A New Construction for Constant Weight Codes

Tuvi Etzion, Fellow, IEEE, and Alexander Vardy, Fellow, IEEE

Abstract — A new construction for constant weight codes is presented. The codes are constructed from $k$-dimensional subspaces of the vector space $F^n_q$. These subspaces form a constant dimension code in a Grassmannian. Some of the constructed codes are optimal constant weight codes with parameters not known before. An efficient algorithm for error-correction is given for these codes. If the constant dimension code has an efficient encoding and decoding algorithm then also the constructed constant weight code has an efficient encoding and decoding algorithm.

I. INTRODUCTION

CONSTRUCT weight codes were extensively studied. These codes have various important applications [1–7]. Let $A(n,d,w)$ be the maximum number of codewords in a constant weight code of length $n$, weight $w$, and minimum distance $d$. The quantity $A(n,d,w)$ was also a subject for dozens of papers, e.g. [8–14]. Some optimal constant weight codes can be translated to other combinatorial structures such as Steiner systems, difference families, and Hadamard matrices and these were also investigated in the context of their coding theory applications [15,16] and combinatorial designs [17–22]. Although we gave many references, it is only a small drop in the sea of references on these topics.

As said, we know some exact values of the quantity $A(n,d,w)$ like those derived from Steiner systems. But, their number is relatively small. There are also some efficient constant weight codes [23,24], and also a general efficient encoding algorithm for some classes of codes [25]. There are also some error-correction for other classes [26,27,28], but these are exceptional and usually given either to relatively small codes or codes which are not interesting from minimum distance point of view. The goal of this note is to present a new construction for constant weight codes. We want that our construction will produce for some parameters codes which are larger than other known codes with the same parameters. We want to design efficient encoding/decoding algorithm for our codes and also to have efficient error-correction algorithm for them.

The paper is organized as follows. In Section II we present the construction of our codes. The main ingredients for our codes are constant dimension codes which is a relatively new concept in coding theory. A codeword in such a code, for our construction, is a subspace of the vector space $F^n_q$, where $F_q$ is a field with $q$ elements, and each such codeword (subspace) and its cosets in $F^n_q$ form the codewords of the new constant weight code. We give a short introduction for the necessary concepts that we need on constant dimension codes. Based on the parameters of these codes we calculate the parameters of the constructed constant weight codes. In Section III we analysis the codes obtained from our construction. We present three examples of known optimal codes derived from our construction. We continue to present new optimal constant weight codes not known before which are generated by our construction. Finally, we discuss in general the size and the parameters of the constructed codes. In Section IV we present efficient encoding/decoding algorithm for the new codes, based on encoding/decoding algorithm for the constant dimension codes. We also describe an efficient error-correction algorithm for them. Conclusion is given in Section V.

II. CONSTRUCTION FOR CONSTANT WEIGHT CODES

In this section we present the construction for constant weight codes. The construction of optical orthogonal codes which appears in [28,29] is a special case of our construction. The main ingredients for our construction are constant dimension codes. These codes got lot of interest recently due to their application in error-correction for network coding [30]. Many papers have been considered this topic recently, e.g. [31–39]. Given a nonnegative integer $k \leq n$, the set of all subspaces of $F^n_q$ that have dimension $k$ is known as a Grassmannian, and usually denoted by $G_q(n,k)$. It turns out that the natural measure of distance in $G_q(n,k)$ is given by

$$d(U,V) \overset{\text{def}}{=} \dim U + \dim V - 2 \dim(U \cap V)$$

(1)

for all $U, V \in G_q(n,k)$. We say that $C \subseteq G_q(n,k)$ is an $[n, M, d, k]$ code in the Grassmannian if $|C| = M$ and $d(U,V) \geq d$ for all $U, V \in C$. The input for our construction is given a set of subspaces of a constant dimension code. The cosets of each subspace are transferred into words with the same length and weight. In other word this is a construction which transfers from dimension to weight and hence we will call it Construction FDTW.

For the construction we will also need the definition of a characteristic vector $ch(A)$ for a subset $A = \{a_1, a_2, \ldots, a_m\}$ of $F^n_q$. The characteristic vector function induces a mapping from the set of all $m$-subsets of $F^n_q$ into the set of all binary vectors of length $q^n$ and weight $m$, where $ch(A) = (c_0, c_1, \ldots, c_{q^n-1})$ given by

$$c_i = 1 \text{ if } \alpha^i \in A \text{ and } c_0 = 0 \text{ if } \alpha^i \notin A, \quad 0 \leq i \leq q^n - 2,$$

$$c_{q^n-1} = 1 \text{ if } 0 \in A \text{ and } c_{q^n-1} = 0 \text{ if } 0 \notin A.$$

Let $X \subseteq F^n_q$ and $\beta \in F^n_q$. The addition $\beta + X$ is defined as the addition of $\beta$ to each element of $X$. If $X = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ then $\beta + X = \{\beta + \alpha_1, \beta + \alpha_2, \ldots, \beta + \alpha_m\}$. 

This work was supported in part by the United States National Science Foundation and in part by the United States — Israel Binational Science Foundation (BSF), Jerusalem, Israel, under Grant 2006097.

Tuvi Etzion is with the Department of Computer Science, Technion, Haifa 32000, Israel. (e-mail: etzion@cs.technion.ac.il).

Alexander Vardy is with the Department of Electrical and Computer Engineering, the Department of Computer Science and Engineering, and the Department of Mathematics, all at the University of California San Diego, La Jolla, CA 92093-0407, U.S.A. (e-mail: vardy@kilimanjaro.ucsd.edu).
Construction FDTW:

Let $C$ be an $[n, M, d, k]$ code. Given a codeword $X = \{0, \alpha_1, \ldots, \alpha_{q^{k-1}}\} \in C$ we form a set of codewords $C_X$ as follows:

$$C_X = \{ch(\{\beta, \beta + \alpha_1, \beta + \alpha_2, \ldots, \beta + \alpha_{2q-1}\}) : \beta \in \mathbb{F}_q\}.$$ 

The codewords $C_X$ are the characteristic vectors for the cosets of the $k$-dimensional subspace $X$. Therefore, $|C_X| = q^{k-1}$. We define our constant weight code $C$ as union of all the sets $C_X$ over all codewords of $C$, i.e.,

$$C = \bigcup_{X \in C} C_X = \{ch(\{\beta, \beta + \alpha_1, \beta + \alpha_2, \ldots, \beta + \alpha_{2q-1}\}) : \{0, \alpha_1, \ldots, \alpha_{q^{k-1}}\} \in C, \beta \in \mathbb{F}_q\}.$$ 

Theorem 1. If $C$ is an $[n, M, d = 2t, k]$ constant dimension code then the code $C$ obtained by Construction FDTW is a $(q^n, q^{n-k}M, 2 \cdot q^k - 2 \cdot q^{k-t}, q^k)$ constant weight code.

Proof. The length of the code $C$ and the weight of its codewords are obvious. Since the number of cosets of a $k$-dimensional subspace in $\mathbb{F}_q^n$ is $q^{n-k}$ it follows that the number of cosets in $C$ is $q^{n-k}M$. It remains to show that the minimum distance of $C$ is $2 \cdot q^k - 2 \cdot q^{k-t}$. Assume that the minimum distance of $C$ is less than $2 \cdot q^k - 2 \cdot q^{k-t}$. Then there exists two distinct codewords in $C$ which have at least $q^{k-t} + 1$ entries with ones located on the same position numbers in both codewords. Hence, the intersection of the corresponding $q^t$-subsets $X, Y$ of $\mathbb{F}_q^n$ has at least $q^{k-t} + 1$ elements. Clearly $X$ and $Y$ are not cosets of the same codeword of $C$ since all the distinct cosets of the same codeword are disjoint. Let $-\beta \in X \cap Y$, $C(X) = \beta + X$, and $C(Y) = \beta + Y$. Since $0 \in C(X) \cap C(Y)$, where $0$ is the allzero vector, it follows that $C(X) \cap C(Y) \subseteq \mathbb{F}_q \cdot \beta$. Therefore $X$ and $Y$ (and hence $C(X)$ and $C(Y)$) have all $k-t+1$ linearly independent elements, i.e., $\text{dim}(C(X) \cap C(Y)) \geq k-t+1$ and by (1) we have $d(X, Y) = d(C(X), C(Y)) \leq k+k-2(k-t+1) = 2t-2$ which contradicts the minimum distance of $C$.

Thus, the minimum distance of $C$ is $2 \cdot q^k - 2 \cdot q^{k-t}$. □

A very simple, but sometimes very effective operation in coding is shortening. For a code $C$ of length $n$ (not necessarily constant weight), over $\mathbb{F}_q$, the shortened code by the coordinate $i$, $C_q^i$, $b \in \mathbb{F}_q$, is defined by

$$C_q^i = \{(c_0, c_i-1, c_i+1, \ldots, c_{n-1}) : (c_0, c_i-1, b, c_i+1, \ldots, c_{n-1}) \in C\}.$$ 

Hence, for each $b, \in \mathbb{F}_q$, we can form $n$ shortened codes. It is readily verified that the length of each shortened code is $n-1$ and its minimum distance is the same as the minimum distance of $C$. The size of the shortened code might depend on the coordinate of the shortening. Since the cosets of a subspace over $\mathbb{F}_q^n$ form a partition of $\mathbb{F}_q^n$ it follows that the size of the shortened codes from Construction FDTW does not depend on the coordinate of the shortening. Hence, the following theorem can be easily verified.

Theorem 2. If $C$ is an $[n, M, d = 2t, k]$ constant dimension code over $\mathbb{F}_q$, then there exist a $(q^n-1, M, 2 \cdot q^k - 2 \cdot q^{k-t}, q^k-1)$ constant weight code and a $(q^n-1, (q^{n-k}-1)M, 2 \cdot q^k - 2 \cdot q^{k-t}, q^k)$ constant weight code.

A construction of a $(q^n-1, (q^{n-k}-1)M, 2 \cdot q^k - 2 \cdot q^{k-1}, q^k)$ code was given in [28] and of a $(q^n-1, (q^{n-k}-1)M, 2 \cdot q^k - 2 \cdot q^k)$ in [29]. Their constructed codes are optical orthogonal codes. In the following section we will explain when the code obtained by Construction FDTW will be an optical orthogonal code.

III. ANALYSIS ON THE SIZE OF THE CODES

In this section we examine the codes that can be obtained by Construction FDTW. We start with two examples over $\mathbb{F}_2$ which result in optimal constant weight codes. We continue with an example over $\mathbb{F}_q$ which also result in an optimal code. The parameters of these three examples were known before. We continue with a theorem which present two more codes over $\mathbb{F}_2$ which are optimal and were not known before. We examine the known construction of constant dimension codes for their induced constant weight codes. Finally, we discuss cyclic codes and a class of codes called optical orthogonal codes and prove when we form an optical orthogonal code from the constant weight code obtained in Construction FDTW.

The sizes of the codes involve the $q$-ary Gaussian coefficient $\begin{bmatrix} n \\ \ell \end{bmatrix}_q$ defined as follows (see [40]):

$$\begin{bmatrix} n \\ \ell \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-\ell+1} - 1)}{(q^{\ell-1})(q^{\ell-2} - 1) \cdots (q - 1)} \cdot \quad \begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1.$$

Example 1. Let $C$ be an $[n, \begin{bmatrix} n \\ 2 \end{bmatrix}_2, 2, 2]$ code which consists of all 2-dimensional subspaces from $\mathbb{F}_2^n$. $C$ is a $(2^n, 2^{n-2} \begin{bmatrix} n \\ 2 \end{bmatrix}_2, 4, 4)$ code forming the codewords of weight four in the extended Hamming code of length $2^n$ [15], i.e., a Steiner system $S(3, 4, 2^n)$.

Example 2. Let $C$ be an $[n, \begin{bmatrix} n-1 \\ 2 \end{bmatrix}_2, 2, n-1]$ code which consists of all $(n-1)$-dimensional subspaces from $\mathbb{F}_2^n$. $C$ is a $(2^n, 2^{n-1} - 2, 2^{n-1} - 2, n-1)$. If we join to $C$ the allone and the allzero codewords then the formed code is a Hadamard code [15, p. 49].

Before we continue to the next example we define two interesting combinatorial designs related to the previous two examples and to the next one.

A Steiner system $S(t, k, n)$ is a collection $Q$ of $k$-subsets (called blocks) taken from an $n$-set (say $Z_n$) such that each $t$-subset of $Z_n$ is a subset of exactly one block of $Q$. A Steiner system $S(t, k, n)$ is also an $[n, M, d, k]$ code with $M = \begin{bmatrix} n \\ t \end{bmatrix}_q / \begin{bmatrix} k \\ t \end{bmatrix}_q$ and $d = 2(k - t + 1)$.

A Steiner structure $S_q[t, k, n]$ is a set $S$ of $k$-dimensional subspaces taken from $\mathbb{F}_q^n$ such that each $t$-dimensional subspace of $\mathbb{F}_q^n$ is contained in exactly one element of $S$. It can be easily verified that a Steiner structure $S_q[t, k, n]$ is an $[n, M, d, k]$ code in $G_q(n, k)$ with $M = \begin{bmatrix} n \\ t \end{bmatrix}_q / \begin{bmatrix} k \\ t \end{bmatrix}_q$ and $d = 2(k - t + 1)$. Steiner structure $S_q[1, k, n]$ exists if and
only if \( k \) divides \( n \). They are also known as spreads in projective spaces. Such spreads were studied in many papers, e.g. [41–45].

Let \( n = sk, r = \frac{q^{n} - 1}{q - 1} \), and let \( \alpha \) be a primitive element in \( \text{GF}(q^n) \). For each \( i, 0 \leq i \leq r - 1 \), we define

\[
H_i = \{ \alpha^i, \alpha^{i+1}, \alpha^{2i+1}, \ldots, \alpha^{(q^k-2)r+i} \}.
\]

The set \( \{ H_i : 0 \leq i \leq r - 1 \} \) is a Steiner structure \( S_q[1, k, n] \), i.e., an \( [n, \frac{q^n - 1}{q - 1}, 2k, k] \) code.

**Example 3.** Let \( \mathbb{C} \) be the \( [n, \frac{q^n - 1}{q - 1}, 2k, k] \) code defined above. By applying Construction FDTW on \( \mathbb{C} \) we obtain a \( (q^n, q^{n-k}\frac{q^n - 1}{q - 1}, 2 \cdot q^k - 2, q^k) \) code \( C \) which is a Steiner system \( S(2, q^k, q^n) \).

For the next two optimal codes we need the following two theorems. The first one is the well-known Jonson bound [8].

**Theorem 3.** If \( n \geq w > 0 \) then

\[
A(n, d, w) \leq \frac{n}{w} A(n - 1, d, w - 1).
\]

The second theorem was developed by Agrell, Vardy, and Zeger [14].

**Theorem 4.** If \( b > 0 \) then

\[
A(n, 2\delta, w) \leq \left\lfloor \frac{\delta}{b} \right\rfloor
\]

where

\[
b = \delta - \frac{w(n - w)}{n} + \frac{n}{M^2} \left( M \frac{w}{n} \right) \left( M \frac{n - w}{n} \right).
\]

**Theorem 5.**

- \( A(2^{2m-1} - 1, 2^{m+1} - 4, 2^{m-1} - 1) = 2^{m+1} + 1 \).
- \( A(2^{2m-1}, 2^{m+1} - 4, 2^m) = 2^{2m-1} + 2^m - 1 \).

**Proof.** The upper bound \( A(2^{2m-1} - 1, 2^{m+1} - 4, 2^{m-1} - 1) \leq 2^{m+1} + 1 \) is a direct application of theorem 4. Using this bound in Theorem 3 we obtain the second upper bound \( A(2^{2m-1}, 2^{m+1} - 4, 2^m) \leq 2^{2m-1} + 2^m - 1 \).

By applying Construction FDTW on a \( [2^{m-1}, 2^{m+1} - 4, 2^{m-1} - 4, 2^m - 2, m] \) code [33] we obtain a \( (2^{2m-1}, 2^{m+1} - 4, 2^{m-1} - 4, 2^m - 2, m] \) code. Hence, \( A(2^{2m-1}, 2^{m+1} - 4, 2^m) \geq 2^{2m-1} + 2^m - 1 \) and thus \( A(2^{2m-1}, 2^{m+1} - 4, 2^m) = 2^{2m-1} + 2^m - 1 \). By shortening the \( (2^{2m-1}, 2^{m+1} - 4, 2^m) \) code we obtain a \( (2^{2m-1} - 1, 2^{m+1} - 1, 2^{m+1} - 4, 2^{m-1} - 1) \) code and hence \( A(2^{2m-1} - 1, 2^{m+1} - 1, 2^{m-1} - 1) = 2^{m+1} + 1 \).

Construction FDTW requires large constant dimension codes. But, usually even the largest constant dimension codes will not induce large constant weight codes via Construction FDTW. The examples we have given in this section represent the three classes of constant dimension codes from which large constant weight codes will be formed via Construction FDTW, where by large we mean, close enough to the value of \( A(n, d, w) \). These three classes are:

1. \( [n, M, 2k, k] \) codes over \( \mathbb{F}_q \).
2. \( [n, M, n-1, n-1] \) codes over \( \mathbb{F}_2 \).
3. \( [n, M, 2k-2, k] \) codes over \( \mathbb{F}_2 \).

For the first class of constant dimension codes is \( [n, M, 2k, k] \) codes. It was proved in [35] that if \( n \equiv r \) (mod \( k \)), then, for all \( q \), we have

\[
A_q(n, 2k, k) \geqq \frac{q^n - q^k (q^k - 1) - 1}{q^k - 1}
\]

By applying construction FDTW on the related code we obtain a \( (2^n, 2^{2n-k} - q^{n-k} - q^{k+1} - 2, k^1 + 2, 2k) \) code, while the related upper bound is \( A(2^n, 2^{k+1} - 2, 2k) \leqq 2^{n-k} \left\lfloor \frac{q^n - 1}{q^k - 1} \right\rfloor \).

The second class is small in its size. For the third class we can use codes obtained by the multilevel construction [33]. The constant weight codes obtained by Construction FDTW are of size not far from the related upper bounds. More codes from this class are discussed next.

Finally, we consider the shortened codes obtained from construction FDTW and we also consider optical orthogonal codes. An \((n, w, \lambda)\) optical orthogonal code \( C \) is a set of codewords (each codeword is a \( w \)-subset) with the following properties:

- Each codeword has length \( n \) and weight \( w \).
- If \( X \subset C \) then all the \( n \) cyclic shift of \( C \) are distinct and does not belong to \( C \).
- If \( X' \) and \( Y' \) be any cyclic shifts of \( X, Y \subset C, X' \neq Y' \), then \( [X' \cap Y'] \leq \lambda \).

Optical orthogonal codes were considered in many papers, e.g., [3, 6, 28, 29, 46–50] We will now show how to use construction FDTW to form optical orthogonal codes. For this purpose, we will define the concept of cyclic code in \( G_q(n, k) \). Let \( \alpha \) be a primitive element of \( \text{GF}(q^n) \). We say that a code \( C \subset G_q(n, k) \) is cyclic if it has the following property: whenever \( \{0, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^m \} \) is a codeword of \( C \), so is its cyclic shift \( \{0, \alpha^j, \alpha^{j+1}, \ldots, \alpha^{j+n-1} \} \). In other words, if we map each vector space \( V \subset \mathbb{C} \) into the corresponding binary characteristic vector of length \( q^n - 1 \) (excluding the zero element) then the set of all such characteristic vectors is closed under cyclic shifts. Note that the property of being cyclic does not depend on the choice of a primitive element \( \alpha \) in \( \text{GF}(q^n) \).

**Lemma 6.** If \( C \) is a cyclic code then the codes \( C_0^{n-1} \) and \( C_1^{n-1} \) are cyclic, where \( C \) is the code obtained by Construction FDTW.

**Proof.** Let \( \alpha \) be a primitive element in \( \text{GF}(q^n) \) and assume that \( \{0, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^m \} \subset C \). If \( 0 \leq j \leq q^n - 2 \), then \( ch(\{0, \alpha^j, \alpha^{j+1}, \ldots, \alpha^{j+n-1} \}) \subset C \) and \( ch(\{\alpha^j, \alpha^{j+1}, \ldots, \alpha^{j+n-1} \}) \subset C \). Since \( C \) is a cyclic code it follows that \( ch(\{0, \alpha^j, \alpha^{j+1}, \ldots, \alpha^{j+n-1} \}) \subset C \) and \( ch(\{\alpha^j, \alpha^{j+1}, \ldots, \alpha^{j+n-1} \}) \subset C \). Therefore, \( C_0^{n-1} \) and \( C_1^{n-1} \) are cyclic. □

Kohnert and Kurz [32], Etzion and Vardy [35] have considered \( [n, M, 2k - 2, k] \) cyclic codes over \( \mathbb{F}_2 \). Some of the codes have the following parameters: [8, 1275, 4, 3]
code (compared to $A_2(8, 4, 3) \leq 1493$); $[9, 5694, 4, 3]$ code (compared to $A_2(9, 4, 3) \leq 6205$); $[10, 21483, 4, 3]$ code (compared to $A_2(10, 4, 3) \leq 24698$). The first two codes are the largest cyclic code with their parameters. The resulting constant weight codes from Construction FDTW have the following parameters: $(256, 40800, 12, 8)$ code (compared to $A(256, 12, 8) \leq 48960$); $(512, 364416, 12, 8)$ code (compared to $A(512, 12, 8) \leq 397120$); $(1024, 2749824, 12, 8)$ code (compared to $A(1024, 12, 8) \leq 31800032$). Given a cyclic constant code $C$ we form an optical orthogonal code as follows. We partition the codewords into equivalence classes such that two codewords are in the same equivalence class if one can be formed from the other by a cyclic shift. From each equivalence class of size $n$ we take one representative to form the optical orthogonal code. The related optical orthogonal codes for the above cyclic codes have the following parameters: $(255, 7, 1)$ and size $1275$; $(255, 8, 2)$ and size $38525$; $(511, 7, 1)$ and size $5621$; $(511, 8, 2)$ and size $354123$; $(1023, 7, 1)$ and size $21483$; $(1023, 8, 2)$ and size $2728341$. Similarly, we can form optical orthogonal codes by shortening the codes of example 3. The codes obtained coincide with the codes in [28,29].

IV. Encoding, Decoding, and Error-Correction

For simplicity we consider only codes over $\mathbb{F}_2$ in this section, even so there is a relatively simple generalization for $\mathbb{F}_q$.

One major necessity of an error-correcting code is an efficient encoding and decoding algorithms as well as an efficient error-correction algorithm. Unfortunately, most large constant weight code do not have efficient encoding and decoding algorithms. The same is true for an efficient error-correction algorithm. It appears that if the constant weight code is constructed via Construction FDTW from a constant dimension code which has an efficient encoding and decoding algorithm then efficient encoding and decoding algorithm can be designed also for the constant weight code. Moreover, unlike most constant weight codes, the codes constructed via Construction FDTW from the constant dimension codes (which were generated by any construction) have efficient error-correction algorithm. The encoding and decoding algorithm which we present will make use of the reduced row echelon form of a subspace. We will start with the definition of this canonical form.

A. Reduced row echelon form

Let $X \in \mathcal{G}_q(n, k)$ be a $k$-dimensional subspace in the Grassmannian. We can represent $X$ by the $k$ linearly independent vectors from $X$ which form a unique $k \times n$ generator matrix in reduced row echelon form (RREF), denoted by $RE(X)$, and defined as follows:

- The leading coefficient of a row is always to the right of the leading coefficient of the previous row.
- All leading coefficients are ones.
- Every leading coefficient is the only nonzero entry in its column.

For each $X \in \mathcal{G}_q(n, k)$ we associate a binary vector of length $n$ and weight $k$, $v(X)$, called the identifying vector of $X$, where the ones in $v(X)$ are exactly in the positions where $RE(X)$ has the leading ones.

Let $\mathcal{I}(X)$ be the set of $n - k$ positions numbers in $v(X)$ with zeros. Let $CP(X)$ be an $(n - k) \times n$ binary matrix with rows of weight one. The set of positions of the ones in these rows is exactly $\mathcal{I}(X)$. Note, that the $k$ rows of $RE(X)$ together with the $n - k$ rows of $CP(X)$ span $\mathbb{F}_2^n$.

B. Encoding and decoding

Let $C$ be an $[n, M, d = 2t, k]$ code with an efficient encoding algorithm EA. Construction FDTW yields a $(2^n, 2^{n-k}M, 2^{k+1} - 2^{k-t+1}, 2^k)$ code $C$. We can consider the set $\{(i, j) : i \in \mathbb{Z}_M, j \in \mathbb{F}_2^{n-k}\}$ as the set of information words for the code $C$ (since $M$ is the number of codeword in $C$ and from each codeword of $C$ we derive $2^{n-k}$ codewords in $C$). The encoding algorithm for an information word $(i, j)$ is straightforward. First, we encode $i$ to a $k$-dimensional subspace $X = \{0, \alpha_1, \ldots, \alpha_{2^{n-k}}\}$ by the algorithm EA. Let $B(j)$ be the row vector of length $n - k$ which forms the binary representation of $j$. We encode the information word $(i, j)$ to the binary codeword $ch(B(j) \cdot CP(X) + X)$ which has weight $2^k$.

Decoding of a codeword into an information word is done similarly in reverse order. What we need for this algorithm is a constant dimension code with an efficient encoding algorithm. For this purpose we can use the constant dimension codes generated by lifting of rank-metric codes [31,33]. Their encoding algorithm are formed directly from the encoding algorithms of the (linear) rank-metric codes which are lifted to form them.

C. Error-correction

Again, let $C$ be an $[n, M, d = 2t, k]$ code from which Construction FDTW yields a $(2^n, 2^{n-k}M, 2^{k+1} - 2^{k-t+1}, 2^k)$ code $C$. As we should assume that the received words also have weight $2^k$, it is required that the code $C$ will be able to correct at least $2^k - 2^k - 2$ errors (at most $2^{k-1} - 2^{k-t+1} - 1$ ones were changed to zeroes, and vice versa, in a codeword which can be recovered).

For simplicity we will consider the codewords as $2^k$-subsets of $\mathbb{F}_2^n$, i.e., $ch(X)$ is the vector notation of the codeword $X$. Assume that the codeword $X = \{x_1, x_2, \ldots, x_{2^k}\}$ was submitted and the word $Y = \{y_1, y_2, \ldots, y_{2^k}\}$ was received. We start by generating the multiset $T(Y)$ of the 2-subsets sums from $Y$, i.e., $T(Y) = \{y_i + y_j : 1 \leq i \leq j \leq 2^k\}$, $|T| = (2^k+1)/2$. Let $z_{1}, z_{2}, \ldots, z_{2^k}$ be the elements with the most appearances in $T$. We form the codeword $Z = \{z_{1}, z_{2}, \ldots, z_{2^k}\} \in C$. Let $\beta \in Y$ be any element that was used at least $2^{k-1} - 1 - (2^{k-t}-1)$ times to form element from $Z$, i.e., $z_{i} = \beta + y_{i}$, where $z_{i} \in Z$ and $y_{i} \in Y$. If not more than $2^k - 2^{k-t} - 2$ errors occurred then the submitted codeword is $\beta + Z = \{\beta + z_{1}, \beta + z_{2}, \ldots, \beta + z_{2^k}\}$.

The correctness of this error-correction algorithm is based on the following two lemmas.
Lemma 7. Let $\mathbb{C}$ be an $[n, M, d, k]$ constant dimension code. Let $C$ be a $(2^n, 2^n - kM, 2^{k+1} - 2^k - t+1, 2^k)$ code generated by Construction FDTW and let $X = \{\alpha_1, \alpha_2, \ldots, \alpha_{2k-1}\} \subseteq C$. Then

1) An element which appears in $T(X)$ has $2^{k-1}$ appearances in $T(X)$.
2) Assume that due to errors, $\tau$ zeroes were changed to ones and $\tau$ ones were changed to zeroes in $X$, and a word $Y$ was formed. Then an element which appears in $T(X)$ has at least $2^{k-1} - \tau$ appearances in $T(Y)$.
3) Assume that due to errors, $\tau$ zeroes were changed to ones and $\tau$ ones were changed to zeroes in $X$, and a word $Y$ was formed. Then an element which does not appear in $T(X)$ has at most $\tau$ appearances in $T(Y)$.
4) For each $\beta \in \mathbb{F}_2^n$ we have $T(X) = T(\beta + X)$.

Lemma 8. Let $\mathbb{C}$ be an $[n, M, d, k]$ constant dimension code. Let $C$ be a $(2^n, 2^n - kM, 2^{k+1} - 2^k - t+1, 2^k)$ code generated by Construction FDTW and $X = \{\alpha_1, \alpha_2, \ldots, \alpha_{2k}\} \subseteq C$ formed from the codeword $Z = \{\gamma_1, \gamma_2, \ldots, \gamma_{2k}\} \subseteq \mathbb{C}$, i.e., $X = \beta + Z$ for some $\beta \in \mathbb{F}_2^n$. Then

1) Each element of $X$ is used to form each one of the elements of $Z$ in $T(X)$ (note, that the elements of $Z$ and $T(X)$ coincides, and each element of $Z$ appears exactly $2^{k-1}$ times in $T(X)$, except for $0$ which appears $2^k$ times in $T(X)$).
2) Assume that due to errors, $\tau$ zeroes were changed to ones and $\tau$ ones were changed to zeroes in $X$, and a word $Y$ was formed. Each element of $Y$ which appears also in $X$ is used to form at least $2^k - \tau$ elements of $Z$ in $T(Y)$.
3) Assume that due to errors $\tau$ zeroes were changed to ones and $\tau$ ones were changed to zeroes in $X$, and a word $Y$ was formed. Each element of $Y$ which does not appear in $X$ is used to form at most $\tau$ elements of $Z$ in $T(Y)$.

V. CONCLUSION

We have presented a construction for a constant weight code from a given constant dimension code. Some of the constructed code are optimal constant weight codes. Some constant weight codes are the largest known. The main advantage of the new code is that it has efficient algorithm for error-correction; and if there exists an efficient encoding/decoding algorithm for the related constant dimension code then also the constant weight code has efficient encoding/decoding algorithm.

The main future research in this direction is to construct large constant dimension codes on which we will apply Construction FDTW.

REFERENCES

[1] E. L. Leiss, “Data integrity in digital optical disks”, IEEE Trans. Computers, vol. C-33, pp. 818–827, 1984.
[2] A. R. Calderbank, M. A. Herro, and V. Telang, “A multilevel approach to the design of DC-free line codes”, IEEE Trans. Inform. Theory, vol. IT-35, pp. 579–583, May 1989.
[3] F. R. K. Chung, J. A. Salehi, and V. K. Wei, “Optical orthogonal codes: Design, analysis, and applications”, IEEE Trans. Inform. Theory, vol. IT-35, pp. 595–604, May 1989.
[4] K. A. Immink, Coding techniques for Digital Recorders. London: Prentice-Hall, 1991.
[5] E. Eleftheriou and R. Cideciyan, “OOn codes satisfying Mth order running digital sum constraints”, IEEE Trans. Inform. Theory, vol. IT-37, pp. 1294–1313, 1991.
[6] N. Q. A. L. Gulya, and J. L. Massey, “Constructions of binary constant-weight cyclic codes and cyclically permutable codes”, IEEE Trans. Inform. Theory, vol. IT-38, pp. 940–949, May 1992.
[7] R. M. Roth, P. H. Siegel, and A. Vardy, “High order spectral-null codes constructions and bounds”, IEEE Trans. Inform. Theory, vol. IT-40, pp. 1826–1840, November 1994.
[8] S. M. Johnson, “A new upper bound for error-correcting codes”, IRE Trans. Inform. Theory, vol. IT-8, pp. 202–207, April 1962.
[9] R. M. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko, and N. J. A. Sloane, “Bounds for binary codes of length less than 25”, IEEE Trans. Inform. Theory, vol. IT-24, pp. 81–93, January 1978.
[10] R. L. Graham and N. J. A. Sloane, “Lower bounds for constant weight codes”, IEEE Trans. Inform. Theory, vol. IT-26, pp. 37–43, 1980.
[11] M. J. Colbourn, “Some new upper bounds for constant weight codes”, IEEE Trans. Inform. Theory, vol. IT-26, p. 478, July 1980.
[12] C. M. van Paal and T. Etzion, “New Lower Bounds for Constant Weight Codes”, IEEE Trans. Inform. Theory, vol. IT-35, pp. 1324–1329, 1989.
[13] A. E. Brouwer, James B. Shearer, N. J. A. Sloane, and Warren D. Smith, “A new table of constant weight codes”, IEEE Trans. Inform. Theory, vol. IT-36, pp. 1334–1380, 1990.
[14] E. A. Agrell, A. Vardy, and K. Zeger, “Upper bounds for constant weight codes,” IEEE Trans. Inform. Theory, vol. 46, pp. 2373–2395, 2000.
[15] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes. Amsterdam: North-Holland, 1977.
[16] R. M. Roth, “Spectral-null codes and null spaces of Hadamard submatrices,” Designs, Codes, and Cryptography, vol. 9, pp. 177–191, October 1996.
[17] R. M. Wilson, “Cycloidity and difference families in elementry abelian groups”, Journal Number Theory, vol. 4, pp. 17–47, 1972.
[18] T. Etzion and A. Hartman, “Towards a large set of Steiner quadruple systems”, SIAM Journal on Discrete Mathematics, vol. 4, pp. 182–195, 1991.
[19] A. Hartman and T. K. Phelps, “Steiner quadruple systems”, in J. H. Dinitz and D. R. Stinson, editors, Contemporary design Theory, pp. 205–240, John Wiley and Sons, Inc., 1992.
[20] T. Etzion, “Optimal constant weight codes over $\mathbb{Z}_n$ and generalized designs”, Discrete Mathematics, vol. 169, pp. 55–82, 1997.
[21] S. Blake-Wilson and K. T. Phelps, “Constant weight codes and group divisible designs”, Designs, Codes, and Cryptography, vol. 16, pp. 11–27, January 1999.
[22] J. Li, “Asymptotic determination of the last packing number of quadruples,” Designs, Codes, and Cryptography, vol. 38, pp. 83–95, 2006.
[23] D. E. Knuth, “Efficient balanced codes”, IEEE Trans. Inform. Theory, vol. IT-32, pp. 51–53, January 1986.
[24] L. G. tallini, R. M. capocelli, and B. Bose, “Design of some new balanced codes”, IEEE Trans. Inform. Theory, vol. IT-42, pp. 790–802, 1996.
[25] T. M. Cover, “Enumerative source encoding,” IEEE Trans. Inform. Theory, vol. IT-19, no. 1, pp. 73–77, Jan. 1973.
[26] H. van Tilborg and m. Blaum, On error-correcting balanced codes, IEEE Trans. Inform. Theory, vol. IT-35, no. 5, pp. 1091–1095, Sept. 1989.
[27] T. Etzion, “Constructions of Error-Correcting DC-Free Block Codes”, IEEE Trans. Inform. Theory, vol. IT-36, pp. 899–905, 1990.
[28] R. Omran, O. Moreno, and P. V. Kumar, “Improved Johnson bounds for optical orthogonal codes with $\lambda > 1$ and some optimal constructions,” Proc. IEEE Intern. Symposium Information Theory, Adelaide, Australia, pp. 259–263, September 2005.
[29] O. Moreno, R. Omran, P. V. Kumar, and H.-F. Lu, “A generalized Bose-Chowla family of optical orthogonal code and distinct difference sets,” IEEE Trans. Inform. Theory, vol. IT-53, no. 5, pp. 1907–1910, May 2007.
[30] R. Koetter and F. R. Kschischang, “Coding for errors and erasures in random network coding,” IEEE Trans. Inform. Theory, vol. 54, no. 8, pp. 3579–3591, August 2008.
[31] D. Silva, F. R. Kschischang, and R. Koetter, “A Rank-metric approach to error control in random network coding,” IEEE Trans. Inform. Theory, vol. IT-54, no. 12, pp. 5951–5967, September 2008.
[32] A. Kohnert and S. Kurz, “Construction of large constant dimension codes with a prescribed minimum distance,” Lecture Notes Computer Science, vol. 5393, pp. 31–42, 2008.
[33] T. Etzion and N. Silberstein, “Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams”, *IEEE Trans. Inform. Theory*, vol. IT-55, pp. 2909–2919, July 2009.

[34] S. T. Xia and F. W. Fu, “Johnson type bounds on constant dimension codes,” *Designs, Codes, and Cryptography*, vol. 50, pp. 163–172, 2009.

[35] T. Etzion and A. Vardy, “Error-correcting codes in projective space,” *Proc. IEEE Intern. Symp. Information Theory*, Toronto, Canada, July 2008.

[36] M. Gadouleau and Z. Yan, “Construction and covering properties of constant-dimension codes,” arxiv.org/abs/0903.2675.

[37] V. Skachek, “Recursive code construction for random network,” arxiv.org/abs/0806.3650.

[38] N. Silberstein and T. Etzion, “Representation of Subspaces and Enumerative Encoding of the Grassmannian Space”, arxiv.org/abs/0911.3256.

[39] N. Silberstein and T. Etzion, “Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams”, arxiv.org/abs/1003.4879.

[40] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*. Cambridge University Press, 1992.

[41] T. Bu, “Partitions of a vector space,” *Discrete Math.*, vol. 31, pp. 79–83, January 1980.

[42] S. J. Hong and A. M. Patel, “A general class of maximal codes for computer applications”, *IEEE Trans. Comput.*, vol. C-21, pp. 1322–1331, 1972.

[43] S. Thomas, “Designs over finite fields,” *Geometriae Dedicata*, vol. 21, pp. 237–242, 1987.

[44] T. Etzion, “Perfect byte-correcting codes,” *IEEE Trans. Inform. Theory*, vol. IT-44, pp. 3140–3146, 1998.

[45] M. Schwartz and T. Etzion, “Codes and anticode in the Grassman graph,” *J. Combin. Theory, Series A*, vol. 97, pp. 27–42, 2002.

[46] H. Chung and P. V. Kumar, “Optical orthogonal codes - new bounds and an optimal construction”, *IEEE Trans. Inform. Theory*, vol. IT-36, pp. 866–873, July 1990.

[47] S. Bitan and T. Etzion, “Constructions for optimal constant weight cyclically permutable codes and difference families”, *IEEE Trans. Inform. Theory*, vol. IT-41, pp. 77–87, January 1995.

[48] O. Moreno, Z. Zhang, P. V. Kumar, and V. Zinoviev, “New constructions of optimal cyclically permutable constant weight codes”, *IEEE Trans. Inform. Theory*, vol. IT-41, pp. 448–455, March 1995.

[49] R. Fuji-hara and Y. Miao, “Optical orthogonal codes: their bounds and new optimal constructions”, *IEEE Trans. Inform. Theory*, vol. IT-46, pp. 2396–2406, 2000.

[50] S. Ma and Y. Chang, “Constructions of optimal optical orthogonal codes with weight five”, *Journal of Combinatorial Designs*, vol. 13, pp. 54–69, 2005.