$
- $((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1\}})^{\perp}$ is an $[n-1,n-m,2]$ code over $\mathrm{GF}(q)$ with weight enumerator
$$\frac{1}{q^{m-1}}\left[(1+(q-1)z)^{n-1}+(q^{m-1}-1)(1-z)^{q^{m-1}}(1+(q-1)z)^{n-1-q^{m-1}}\right].$$

Proof: By Lemma 4, $\mathcal{B}_{q^{m-1}}(\mathcal{H}^{\perp}_{(q,m)})$ does not have repeated blocks. By Lemma 17, the incidence structure $(\mathcal{P}(\mathcal{H}^{\perp}_{(q,m)}),\mathcal{B}_{q^{m-1}}(\mathcal{H}^{\perp}_{(q,m)}))$ is a 2-design. Since the Simplex code $\mathcal{H}^{\perp}_{(q,m)}$ has weight enumerator $1+(q^m-1)z^{q^{m-1}}$, $(\mathcal{P}(\mathcal{H}^{\perp}_{(q,m)}),\mathcal{B}_k(\mathcal{H}^{\perp}_{(q,m)}))$ is the trivial 2-design $(\mathcal{P}(\mathcal{H}^{\perp}_{(q,m)}),\{\emptyset\})$ or $(\mathcal{P}(\mathcal{H}^{\perp}_{(q,m)}),\emptyset)$ for each k with $0\le k\le n$ and $k\ne q^{m-1}$. It then follows from Theorem 5 that $(\mathcal{P}(\mathcal{H}_{(q,m)}),\mathcal{B}_k(\mathcal{H}_{(q,m)}))$ is a 2-design for each k with $0\le k\le n$. The desired conclusions on $(\mathcal{H}_{(q,m)})_{\{t_1\}}$ and $(\mathcal{H}^{\perp}_{(q,m)})_{\{t_1\}}$ then follow from Theorem 10 and Lemma 16. In particular,

$$A_3((\mathcal{H}_{(q,m)})_{\{t_1\}}) = \frac{n-3}{n}A_3(\mathcal{H}_{(q,m)}) > 0.$$

Hence, $d((\mathcal{H}_{(q,m)})_{\{t_1\}})=3$.

It follows from Theorems 8 and 11 that

$$\begin{aligned} &A_k(((\mathcal{H}_{(q,m)})_{\{t_1\}})^{\perp}) \\ &\quad= A_k(((\mathcal{H}_{(q,m)})^{\perp})^{\{t_1\}}) \\ &\quad= \sum_{i=0}^{1}\frac{\binom{n-1}{k}\binom{k+i}{1}\binom{1}{i}}{\binom{n-1}{k-1+i}\binom{n}{1}}A_{k+i}((\mathcal{H}_{(q,m)})^{\perp}). \end{aligned} \tag{6}$$

Notice that $(\mathcal{H}_{(q,m)})^{\perp}$ has weight enumerator $1+(q^m-1)z^{q^{m-1}}$. Combining this with (6), we deduce that $A_k(((\mathcal{H}_{(q,m)})_{\{t_1\}})^{\perp})=0$ for all $k\notin\{0,q^{m-1}-1,q^{m-1}\}$ and

$$A_{q^{m-1}-1}(((\mathcal{H}_{(q,m)})_{\{t_1\}})^{\perp}) = (q-1)q^{m-1}$$

and

$$A_{q^{m-1}}(((\mathcal{H}_{(q,m)})_{\{t_1\}})^{\perp}) = q^{m-1}-1.$$

This completes the proof of the desired conclusions on $((\mathcal{H}_{(q,m)})_{\{t_1\}})^{\perp}$.

Finally, we prove the conclusions on the code $((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1\}})^{\perp}$. Note that the weight enumerator of $((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1\}})^{\perp}$ is $1+(q^{m-1}-1)z^{q^{m-1}}$. The desired weight enumerator in (6) then follows from the MacWilliams identity [9, p. 65]. It is easily verified that the coefficient of z in the polynomial in (6) equals 0, and the coefficient of z^2 is

$$\begin{aligned} &\frac{\binom{n-1}{2}(q-1)^2+(q^{m-1}-1)[\binom{q^{m-1}}{2}+\binom{n-1-q^{m-1}}{2}(q-1)^2]}{q^{m-1}} \\ &\quad -(q^{m-1}-1)(q-1)(n-1-q^{m-1}) \\ &\quad = \frac{q(q-1)(q^{m-1}-1)}{2} > 0. \end{aligned}$$

Consequently, $((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1\}})^{\perp}$ has minimum weight 2. It also follows from Lemma 7 that the code $((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1\}})^{\perp}$ has minimum distance 2. □

We have the following remarks on the two shortened codes in Theorem 18 and their duals.

- It is known that the automorphism group of the Hamming code $(\mathcal{H}_{(q,m)})$ is transitive. Hence, the weight distribution of $(\mathcal{H}_{(q,m)})_{\{t_1\}}$ can also be derived from Theorem 9 and was known. Our approach to the determination of the weight distribution of $(\mathcal{H}_{(q,m)})_{\{t_1\}}$ is different. The weight distribution of the binary code $(\mathcal{H}_{(2,m)})_{\{t_1\}}$ was also pointed out in the proof of the corollary of Theorem 5.1 in [2]. The dimension of $(\mathcal{H}_{(q,m)})_{\{t_1\}}$ follows directly from Theorem 8, and was also pointed out in Proposition 4.5 in [2], [6].

- It follows from Proposition 4.5 in [6] and Theorem 18 that the shortened code $(\mathcal{H}_{(q,m)})_{\{t_1\}}$ is dimension-optimal.
- Let $n \geq 7$ and $m \geq 2$. Then the shortened code $(\mathcal{H}_{(q,m)})_{\{t_1\}}$ is length-optimal with respect to the sphere-packing bound. $(\mathcal{H}^{\perp}_{(q,m)})_{\{t_1\}}$ and its dual both meet the Griesmer bound.
- The code $((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1\}})^{\perp}$ is distance-optimal with respect to the sphere-packing bound, and is MDS when $m = 2$. Note that $((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1\}})^{\perp} = (\mathcal{H}_{(q,m)})^{\{t_1\}}$, which is a punctured Hamming code.

Theorem 19: Let $n = (q^m-1)/(q-1) \geq 6$, $m \geq 2$, and let t_1 and t_2 be any two distinct coordinate positions in $\mathcal{H}_{(q,m)}$. Then the following hold:

1) $(\mathcal{H}_{(q,m)})_{\{t_1,t_2\}}$ is an $[n-2, n-m-2, 3]$ code over $\mathrm{GF}(q)$ with
$$A_k((\mathcal{H}_{(q,m)})_{\{t_1,t_2\}}) = \frac{\binom{k}{2}\binom{n-2}{k}}{\binom{n}{2}\binom{n-2}{k-2}} A_k(\mathcal{H}_{(q,m)})$$
for $0 \leq k \leq n-2$, where $A_k(\mathcal{H}_{(q,m)})$ was given in Lemma 16.
2) $(\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}$ is an $[n-2, m-2, q^{m-1}]$ code over $\mathrm{GF}(q)$ with weight enumerator $1 + (q^{m-2}-1)z^{q^{m-1}}$.
3) $((\mathcal{H}_{(q,m)})_{\{t_1,t_2\}})^{\perp}$ is an $[n-2, m, q^{m-1}-2]$ code over $\mathrm{GF}(q)$ with weight enumerator
$$1 + (q-1)^2 q^{m-2} z^{q^{m-1}-2} + 2(q-1)q^{m-2} z^{q^{m-1}-1} + (q^{m-2}-1)z^{q^{m-1}}.$$
4) $\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^{\perp}$ has parameters $[n-2, n-m, 1]$ and weight enumerator
$$\frac{1}{q^{m-2}}\left[(1+(q-1)z)^{n-2} + (q^{m-2}-1)(1-z)^{q^{m-1}}(1+(q-1)z)^{n-2-q^{m-1}}\right].$$
In particular,
$$A_1\left(\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^{\perp}\right) = (q-1)^2. \tag{7}$$

Proof: By Lemma 4, $\mathcal{B}_{q^{m-1}}(\mathcal{H}^{\perp}_{(q,m)})$ does not have repeated blocks. Lemma 17 tells us that the incidence structure $(\mathcal{P}(\mathcal{H}^{\perp}_{(q,m)}), \mathcal{B}_{q^{m-1}}(\mathcal{H}^{\perp}_{(q,m)}))$ is a 2-design. Since the Simplex code $\mathcal{H}^{\perp}_{(q,m)}$ has weight enumerator $1 + (q^m - 1)z^{q^{m-1}}$, $(\mathcal{P}(\mathcal{H}^{\perp}_{(q,m)}), \mathcal{B}_k(\mathcal{H}^{\perp}_{(q,m)}))$ is the trivial 2-design $(\mathcal{P}(\mathcal{H}^{\perp}_{(q,m)}), \{\emptyset\})$ or $(\mathcal{P}(\mathcal{H}^{\perp}_{(q,m)}), \emptyset)$ for each k with $0 \leq k \leq n$ and $k \neq q^{m-1}$. It then follows from Theorem 5 that $(\mathcal{P}(\mathcal{H}_{(q,m)}), \mathcal{B}_k(\mathcal{H}_{(q,m)}))$ is a 2-design for each k with $0 \leq k \leq n$. The desired conclusions on $(\mathcal{H}_{(q,m)})_{\{t_1,t_2\}}$ and $(\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}$ then follow from Theorem 10 and Lemma 16. In particular,
$$A_3((\mathcal{H}_{(q,m)})_{\{t_1,t_2\}}) = \frac{\binom{3}{2}\binom{n-2}{3}}{\binom{n}{2}\binom{n-2}{3-2}} A_3(\mathcal{H}_{(q,m)}) > 0.$$
Consequently,
$$d((\mathcal{H}_{(q,m)})_{\{t_1,t_2\}}) = 3.$$

It follows from Theorems 8 and 11 that
$$\begin{aligned} A_k(((\mathcal{H}_{(q,m)})_{\{t_1,t_2\}})^{\perp}) &= A_k(((\mathcal{H}_{(q,m)})^{\perp})^{\{t_1,t_2\}}) \\ &= \sum_{i=0}^{2} \frac{\binom{n-2}{k}\binom{k+i}{2}\binom{2}{i}}{\binom{n-2}{k-2+i}\binom{n}{2}} A_{k+i}((\mathcal{H}_{(q,m)})^{\perp}). \end{aligned} \tag{8}$$

Notice that $(\mathcal{H}_{(q,m)})^{\perp}$ has weight enumerator $1 + (q^m-1)z^{q^{m-1}}$. Combining this with (8), we deduce that $A_k(((\mathcal{H}_{(q,m)})_{\{t_1,t_2\}})^{\perp}) = 0$ for all $k \notin \{0, q^{m-1}-2, q^{m-1}-1, q^{m-1}\}$ and
$$\begin{aligned} A_{q^{m-1}-2}(((\mathcal{H}_{(q,m)})_{\{t_1,t_2\}})^{\perp}) &= (q-1)^2 q^{m-2}, \\ A_{q^{m-1}-1}(((\mathcal{H}_{(q,m)})_{\{t_1,t_2\}})^{\perp}) &= 2(q-1)q^{m-2}, \\ A_{q^{m-1}}(((\mathcal{H}_{(q,m)})_{\{t_1,t_2\}})^{\perp}) &= q^{m-2}-1. \end{aligned}$$
This completes the proof of the desired conclusions on $((\mathcal{H}_{(q,m)})_{\{t_1,t_2\}})^{\perp}$.

Recall that the weight enumerator of $(\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}$ is $1 + (q^{m-2}-1)z^{q^{m-1}}$. It then follows from the MacWilliam Identity that the weight enumerator of $\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^{\perp}$ is
$$\begin{aligned} &\frac{(1+(q-1)z)^{n-2}\left(1 + (q^{m-2}-1)\left(\frac{1-z}{1+(q-1)z}\right)^{q^{m-1}}\right)}{q^{m-2}} \\ &= \frac{(1+(q-1)z)^{n-2}}{q^{m-2}} + \\ &\quad \frac{(q^{m-2}-1)(1-z)^{q^{m-1}}(1+(q-1)z)^{n-2-q^{m-1}}}{q^{m-2}}. \end{aligned} \tag{9}$$

We have obviously
$$\begin{aligned} (1+(q-1)z)^{n-2} &= 1 + (n-2)(q-1)z + \cdots, \\ (1-z)^{q^{m-1}} &= 1 - q^{m-1}z + \cdots, \\ (1+(q-1)z)^{n-2-q^{m-1}} &= \\ &\quad 1 + (n - q^{m-1} - 2)(q-1) + \cdots. \end{aligned}$$

Consequently, the coefficient of the term z in the polynomial of (9) is given by
$$\begin{aligned} &\frac{(n-2)(q-1)}{q^{m-2}} + \\ &\frac{(q^{m-2}-1)\left((n-q^{m-1}-2)(q-1) - q^{m-1}\right)}{q^{m-2}} \\ &= (q-1)^2. \end{aligned}$$
The desired conclusion on $A_1\left(\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^{\perp}\right)$ then follows. □

The reader is informed that the weight distribution of some binary code $(\mathcal{H}_{(2,m)})_{\{t_1,t_2\}}$ was pointed out in the proof of the corollary of Theorem 5.1 in [2]. Let $n \geq 7$ and $m \geq 2$. Then the shortened code $(\mathcal{H}_{(q,m)})_{\{t_1,t_2\}}$ is both length-optimal and dimension-optimal with respect to the sphere-packing bound. The code $((\mathcal{H}_{(q,m)})_{\{t_1,t_2\}})^{\perp}$ is MDS when $m = 2$, and meets the Griesmer bound when $q > 2$. Numerical data by Magma shows that $(\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}$ is distance-optimal in many cases. However, the following theorem shows that $(\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}$ is

not length-optimal, and can be further punctured into a much better code for every pair of distinct t_1 and t_2.

Theorem 20: Let $n = (q^m - 1)/(q - 1) \geq 6$, $m \geq 3$, and let t_1 and t_2 be any two distinct coordinate positions in $\mathcal{H}_{(q,m)}$. Then there is a set T of $q - 1$ coordinate positions in $(\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}$ such that the punctured code $\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T$ has parameters $[n - 1 - q, m - 2, q^{m-1}]$ and weight enumerator $1 + (q^{m-2} - 1)z^{q^{m-1}}$. Furthermore, the code $\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T$ meets the Griesmer bound. The dual code $\left(\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T\right)^{\perp}$ has parameters $[n - 1 - q, n + 1 - q - m, 2]$.

Proof: By Theorem 19,

$$A_1\left(\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^{\perp}\right) = (q-1)^2.$$

Hence, there is a set $T = \{t_1, \cdots, t_{q-1}\}$ of $q-1$ coordinate positions in $(\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}$ such that

$$c_{t_1} = c_{t_2} = \cdots = c_{t_{q-1}} = 0$$

for all codewords $c = (c_1, c_2, \cdots, c_{n-2}) \in (\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}$. Consequently, the desired conclusions on the parameters and weight enumerator of the code $\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T$ follow from those of $(\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}$. Note that

$$\sum_{i=0}^{m-3} \left\lceil \frac{q^{m-1}}{q^i} \right\rceil = n - 1 - q.$$

We conclude that the code $\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T$ meets the Griesmer bound.

By the definition of $\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T$, any column of any generator matrix of $\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T$ is not the zero vector. Consequently, the minimum distance of $\left(\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T\right)^{\perp}$ is at least 2. It follows from the sphere-packing bound that the minimum distance of $\left(\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T\right)^{\perp}$ is at most 2. Consequently,

$$d\left(\left(\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T\right)^{\perp}\right) = 2.$$

Note that $\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T$ is a one-weight code. It also follows from Lemma 7 that the code $\left(\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T\right)^{\perp}$ has minimum distance 2. □

The code $\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^{\perp}$ documented in Theorem 19 has parameters $[n - 2, n - m, 1]$ and is not interesting in terms of its error-correcting capability. However, Theorem 20 demonstrates that information about this code can be used to puncture its dual code $(\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}$ and obtain the optimal code $\left((\mathcal{H}^{\perp}_{(q,m)})_{\{t_1,t_2\}}\right)^T$. Therefore, studying linear codes with minimum distance 1 and the structure of the minimum weight codewords with weight 1 is valuable. We inform that the trace codes over $\mathrm{GF}(r)$ of one-weight codes over $\mathrm{GF}(r^m)$ with the same parameters may have different dimensions or minimum distances. Hence, one-weight codes can be used to construct new codes over smaller fields and are thus interesting. The reader is also informed that the parameters of some shortened Hamming codes were also discussed in [20].

IV. Some Shortened Codes of the Reed-Muller Codes

Our task in this section is to study some shortened codes of some binary Reed-Muller codes. Reed-Muller codes can be defined by either the univariate or the multivariate approach. Each approach has advantages and disadvantages. We briefly recall the univariate definition below. Let m be a positive integer. Any function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$ is called a (univariate) Boolean function. Let $\mathbf{B}_m$ denote the set of all Boolean functions on $\mathrm{GF}(2^m)$. Every nonzero Boolean function f on $\mathrm{GF}(2^m)$ can be uniquely expressed as

$$f(x) = \sum_{i=0}^{2^m-1} f_i x^i, \tag{10}$$

where $f_i \in \mathrm{GF}(2^m)$. Every integer i with $0 \leq i \leq 2^m - 1$ has the unique 2-adic expansion $i = \sum_{j=0}^{m-1} i_j 2^j$, where $i_j \in \{0, 1\}$. The 2-weight of i is defined to be the Hamming weight of $(i_0, i_1, \ldots, i_{m-1})$. The algebraic degree of a Boolean function f on $\mathrm{GF}(2^m)$ defined in (10), denoted by $\deg(f)$, is defined to be the maximum 2-weight of all i such that $f_i \neq 0$.

Let α be a generator of $\mathrm{GF}(2^m)^*$. Define $P_0 = 0$ and $P_i = \alpha^{i-1}$ for $1 \leq i \leq 2^m - 1$. The Reed-Muller code of length 2^m and order r is defined by

$$\mathcal{R}(r, m) = \{(f(P_0), \ldots, f(P_{2^m-1})) : f \in \mathbf{B}_m, \deg(f) \leq r\}.$$

The reader is referred to [9, Chapter 5] and [23, Chapter 13] for detailed information on the Reed-Muller code. The following are well known:

- $\mathcal{R}(r, m)^{\perp} = \mathcal{R}(m - 1 - r, m)$.
- $\mathcal{R}(1, m)$ has parameters $[2^m, m + 1, 2^{m-1}]$ and weight enumerator $1 + (2^{m+1} - 2)z^{2^{m-1}} + z^{2^m}$.
- $\mathcal{R}(m - 2, m)$ has parameters $[2^m, 2^m - m - 1, 4]$.

Our objective in this section is to study some shortened codes of $\mathcal{R}(1, m)$ and $\mathcal{R}(m-2, m)$ and their duals. As before, we are only interested in optimal codes, almost-optimal codes and codes meeting a bound for linear codes. The first result of this section is the following.

Theorem 21: Let $m \geq 3$, and let t_1 be any coordinate position in $\mathcal{R}(1, m)$. Then the following hold.

1) $\mathcal{R}(1, m)_{\{t_1\}}$ is a $[2^m - 1, m, 2^{m-1}]$ binary code with weight enumerator $1 + (2^m - 1)z^{2^{m-1}}$, and is permutation-equivalent to a binary Simplex code. The code meets the Griesmer bound.
2) $(\mathcal{R}(1, m)_{\{t_1\}})^{\perp}$ is a $[2^m - 1, 2^m - m - 1, 3]$ binary code, and is permutation-equivalent to a binary Hamming code. The code meets the sphere-packing bound.

3) $\mathcal{R}(m-2,m)_{\{t_1\}}$ is a $[2^m-1, 2^m-m-2, 4]$ binary code. The code is distance-optimal with respect to the sphere-packing bound.
4) $(\mathcal{R}(m-2,m)_{\{t_1\}})^{\perp}$ is a $[2^m-1, m+1, 2^{m-1}-1]$ binary code with weight enumerator

$$1+(2^m-1)z^{2^{m-1}-1}+(2^m-1)z^{2^{m-1}}+z^{2^m-1}.$$

This code meets the Griesmer bound.

Proof: Recall that $\mathcal{R}(1,m)$ has parameters $[2^m, m+1, 2^{m-1}]$ and weight enumerator $1+(2^{m+1}-2)z^{2^{m-1}}+z^{2^m}$. By Theorem 8, $\mathcal{R}(1,m)_{\{t_1\}}$ has length 2^m-1 and dimension m. The weight enumerator of $\mathcal{R}(1,m)$ tells us that every codeword other than the zero codeword and the all-1 codeword in $\mathcal{R}(1,m)$ has weight 2^{m-1}. As a result, every nonzero codeword in $\mathcal{R}(1,m)_{\{t_1\}}$ has weight 2^{m-1}. Hence, $\mathcal{R}(1,m)_{\{t_1\}}$ is a $[2^m-1, m, 2^{m-1}]$ binary code with weight enumerator $1+(2^m-1)z^{2^{m-1}}$. It follows from Lemma 7 that $\mathcal{R}(1,m)_{\{t_1\}}$ is permutation-equivalent to a binary Simplex code. Consequently, $(\mathcal{R}(1,m)_{\{t_1\}})^{\perp}$ is permutation-equivalent to a binary Hamming code. This completes the proof of the conclusions in Part 1) and Part 2).

By Theorem 8,

$$(\mathcal{R}(m-2,m)_{\{t_1\}})^{\perp}=((\mathcal{R}(1,m)^{\perp})_{\{t_1\}})^{\perp}=\mathcal{R}(1,m)^{\{t_1\}}.$$

It follows from Theorem 8 that $\mathcal{R}(1,m)$ has dimension $m+1$. Let M denote a $2^{m+1}\times 2^m$ matrix consisting of all the codewords of $\mathcal{R}(1,m)$ as row vectors. Since $\mathcal{R}(m-2,m)$ has minimum distance 4, it follows from Lemma 3 that the matrix M is an orthogonal array with strength 3. Every column vector of M has the same number of 1's and 0's. The conclusion on the weight distribution of $(\mathcal{R}(m-2,m)_{\{t_1\}})^{\perp}$ then follows. The dimension of $\mathcal{R}(m-2,m)_{\{t_1\}}$ follows from that of $(\mathcal{R}(m-2,m)_{\{t_1\}})^{\perp}$. It follows from the sphere-packing bound that $d(\mathcal{R}(m-2,m)_{\{t_1\}})\le 4$. Recall that $d(\mathcal{R}(m-2,m))=4$. By the definition of shortened codes, $d(\mathcal{R}(m-2,m)_{\{t_1\}})\ge 4$. Consequently, $d(\mathcal{R}(m-2,m)_{\{t_1\}})=4$. This completes the proof. □

Theorem 22: Let $m\ge 3$, and let t_1 and t_2 be two distinct coordinate positions in $\mathcal{R}(m-2,m)$. Then the following hold.

1) $\mathcal{R}(1,m)_{\{t_1,t_2\}}$ is a $[2^m-2, m-1, 2^{m-1}]$ binary code with weight enumerator

$$1+(2^{m-1}-1)z^{2^{m-1}}.$$

This code meets the Griesmer bound.
2) $(\mathcal{R}(1,m)_{\{t_1,t_2\}})^{\perp}$ is a $[2^m-2, 2^m-m-1, 2]$ binary code, and is distance-optimal with respect to the sphere-packing bound.
3) $\mathcal{R}(m-2,m)_{\{t_1,t_2\}}$ is a $[2^m-2, 2^m-m-3, 4]$ binary code and is distance-optimal with respect to the sphere-packing bound.
4) $(\mathcal{R}(m-2,m)_{\{t_1,t_2\}})^{\perp}$ is a $[2^m-2, m+1, 2^{m-1}-2]$ binary code with weight enumerator

$$1+(2^{m-1}-1)z^{2^{m-1}-2}+2^m z^{2^{m-1}-1}+(2^{m-1}-1)z^{2^{m-1}}+z^{2^m-2}.$$

This code meets the Griesmer bound.

Proof: By Part 1) of Theorem 21, $\mathcal{R}(1,m)_{\{t_1,t_2\}}$ is permutation-equivalent to a shortened code $\left(\mathcal{S}_{(2,m)}\right)_{\{t\}}$ of the Simplex code, where t is a coordinate position in $\mathcal{S}_{(2,m)}$. By the second part of Theorem 18, $\mathcal{R}(1,m)_{\{t_1,t_2\}}$ is a $[2^m-2, m-1, 2^{m-1}]$ binary code with weight enumerator $1+(2^{m-1}-1)z^{2^{m-1}}$. It is easily verified that $\mathcal{R}(1,m)_{\{t_1,t_2\}}$ meets the Griesmer bound. This completes the proof of Part 1).

Note that $(\mathcal{R}(1,m)_{\{t_1,t_2\}})^{\perp}$ is permutation-equivalent to $\left(\left(\mathcal{S}_{(2,m)}\right)_{\{t\}}\right)^{\perp}$. The desired conclusion then follows from the fourth part of Theorem 18.

By Theorem 8,

$$(\mathcal{R}(m-2,m)_{\{t_1,t_2\}})^{\perp}=\mathcal{R}(1,m)^{\{t_1,t_2\}}.$$

Recall that $d(\mathcal{R}(1,m))=2^{m-1}\ge 4$ and $d(\mathcal{R}(m-2,m))=4$. It then follows from Theorem 8 that $\dim(\mathcal{R}(1,m)^{\{t_1,t_2\}})=\dim(\mathcal{R}(1,m))=m+1$. Recall that $\mathcal{R}(1,m)$ has parameters $[2^m, m+1, 2^{m-1}]$ and weight enumerator $1+(2^{m+1}-2)z^{2^{m-1}}+z^{2^m}$. We then deduce that

$$\begin{aligned}
&A_0(\mathcal{R}(1,m)^{\{t_1,t_2\}})=A_0(\mathcal{R}(1,m))=1,\\
&A_{2^{m-1}}(\mathcal{R}(1,m)^{\{t_1,t_2\}})\\
&\quad=N_{(i_1,i_2)}(0,0)-1=2^{m-1}-1,\\
&A_{2^{m-1}-1}(\mathcal{R}(1,m)^{\{t_1,t_2\}})\\
&\quad=N_{(i_1,i_2)}(0,1)+N_{(i_1,i_2)}(1,0)\\
&\quad=2^m,\\
&A_{2^{m-1}-2}(\mathcal{R}(1,m)^{\{t_1,t_2\}})\\
&\quad=N_{(i_1,i_2)}(1,1)-1=2^{m-1}-1,\\
&A_{2^m-2}(\mathcal{R}(1,m)^{\{t_1,t_2\}})=A_{2^m}(\mathcal{R}(1,m))=1,
\end{aligned}$$

and $A_k(\mathcal{R}(1,m)^{\{t_1,t_2\}})=0$ for all $k\notin\{0, 2^{m-1}-2, 2^{m-1}-1, 2^{m-1}, 2^m-2\}$. Note that

$$\sum_{i=0}^{m}\left\lceil\frac{2^{m-1}-2}{2^i}\right\rceil=2^m-2.$$

This means that the code $(\mathcal{R}(m-2,m)_{\{t_1,t_2\}})^{\perp}$ meets the Griesmer bound. This completes the proof of Part 4).

Clearly, we have

$$\begin{aligned}
&\dim(\mathcal{R}(m-2,m)_{\{t_1,t_2\}})\\
&\quad=\ 2^m-2-\dim((\mathcal{R}(m-2,m)_{\{t_1,t_2\}})^{\perp})\\
&\quad=\ 2^m-m-3.
\end{aligned}$$

Note that $d(\mathcal{R}(m-2,m))=4$. By the definition of shortened codes, $d(\mathcal{R}(m-2,m)_{\{t_1,t_2\}})\ge 4$. It follows from the sphere-packing bound that $d(\mathcal{R}(m-2,m)_{\{t_1,t_2\}})\le 4$. Consequently, $d(\mathcal{R}(m-2,m)_{\{t_1,t_2\}})=4$. This completes the proof of Part 3). □

Note that all the codes in Theorems 21 and 22 are either distance-optimal, or dimension-optimal, or distance-almost-optimal or dimension-almost-optimal. We have also the following.

Theorem 23: Let $m\ge 3$, and let t_1, t_2 and t_3 be three pairwise distinct coordinate positions in $\mathcal{R}(m-2,m)$. Then the following hold.

1) $(\mathcal{R}(m-2,m)_{\{t_1,t_2,t_3\}})^{\perp}$ is a $[2^m-3, m+1, 2^{m-1}-3]$ binary code with weight enumerator

$$1+(2^{m-2}-1)z^{2^{m-1}-3}+3\times 2^{m-2}z^{2^{m-1}-2}+ 3\times 2^{m-2}z^{2^{m-1}-1}+(2^{m-2}-1)z^{2^{m-1}}+z^{2^m-3}.$$

This code almost meets the Griesmer bound.

2) $\mathcal{R}(m-2,m)_{\{t_1,t_2,t_3\}}$ is a $[2^m-3, 2^m-m-4, 4]$ binary code and is distance-optimal with respect to the sphere-packing bound.

Proof: By Theorem 8, we have

$$(\mathcal{R}(m-2,m)_{\{t_1,t_2,t_3\}})^{\perp}=\mathcal{R}(1,m)^{\{t_1,t_2,t_3\}}. \tag{11}$$

Recall that $d(\mathcal{R}(1,m))=2^{m-1}\geq 4$ and $d(\mathcal{R}(m-2,m))=4$. It then follows from Theorem 8 that

$$\begin{aligned}&\dim((\mathcal{R}(m-2,m)_{\{t_1,t_2,t_3\}})^{\perp})\\ &=\dim(\mathcal{R}(1,m)^{\{t_1,t_2,t_3\}})\\ &=\dim(\mathcal{R}(1,m))=m+1.\end{aligned}$$

Let M denote a $2^{m+1}\times 2^m$ matrix consisting of all the codewords of $\mathcal{R}(1,m)$ as row vectors. Since $\mathcal{R}(m-2,m)$ has minimum distance 4, it follows from Lemma 3 that the matrix M is an orthogonal array with strength 3. Let $N_{(i_1,i_2,i_3)}(u,v,h)$ denote the number of codewords $c=(c_0,c_1,\ldots,c_{2^m-1})$ in $\mathcal{R}(1,m)$ such that $c_{i_1}=u$ and $c_{i_2}=v$ and $c_{i_3}=h$. Since M is an orthogonal array with strength 3, we have $N_{(i_1,i_2,i_3)}(u,v,h)=2^{m-2}$ for each $(u,v,h)\in \mathrm{GF}(2)^3$. Recall that $\mathcal{R}(1,m)$ has parameters $[2^m,m+1,2^{m-1}]$ and weight enumerator $1+(2^{m+1}-2)z^{2^{m-1}}+z^{2^m}$. We then deduce that

$$\begin{aligned}&A_0(\mathcal{R}(1,m)^{\{t_1,t_2,t_3\}})=A_0(\mathcal{R}(1,m))=1,\\ &A_{2^{m-1}-3}(\mathcal{R}(1,m)^{\{t_1,t_2,t_3\}})\\ &\quad=\ N_{(i_1,i_2,i_3)}(1,1,1)-1=2^{m-2}-1,\\ &A_{2^{m-1}-2}(\mathcal{R}(1,m)^{\{t_1,t_2,t_3\}})\\ &\quad=\ N_{(i_1,i_2,i_3)}(0,1,1)+N_{(i_1,i_2,i_3)}(1,0,1)+\\ &\qquad N_{(i_1,i_2,i_3)}(1,1,0)\\ &\quad=\ 3\times 2^{m-2},\\ &A_{2^{m-1}-1}(\mathcal{R}(1,m)^{\{t_1,t_2,t_3\}})\\ &\quad=\ N_{(i_1,i_2,i_3)}(0,0,1)+N_{(i_1,i_2,i_3)}(0,1,0)+\\ &\qquad N_{(i_1,i_2,i_3)}(1,0,0)\\ &\quad=\ 3\times 2^{m-2},\\ &A_{2^{m-1}}(\mathcal{R}(1,m)^{\{t_1,t_2,t_3\}})\\ &\quad=\ N_{(i_1,i_2,i_3)}(0,0,0)-1=2^{m-2}-1,\\ &A_{2^m-3}(\mathcal{R}(1,m)^{\{t_1,t_2,t_3\}})=A_{2^m}(\mathcal{R}(1,m))=1,\end{aligned}$$

and $A_k(\mathcal{R}(1,m)^{\{t_1,t_2,t_3\}})=0$ for all k that are not in the set

$$\{0,2^{m-1}-3,2^{m-1}-2,2^{m-1}-1,2^{m-1},2^m-3\}.$$

This proved the desired weight enumerator of the binary code $(\mathcal{R}(m-2,m)_{\{t_1,t_2,t_3\}})^{\perp}$. Note that

$$\sum_{i=0}^{m}\left\lceil\frac{2^{m-1}-3}{2^i}\right\rceil=2^m-4.$$

This means that the code $(\mathcal{R}(m-2,m)_{\{t_1,t_2,t_3\}})^{\perp}$ almost meets the Griesmer bound. This completes the proof of Part 1).

It is straightforward that

$$\begin{aligned}&\dim(\mathcal{R}(m-2,m)_{\{t_1,t_2,t_3\}})\\ &\quad=2^m-3-\dim((\mathcal{R}(m-2,m)_{\{t_1,t_2,t_3\}})^{\perp})\\ &\quad=2^m-m-4.\end{aligned}$$

Note that $d(\mathcal{R}(m-2,m))=4$. By the definition of shortened codes, $d(\mathcal{R}(m-2,m)_{\{t_1,t_2,t_3\}})\geq 4$. It follows from the sphere-packing bound that $d(\mathcal{R}(m-2,m)_{\{t_1,t_2,t_3\}})\leq 4$. Consequently, $d(\mathcal{R}(m-2,m)_{\{t_1,t_2,t_3\}})=4$. This completes the proof of Part 2). □

At the end of this section, we remark that Theorems 21, 22 and 23 can be proved in another way. Note that $\mathcal{B}_{2^m}(\mathcal{R}(1,m))=\{\mathcal{P}(\mathcal{R}(1,m))\}$. It is easily seen that $(\mathcal{P}(\mathcal{R}(1,m)),\mathcal{B}_{2^m}(\mathcal{R}(1,m)))$ is a 3-$(2^m,2^m,1)$ simple design. It is well known that $(\mathcal{P}(\mathcal{R}(1,m)),\mathcal{B}_{2^{m-1}}(\mathcal{R}(1,m)))$ is a 3-$(2^m,2^{m-1},2^{m-2}-1)$ simple design [9, p. 143]. Clearly, $(\mathcal{P}(\mathcal{R}(1,m)),\mathcal{B}_k(\mathcal{R}(1,m)))$ is the trivial 3-design $(\mathcal{P}(\mathcal{R}(1,m)),\{\emptyset\})$ or $(\mathcal{P}(\mathcal{R}(1,m)),\emptyset)$ for all $k\notin\{2^{m-1},2^m\}$. It then follows from Theorem 5 that $(\mathcal{P}(\mathcal{R}(1,m)^{\perp}),\mathcal{B}_k(\mathcal{R}(1,m)^{\perp}))$ is a 3-design for all k with $0\leq k\leq 2^m$. One can also apply Theorems 8, 10 and 11 to prove Theorems 21, 22 and 23.

V. Some Shortened Codes of the Ovoid Codes

In the projective space $\mathrm{PG}(3,\mathrm{GF}(q))$ with $q>2$, an *ovoid* $\mathcal{V}$ is a set of q^2+1 points such that no three of them are collinear (i.e., on the same line) [9, Chapter 13]. Two ovoids are said to be *equivalent* if there is a collineation (i.e., automorphism) of $\mathrm{PG}(3,\mathrm{GF}(q))$ that sends one to the other.

A *classical ovoid* $\mathcal{V}$ can be defined as the set of all points given by

$$\begin{aligned}\mathcal{V}\ =\ &\{(0,0,1,0)\}\cup\\ &\{(x,\,y,\,x^2+xy+ay^2,\,1):x,\,y\in\mathrm{GF}(q)\},\end{aligned}$$

where $a\in\mathrm{GF}(q)$ is such that the polynomial x^2+x+a has no root in $\mathrm{GF}(q)$. Such ovoid is called an *elliptic quadric*, as the points come from a non-degenerate elliptic quadratic form. For $q=2^{2e+1}$ with $e\geq 1$, there is an ovoid which is not an elliptic quadric, and is called the *Tits oviod*. It is defined by

$$\begin{aligned}\mathcal{T}\ =\ &\{(0,0,1,0)\}\cup\\ &\{(x,\,y,\,x^{\sigma}+xy+y^{\sigma+2},\,1):x,\,y\in\mathrm{GF}(q)\},\end{aligned}$$

where $\sigma=2^{e+1}$. For odd q, any ovoid is an elliptic quadric. For even q, Tits ovoids are the only known ones which are not elliptic quadratics. In the case that q is even, the elliptic quadrics and the Tits ovoid are not equivalent.

Let $\mathcal{V}$ be an ovoid in $\mathrm{PG}(3,\mathrm{GF}(q))$ with $q>2$. Denote by

$$\mathcal{V}=\{\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_{q^2+1}\},$$

where each $\mathbf{v}_i$ is a column vector in $\mathrm{GF}(q)^4$. Let $\mathcal{C}_{\mathcal{V}}$ be the linear code over $\mathrm{GF}(q)$ with generator matrix

$$G_{\mathcal{V}}=\left[\mathbf{v}_1\mathbf{v}_2\cdots\mathbf{v}_{q^2+1}\right]. \tag{12}$$

It is known that $\mathcal{C}_{\mathcal{V}}$ is a $[q^2+1, 4, q^2-q]$ code over $\mathrm{GF}(q)$ with weight enumerator

$$1 + (q^2-q)(q^2+1)z^{q^2-q} + (q-1)(q^2+1)z^{q^2} \qquad (13)$$

and its dual $\mathcal{C}_{\mathcal{V}}^{\perp}$ is a $[q^2+1, q^2-3, 4]$ code over $\mathrm{GF}(q)$ [9, Chapter 13]. Conversely, the set of column vectors of a generator matrix of any $[q^2+1, q^2-3, 4]$ code over $\mathrm{GF}(q)$ is an ovoid in $\mathrm{PG}(3, \mathrm{GF}(q))$. Hence, ovoids in $\mathrm{PG}(3, \mathrm{GF}(q))$ and $[q^2+1, q^2-3, 4]$ codes over $\mathrm{GF}(q)$ are the same, and a $[q^2+1, 4, q^2-q]$ code over $\mathrm{GF}(q)$ is called an ovoid code over $\mathrm{GF}(q)$.

The reader is referred to [9, Chapter 13] for detailed information about ovoids and ovoid codes. The weight distribution of an ovoid is given in the following lemma [9, p. 324, p. 327].

Lemma 24: Let $q \geq 4$, and let $\mathcal{C}$ be a $[q^2+1, 4, q^2-q]$ code over $\mathrm{GF}(q)$. Then the weight distribution of $\mathcal{C}^{\perp}$ is given by

$$q^4\ A_\ell(\mathcal{C}^{\perp}) = \binom{q^2+1}{\ell}(q-1)^\ell + u\sum_{i+j=\ell}\binom{q^2-q}{i}(-1)^i\binom{q+1}{j}(q-1)^j + v\left[(-1)^\ell\binom{q^2}{\ell} + (-1)^{\ell-1}(q-1)\binom{q^2}{\ell-1}\right]$$

for all $4 \leq \ell \leq q^2$, and

$$q^4\ A_{q^2+1}(\mathcal{C}^{\perp}) = (q-1)^{q^2+1} + u(q-1)^{q+1} + v(q-1),$$

where

$$u = (q^2-q)(q^2+1),\ v = (q-1)(q^2+1).$$

In particular,

$$A_4(\mathcal{C}^{\perp}) = \frac{(q-2)(q-1)^2q^2(q+1)(q^2+1)}{24}.$$

Lemma 25: [9, p. 327] Let $\mathcal{C}$ be the ovoid code defined above. Then $(\mathcal{P}(\mathcal{C}), \mathcal{B}_{q^2-q}(\mathcal{C}))$ is a 3-$(q^2+1, q^2-q, (q-2)(q^2-q-1))$ simple design.

We are now ready to study some shortened codes of ovoid codes, and have the following results.

Theorem 26: Let $q \geq 4$, and let $\mathcal{C}$ be a $[q^2+1, 4, q^2-q]$ code over $\mathrm{GF}(q)$. For any coordinate position t_1, the following hold.

1) $\mathcal{C}_{\{t_1\}}$ is a $[q^2, 3, q^2-q]$ code over $\mathrm{GF}(q)$ with weight enumerator
$$1 + q(q^2-1)z^{q^2-q} + (q-1)z^{q^2}. \qquad (14)$$
2) $(\mathcal{C}_{\{t_1\}})^{\perp}$ is a $[q^2, q^2-3, 3]$ almost MDS code over $\mathrm{GF}(q)$.
3) $((\mathcal{C}^{\perp})_{\{t_1\}})^{\perp}$ is a $[q^2, 4, q^2-q-1]$ code over $\mathrm{GF}(q)$ with weight enumerator
$$1 + q^2(q-1)^2z^{q^2-q-1} + q(q^2-1)z^{q^2-q} + q^2(q-1)z^{q^2-1} + (q-1)z^{q^2}.$$
4) $(\mathcal{C}^{\perp})_{\{t_1\}}$ is a $[q^2, q^2-4, 4]$ almost MDS code over $\mathrm{GF}(q)$ with weight distribution
$$A_k((\mathcal{C}^{\perp})_{\{t_1\}}) = \frac{\binom{k}{1}\binom{q^2}{k}}{\binom{q^2+1}{1}\binom{q^2}{k-1}}A_k(\mathcal{C}^{\perp}),$$
where $1 \leq k \leq q^2$, and $A_k(\mathcal{C}^{\perp})$ was given in Lemma 24.

Proof: It is straightforward to see that two codewords of weight q^2 in $\mathcal{C}$ have the same support if and only if one is a nonzero multiple of the other. Hence, $\mathcal{B}_{q^2}(\mathcal{C})$ has no repeated block and cardinality q^2+1, and every q^2-subset of $\mathcal{P}(\mathcal{C})$ appears exactly once in $\mathcal{B}_{q^2}(\mathcal{C})$. Consequently, $(\mathcal{P}(\mathcal{C}), \mathcal{B}_{q^2}(\mathcal{C}))$ is a 3-(q^2+1, q^2, q^2-2) design. Lemma 25 tells us that $(\mathcal{P}(\mathcal{C}), \mathcal{B}_{q^2-q}(\mathcal{C}))$ is a 3-$(q^2+1, q^2-q, (q-2)(q^2-q-1))$ simple design. Hence, $(\mathcal{P}(\mathcal{C}), \mathcal{B}_k(\mathcal{C}))$ is a 3-design for all k with $0 \leq k \leq q^2+1$. It then follows from Theorem 5 that $(\mathcal{P}(\mathcal{C}^{\perp}), \mathcal{B}_k(\mathcal{C}^{\perp}))$ is a 3-design for all k with $0 \leq k \leq q^2+1$. The desired conclusions on $\mathcal{C}_{\{t_1\}}$ then follow from Theorem 10 and the weight enumerator of $\mathcal{C}$ given in (13). Using the weight enumerator of $\mathcal{C}_{\{t_1\}}$ in (14) and the MacWilliams identity [9, p. 65], one can prove that the minimum distance $d((\mathcal{C}_{\{t_1\}})^{\perp}) = 3$. Thus, $(\mathcal{C}_{\{t_1\}})^{\perp}$ is a $[q^2, q^2-3, 3]$ almost MDS code over $\mathrm{GF}(q)$.

By Theorem 8, we have

$$((\mathcal{C}^{\perp})_{\{t_1\}})^{\perp} = \mathcal{C}^{\{t_1\}}.$$

It then follows from Theorem 11 that

$$A_k(((\mathcal{C}^{\perp})_{\{t_1\}})^{\perp}) = A_k(\mathcal{C}^{\{t_1\}}) = \sum_{i=0}^{1}\frac{\binom{q^2}{k}\binom{k+i}{1}}{\binom{q^2}{k-1+i}\binom{q^2+1}{1}}A_{k+i}(\mathcal{C}). \qquad (15)$$

The desired conclusions then follow from the weight enumerator of $\mathcal{C}$ in (13).

Since $d(\mathcal{C}^{\perp}) = 4$, by definition $d((\mathcal{C}^{\perp})_{\{t_1\}}) \geq 4$. If $d((\mathcal{C}^{\perp})_{\{t_1\}}) = 5$, then $(\mathcal{C}^{\perp})_{\{t_1\}}$ would be a $[q^2, q^2-4, 5]$ MDS code, and $((\mathcal{C}^{\perp})_{\{t_1\}})^{\perp}$ would be $[q^2, 4, q^2-3]$ MDS code, which is a contradiction. Therefore, $d((\mathcal{C}^{\perp})_{\{t_1\}}) = 4$. The desired conclusion on the weight distribution of $(\mathcal{C}^{\perp})_{\{t_1\}}$ then follows from (15) and the weight enumerator of $\mathcal{C}$ given in (13). □

Notice that all ovoid codes meet the Griemer bound. The shortened codes and their duals documented in Theorem 26 are very interesting due to the following.

- Both $\mathcal{C}_{\{t_1\}}$ and $(\mathcal{C}^{\perp})_{\{t_1\}}$ meet the Griesmer bound.
- All the four classes of codes in Theorem 26 support 2-designs (see Theorem 27 below).

Theorem 27: Let $q \geq 4$, and let $\mathcal{C}$ be a $[q^2+1, 4, q^2-q]$ code over $\mathrm{GF}(q)$. For any coordinate position t_1, the following hold.

1) The incidence structure $(\mathcal{P}(\mathcal{C}_{\{t_1\}}), \mathcal{B}_{q^2-q}(\mathcal{C}_{\{t_1\}}))$ is a 2-(q^2, q^2-q, q^2-q-1) simple design.
2) The incidence structure $(\mathcal{P}((\mathcal{C}_{\{t_1\}})^{\perp}), \mathcal{B}_3((\mathcal{C}_{\{t_1\}})^{\perp}))$ is a 2-$(q^2, 3, \lambda_1^{\perp})$ simple design for some integer $\lambda_1^{\perp}$.
3) The incidence structure $(\mathcal{P}((\mathcal{C}^{\perp})_{\{t_1\}}), \mathcal{B}_4((\mathcal{C}^{\perp})_{\{t_1\}}))$ is a 2-$(q^2, 4, (q^2-3)(q-2)/2)$ simple design.
4) The incidence structure
$$(\mathcal{P}(((\mathcal{C}^{\perp})_{\{t_1\}})^{\perp}), \mathcal{B}_{q^2-q-1}(((\mathcal{C}^{\perp})_{\{t_1\}})^{\perp}))$$
is a 2-$(q^2, q^2-q-1, (q-2)(q^2-q-1))$ simple design. The complement of this design is a 2-$(q^2, q+1, q)$ design.
5) The incidence structure
$$(\mathcal{P}(((\mathcal{C}^{\perp})_{\{t_1\}})^{\perp}), \mathcal{B}_{q^2-q}(((\mathcal{C}^{\perp})_{\{t_1\}})^{\perp}))$$

is a 2-(q^2, q^2-q, q^2-q-1) simple design. The complement of this design is a Steiner system 2-$(q^2, q, 1)$, i.e., an affine plane.

Proof: We first prove Part 1) and Part 2). Put $d_1 = q^2-q$ and $d_1^\perp = 3$. According to Theorem 26, $\mathcal{C}_{\{t_1\}}$ is a $[q^2, 3, q^2-q]$ code over $\mathrm{GF}(q)$ with weight enumerator

$$1 + q(q^2-1)z^{q^2-q} + (q-1)z^{q^2} \tag{16}$$

and $(\mathcal{C}_{\{t_1\}})^\perp$ is a $[q^2, q^2-3, 3]$ code over $\mathrm{GF}(q)$. Let $t = 2$ and $n = q^2$. Then $t < \min\{d_1, d_1^\perp\} = 3$ and $n - t = q^2 - 2 > q^2 - q$. It is clear that $\mathcal{C}_{\{t_1\}}$ has $d_1^\perp - t$ weight in the range $\{1, 2, \cdots, n-t\}$. Put $w_1 = q^2-q$ and $w_1^\perp = 3$. Then we have

$$w_1 - \left\lfloor \frac{w_1 + q - 2}{q-1} \right\rfloor = q^2 - 2q < q^2 - q = d_1$$

and

$$w_1^\perp - \left\lfloor \frac{w_1^\perp + q - 2}{q-1} \right\rfloor = 2 < d_1^\perp.$$

Hence, all the conditions in Theorem 6 are met. It then follows from Theorem 6 that the incidence structure $(\mathcal{P}(\mathcal{C}_{\{t_1\}}), \mathcal{B}_{q^2-q}(\mathcal{C}_{\{t_1\}}))$ is a 2-(q^2, q^2-q, λ_1) simple design for some integer λ_1 and $(\mathcal{P}((\mathcal{C}_{\{t_1\}})^\perp), \mathcal{B}_3((\mathcal{C}_{\{t_1\}})^\perp))$ is a 2-$(q^2, 3, \lambda_1^\perp)$ simple design for some integer $\lambda_1^\perp$. It then follows from Lemma 4 that

$$\left|\mathcal{B}_{q^2-q}(\mathcal{C}_{\{t_1\}})\right| = \frac{A_{q^2-q}(\mathcal{C}_{\{t_1\}})}{q-1} = q(q+1).$$

Consequently,

$$\lambda_1 = \left|\mathcal{B}_{q^2-q}(\mathcal{C}_{\{t_1\}})\right| \frac{\binom{q^2-q}{2}}{\binom{q^2}{2}} = q^2 - q - 1.$$

This competes the proof of Part 1). It follows from Lemma 4 that

$$\left|\mathcal{B}_3((\mathcal{C}_{\{t_1\}})^\perp)\right| = \frac{A_3((\mathcal{C}_{\{t_1\}})^\perp)}{q-1}.$$

Whence,

$$\lambda_1^\perp = \left|\mathcal{B}_3((\mathcal{C}_{\{t_1\}})^\perp)\right| \frac{\binom{3}{2}}{\binom{q^2}{2}} = \frac{6A_3((\mathcal{C}_{\{t_1\}})^\perp)}{(q-1)q^2(q^2-1)}.$$

This completes the proof of Part 2).

Finally, we prove Part 3), Part 4) and Part 5). By Theorem 26 $((\mathcal{C}^\perp)_{\{t_1\}})^\perp$ is a $[q^2, 4, q^2-q-1]$ code over $\mathrm{GF}(q)$ with weight enumerator

$$1 + q^2(q-1)^2 z^{q^2-q-1} + q(q^2-1)z^{q^2-q} + q^2(q-1)z^{q^2-1} + (q-1)z^{q^2}.$$

and $(\mathcal{C}^\perp)_{\{t_1\}}$ is a $[q^2, q^2-4, 4]$ almost MDS code over $\mathrm{GF}(q)$.

Put $d_2 = q^2-q-1$ and $d_2^\perp = 4$. Then $t < \min\{d_1, d_1^\perp\} = 4$ and $n - t = q^2 - 2 > q^2 - q$. It is clear that $(\mathcal{C}_{\{t_1\}})^\perp$ has $d_1^\perp - t$ weights in the range $\{1, 2, \cdots, n-t\}$. Put $w_2 = q^2-q$ and $w_2^\perp = 4$. Then we have

$$w_2 - \left\lfloor \frac{w_2 + q - 2}{q-1} \right\rfloor = q^2 - 2q < q^2 - q - 1 = d_2$$

and

$$w_2^\perp - \left\lfloor \frac{w_2^\perp + q - 2}{q-1} \right\rfloor \le 3 < d_2^\perp.$$

Hence, all the conditions in Theorem 6 are met. It then follows from Theorem 6 that the following hold:

- $(\mathcal{P}((\mathcal{C}^\perp)_{\{t_1\}}), \mathcal{B}_4((\mathcal{C}^\perp)_{\{t_1\}}))$ is a 2-$(q^2, 4, \lambda_2^\perp)$ simple design for some integer $\lambda_2^\perp$;
- $(\mathcal{P}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp), \mathcal{B}_{q^2-q-1}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp)))$ is a 2-$(q^2, q^2-q-1, \lambda_2)$ simple design for some integer λ_2; and
- $(\mathcal{P}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp), \mathcal{B}_{q^2-q}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp)))$ is a 2-(q^2, q^2-q, λ_3) simple design for some integer λ_3.

We will determine the specific values of $\lambda_2^\perp$, λ_2 and λ_3 below.

It follows from Lemma 4 that

$$\left|\mathcal{B}_{q^2-q-1}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp)\right| = \frac{A_{q^2-q-1}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp))}{q-1} = q^2(q-1).$$

Consequently,

$$\lambda_2 = \left|\mathcal{B}_{q^2-q-1}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp)\right| \frac{\binom{q^2-q-1}{2}}{\binom{q^2}{2}} = (q-2)(q^2-q-1).$$

It is then easily verified that the complement of $(\mathcal{P}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp), \mathcal{B}_{q^2-q-1}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp)))$ is a 2-$(q^2, q+1, q)$ design.

It follows from Lemma 4 that

$$\left|\mathcal{B}_{q^2-q}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp)\right| = \frac{A_{q^2-q}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp))}{q-1} = q(q+1).$$

Consequently,

$$\lambda_3 = \left|\mathcal{B}_{q^2-q}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp)\right| \frac{\binom{q^2-q}{2}}{\binom{q^2}{2}} = q^2 - q - 1.$$

It is then easily verified that the complement of $(\mathcal{P}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp), \mathcal{B}_{q^2-q}(((\mathcal{C}^\perp)_{\{t_1\}})^\perp)))$ is a 2-$(q^2, q, 1)$ design.

We now determine $\lambda_2^\perp$. By Lemma 24,

$$A_4(\mathcal{C}^\perp) = \frac{(q-2)(q-1)^2q^2(q+1)(q^2+1)}{24}.$$

It then follows from Theorem 26 that

$$\begin{aligned} A_4((\mathcal{C}^\perp)_{\{t_1\}}) &= \frac{\binom{4}{1}\binom{q^2}{4}}{\binom{q^2+1}{1}\binom{q^2}{3}} A_4(\mathcal{C}^\perp) \\ &= \frac{(q^2-3)(q-2)(q-1)^2q^2(q+1)}{24}. \end{aligned}$$

We then deduce that

$$\begin{aligned} \left|\mathcal{B}_4((\mathcal{C}^\perp)_{\{t_1\}})\right| &= \frac{A_4((\mathcal{C}^\perp)_{\{t_1\}})}{q-1} \\ &= \frac{(q^2-3)(q-2)(q-1)q^2(q+1)}{24}. \end{aligned}$$

Consequently,

$$\lambda_2^\perp = \left|\mathcal{B}_4((\mathcal{C}^\perp)_{\{t_1\}})\right| \frac{\binom{4}{2}}{\binom{q^2}{2}} = \frac{(q^2-3)(q-2)}{2}.$$

This completes the proofs of Part 3), Part 4) and Part 5). □

Since $(\mathcal{P}(\mathcal{C}^{\perp}), \mathcal{B}_k(\mathcal{C}^{\perp}))$ is a 3-design for all k with $0 \leq k \leq q^2+1$, we can similarly determine the parameters and weight distributions of the codes $(\mathcal{C}^{\perp})_{\{t_1,t_2\}}$ and $(\mathcal{C}^{\perp})_{\{t_1,t_2,t_3\}}$. However, these shortened codes are less interesting, as they are not optimal and do not support 2-designs.

VI. Summary and Concluding Remarks

The main contributions of this paper are the following.

- It was proved in Theorem 12 that every linear code $\mathcal{C}$ over $\mathrm{GF}(q)$ with minimum distance $d \geq 3$ is permutation-equivalent to a shortened code of $\mathcal{C}(m,q,\alpha)^{\perp}$ for some m, q and α, where α is a generator of $\mathrm{GF}(q)^*$ and $\mathcal{C}(m,q,\alpha)$ was defined in (2). This showed the importance of the shortening technique and the family of cyclic codes $\mathcal{C}(m,q,\alpha)^{\perp}$.
- The parameters and weight distributions of two families of shortened codes of the Hamming codes and their duals were settled in Theorem 18. All of the shortened codes are optimal.
- The parameters and weight distributions of another two families of shortened codes of the Hamming codes and their duals were settled in Theorem 19. All of the shortened codes are optimal.
- The parameters of three families of shortened codes of the Reed-Muller codes $\mathcal{R}(1,m)$ and $\mathcal{R}(m-2,m)$ were settled in Theorems 21 and 23. All of the shortened codes are optimal.
- The parameters of another two families of shortened codes of the Reed-Muller codes $\mathcal{R}(1,m)$ and $\mathcal{R}(m-2,m)$ were settled in Theorem 22. All of the shortened codes are either distance-optimal, or dimension-optimal, or distance-almost-optimal, or dimension-almost-optimal.
- The parameters of shortened codes of the oviod code and its dual were settled in Theorem 26. The shortened codes are either distance-optimal, or dimension-optimal, or distance-almost-optimal.
- Five families of 2-designs were obtained from the shortened codes of the ovoid codes and their duals and were documented in Theorem 27. Some of the 2-designs are interesting, as they are related to affine planes.

In summary, eleven infinite families of optimal shortened codes were presented in this paper. Note that all the one-weight codes meeting the Griesmer bound presented in this paper are not new up to equivalence, as they are permutation-equivalent to a concatenation of a number of Simplex codes by Lemma 7. The shortened code $(\mathcal{R}(1,m)_{\{t_1\}})^{\perp}$ is permutation-equivalent to a binary Hamming code and is thus not new up to equivalence.

Since every linear code with minimum distance at least 3 is a shortened code of a Hamming code, some shortened codes of a Hamming code must have bad parameters and some shortened codes must have good or optimal parameters. To obtain an optimal or good shortened code, a linear code $\mathcal{C}$ and the set T of coordinate positions for shortening must be properly selected.

One part of the originality of this paper is to find suitable codes $\mathcal{C}$ satisfying all the conditions in Theorems 10 and 11. In both theorems, the required conditions are that $(\mathcal{P}(\mathcal{C}), \mathcal{B}_i(\mathcal{C}))$ is a t-design for any i with $d \leq i \leq n-t$ for the underlying code $\mathcal{C}$. These conditions are very demanding. It is not easy to find a linear code $\mathcal{C}$ satisfying these conditions. Note that both Theorems 10 and 11 are just tools for obtaining linear codes with new and interesting parameters. The second part of the originality of this paper is the use of orthogonal arrays for studying shortened codes (see the proofs of Theorems 15, 21, 22, and 23). The last part of the originality of this paper is the shortened codes with new parameters.

Acknowledgment

The authors would like to thank the reviewers and the Associate Editor, Dr. Vladimir Sidorenko, for their very constructive comments and suggestions that much improved the quality and presentation of this paper. In particular, the direct proof of Corollary 13 was given by Vladimir Sidorenko.

References

[1] E. F. Assmus, Jr., and H. F. Mattson, Jr., "New 5-designs," *J. Combinat. Theory*, vol. 6, no. 2, pp. 122–151, Mar. 1969.
[2] M. R. Best and A. E. Brouwer, "The triply shortened binary Hamming code is optimal," *Discrete Math.*, vol. 17, no. 3, pp. 235–245, 1977.
[3] A. Beutelspacher, "On t-covers in finite projective spaces," *J. Geom.*, vol. 12, no. 1, pp. 10–16, 1979.
[4] A. Bonisoli, "Every equidistant linear code is a sequence of dual Hamming codes," *Ars Combinat.*, vol. 18, pp. 181–186, 1984.
[5] A. S. Hedayat, N. J. A. Slone, and J. Stufken, *Orthogonal Arrays: Theory and Applications*. New York, NY, USA: Springer, 1999.
[6] A. E. Brower, H. O. Hämäläinen, P. R. J. Östgård, and N. J. A. Sloane, "Bounds on mixed binary/ternary codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 140–161, Jan. 1998.
[7] C. L. Chen, "On shortened finite geometry codes," *Inf. Control*, vol. 20, no. 3, pp. 216–221, Apr. 1972.
[8] C. Ding, "Linear codes from some 2-designs," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3265–3275, Jun. 2015.
[9] C. Ding, *Designs From Linear Codes*. Singapore: World Scientific, 2018.
[10] C. Ding and C. Li, "Infinite families of 2-designs and 3-designs from linear codes," *Discrete Math.*, vol. 340, no. 10, pp. 2415–2431, Oct. 2017.
[11] C. Ding, J. Luo, and H. Niederreiter, "Two weight codes punctured from irreducible cyclic codes," in *Proc. 1st Int. Workshop Coding Theory Cryptogr.*, Y. Li, S. Ling, H. Niederreiter, H. Wang, C. Xing, and S. Zhang, Eds. Singapore: World Scientific, 2008, pp. 119–124.
[12] C. Ding and H. Niederreiter, "Cyclotomic linear codes of order 3," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2274–2277, May 2007.
[13] C. Ding and J. Yang, "Hamming weights in irreducible cyclic codes," *Discrete Math.*, vol. 313, no. 4, pp. 434–446, Feb. 2013.
[14] J. L. Goldwasser, "Shortened and punctured codes and the MacWilliams identities," *Linear Algebra Appl.*, vol. 253, nos. 1–3, pp. 1–13, Mar. 1997.
[15] H. Helgert and R. Stinaff, "Shortened BCH codes," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 6, pp. 818–820, Nov. 1973.
[16] Z. Heng and C. Ding, "A construction of q-ary linear codes with irreducible cyclic codes," *Des., Codes Cryptogr.*, vol. 87, no. 5, pp. 1087–1108, May 2019.
[17] Z. Heng, W. Wang, and Y. Wang, "Projective binary linear codes from special Boolean functions," *Appl. Algebra Eng. Commun. Comput.*, pp. 1–32, Jan 2020, doi: 10.1007/s00200-019-00412-z.
[18] H. T. Hsu, "A class of binary shortened cyclic codes for a compound channel," *Inf. Control*, vol. 18, no. 2, pp. 126–139, Mar. 1971.
[19] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[20] G. A. Kabatiansky and V. I. Panchenko, "Unit sphere packings and coverings of the Hamming space," *Probl. Peredachi Inf.*, vol. 24, no. 4, pp. 3–16, 1988.
[21] T. Kasami, "Optimum shortened cyclic codes for burst-error correction," *IEEE Trans. Inf. Theory*, vol. IT-9, no. 2, pp. 105–109, Apr. 1963.
[22] S. Lin, "Shortened finite geometry codes," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 5, pp. 692–696, Sep. 1972.

[23] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.
[24] P. Nelson and S. H. M. van Zwam, "On the existence of asymptotically good linear codes in minor-closed classes," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1153–1158, Mar. 2015.
[25] C. Tang, C. Ding, and M. Xiong, "Steiner systems $S(2, 4, \frac{3^m-1}{2})$ and 2-designs from ternary linear codes of length $\frac{3^m-1}{2}$," *Des., Codes Cryptogr.*, vol. 87, no. 12, pp. 2793–2811, Dec. 2019.
[26] C. Tang, C. Ding, and M. Xiong, "Codes, differentially δ-uniform functions and t-designs," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3691–3703, Jun. 2020.
[27] J. Wolfmann, "Codes projectifs à deux ou trois poids associés aux hyperquadriques d'une géométrie finie," *Discrete Math.*, vol. 13, no. 2, pp. 185–211, 1975.
[28] C. Xiang, "It is indeed a fundamental construction of all linear codes," 2016, *arXiv:1610.06355*. [Online]. Available: http://arxiv.org/abs/1610.06355
[29] A. Yardi and R. Pellikaan, "On shortened and punctured cyclic codes," 2017, *arXiv:1705.09859*. [Online]. Available: http://arxiv.org/abs/1705.09859

Yang Liu was born in Hebei, China, in 1986. She received the M.Sc. and Ph.D. degrees from Hebei Normal University, Shijiazhuang, China, in 2011 and 2014, respectively. Since 2014, she has been a Lecturer of Mathematics with the Tianjin University of Commerce, China. Her research interests include cryptography and coding theory.

Cunsheng Ding (Senior Member, IEEE) was born in Shaanxi, China, in 1962. He received the M.Sc. degree from the Northwestern Telecommunications Engineering Institute, Xian, China, in 1988, and the Ph.D. degree from the University of Turku, Turku, Finland, in 1997.

From 1988 to 1992, he was a Lecturer of Mathematics with 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 with the National University of Singapore. His research interests include combinatorial designs, cryptography, and coding theory. He has coauthored five research monographs, and has served as a guest editor or an editor for ten journals. He co-received the State Natural Science Award of China in 1989.

Chunming Tang was born in Sichuan, China, in 1982. He received the B.S. degree from Sichuan Normal University, Chengdu, China, in 2004, and the M.S. and Ph.D. degrees from Peking University, Beijing, China, in 2012. From 2017 to 2018, he was a Post-Doctoral Member with the Department of Mathematics, University of Paris VIII. He is currently a Professor with the School of Mathematics and Information, China West Normal University, Nanchong, China. His research interests include cryptography, coding theory, and information security.