Lemma for Linear Feedback Shift Registers and DFTs Applied to Affine Variety Codes

Hajime Matsui

Abstract

In this paper, we establish a lemma in algebraic coding theory that frequently appears in the encoding and decoding of, e.g., Reed-Solomon codes, algebraic geometry codes, and affine variety codes. Our lemma corresponds to the non-systematic encoding of affine variety codes, and can be stated by giving a canonical linear map as the composition of an extension through linear feedback shift registers from a Gröbner basis and a generalized inverse discrete Fourier transform. We clarify that our lemma yields the error-value estimation in the fast erasure-and-error decoding of a class of dual affine variety codes. Moreover, we show that systematic encoding corresponds to a special case of erasure-only decoding. The lemma enables us to reduce the computational complexity of error-evaluation from $O(n^3)$ using Gaussian elimination to $O(qn^2)$ with some mild conditions on $n$ and $q$, where $n$ is the code length and $q$ is the finite-field size.

Index Terms

Gröbner bases, evaluation codes from order domains, fast decoding, systematic encoding, Berlekamp-Massey-Sakata algorithm.

I. INTRODUCTION

Affine variety codes [8,12,20,28] belong to a naturally generalized class of algebraic geometry (AG) codes, and are also known as evaluation codes from order domains of finitely generated types [1,11,18,19]. It is known [8] that affine variety codes represent all linear codes. On the other hand, Pellikaan et al. [30] have already shown that AG codes, especially codes on algebraic curves, also represent all linear codes. Thus, from the viewpoint of code construction, one might consider only codes on algebraic curves. However, in terms of decoding, it is insufficient to focus only on AG codes, because many efficient decoding algorithms can correct errors up to half the generalized Feng–Rao minimum distance bound $d_{FR}$ [4,27,32,37], which depends on orders among vector basis or monomial basis. Whereas AG codes use a specified order, affine variety codes have the advantage that they can choose their orders flexibly, allowing them to reach potentially good $d_{FR}$ values.

Manuscript submitted October 28, 2012. This work was supported in part by KAKENHI, Grant-in-Aid for Scientific Research (C) (23560478). The material in this paper was presented in part at the 34th Symposium on Information Theory and Its Applications, Ousyuku, Iwate, Japan, Nov. 29–Dec. 2, 2011.

H. Matsui is with Toyota Technological Institute, Hisakata 2–12–1, Tenpaku, Nagoya 468–0034, Japan (e-mail: matsui@toyota-ti.ac.jp).
Pellikaan [31] developed a decoding algorithm for all linear codes using a $t$-error correcting pair and solving a system of linear equations; its computational complexity is of the order $n^3$, where $n$ is the code length. On the other hand, Fitzgerald et al. [8] and Marcola et al. [20] proposed decoding algorithms via the Gröbner basis that correct errors of up to half the minimum distance $[(d_{\min} - 1)/2]$ for affine variety codes. As this type of decoding belongs to the class of NP-hard problems [2], it is possible that the algorithms in [8], [20] do not run in polynomial time.

The decoding of dual affine variety codes up to $[(d_{FR} - 1)/2]$ can be divided into two steps, namely error-location and error-evaluation. For the error-location step, O’Sullivan [4], [7] gave a generalization of the Berlekamp–Massey–Sakata (BMS) algorithm for finding the Gröbner bases of error-locator ideals for affine variety codes. The computational complexity of this algorithm is $zn^2$ (where $z$ is the number of elements in the Gröbner bases), which is less than $n^3$. However, for the error-evaluation step in the decoding, no efficient method with a computational complexity of less than $n^3$ has been found. Although there is a method [18] for error-value estimation based on the generalization of the key equation, its relation to the BMS algorithm has not been clarified, as discussed in page 15 of [18], and its computational complexity has not been determined. Another method that uses the inverse matrix of the proper transform was introduced by Saints et al. [34], but its computational complexity is of the order $n^3$, because the inverse matrix must be computed for each error-evaluation step per decoding. Thus, there is currently no efficient method for error-value estimation in conjunction with the BMS algorithm.

The contents of this paper can be divided into three parts. First, we realize a generalization of the $N$-dimensional ($N$-D) discrete Fourier transform (DFT) and its inverse (IDFT) over finite fields, where $N$ is a positive integer. Let $q$ be a prime power, $\mathbb{F}_q$ be the finite field of $q$ elements, $\mathbb{F}_q^\times = \mathbb{F}_q \backslash \{0\}$, $(\mathbb{F}_q^\times)^N$ be the set of all $N$-tuples of elements in $\mathbb{F}_q^\times$, and $\mathbb{F}_q^N$ be similar to $(\mathbb{F}_q^\times)^N$. Whereas the conventional $N$-D DFT and IDFT over finite fields are defined upon vectors whose components are indexed by $(\mathbb{F}_q^\times)^N$, our generalized transforms are defined upon vectors whose components are indexed by $\mathbb{F}_q^N$, and agree with the conventional ones if they are restricted to $(\mathbb{F}_q^\times)^N$. In particular, our generalized transforms satisfy the Fourier inversion formulae; the inclusion-exclusion principal plays an essential role in their proofs.

Secondly, we prove a lemma, which we call Main Lemma, concerning the linear feedback shift registers made by Gröbner bases and the generalized IDFT. Intuitively, Main Lemma corresponds to the encoding of affine variety codes with zero-dimensional information. We reveal that Main Lemma describes not only non-systematic and systematic encoding but also the error-value estimation. More specifically, Main Lemma provides a canonical isomorphic map from one vector space, consisting of vectors whose components are indexed by $D(\Psi)$, onto another vector space consisting of vectors whose components are indexed by $\Psi$. Here, for any subset $\Psi$ of $\mathbb{F}_q^N$, $D(\Psi)$ is the delta set (or footprint) of the Gröbner basis for an ideal of $N$-variable polynomials over $\mathbb{F}_q$ that have zeros at $\Psi$. Although these two vector spaces have the same dimension and are obviously isomorphic, our Main Lemma asserts that there is a canonical one-to-one map that does not depend on the choice of the bases of the vector spaces. This canonical isomorphic map can be explicitly written as the composition of the generalized IDFT after a map coming from the linear recurrence relations given by the Gröbner bases. The inverse of this canonical isomorphic map agrees with
the proper transform introduced by Saints et al. [34].

Finally, Main Lemma is applied to affine variety codes in the following three topics. The first is the construction of affine variety codes, specifically their non-systematic encoding. Usually, the parity check matrices of affine variety codes must be derived from their generator matrices through matrix elimination. Using Main Lemma, we directly construct the dual affine variety codes as images of the canonical isomorphic map; this is analogous to the direct construction of affine variety codes as the images of the evaluation map. The second topic is the error-value estimation in the fast erasure-and-error decoding of a class of dual affine variety codes. We show that there is an efficient error-value estimation in conjunction with the BMS algorithm. Our method corresponds to a generalization of the methods of Sakata et al. [35], [36] for error-value estimation by DFT in case of one-point AG codes from algebraic curves, a subclass of AG codes. The final topic is the systematic encoding of the class of dual affine variety codes and the improved erasure-correcting capability. If a linear code has a non-trivial automorphism group, then it can be encoded systematically by the method of Heegard et al. [14] and Little [19]. Our systematic encoding does not use any automorphism group, and is applicable to a sufficiently wide class of dual affine variety codes. Moreover, we reveal that systematic encoding is a special type of erasure-only decoding; this fact is well-known in the case of maximum-distance codes [3], and is shown for the class of dual affine variety codes.

The content of this paper is attributable to the author, except for the definition of proper transforms [34], the definition of affine variety codes [8], and the error-value estimation of AG codes [35], [36]. This other content is still the author’s work, even for the limited case of AG codes. Some of the results in this paper have already been presented in [25]. The crucial advantage of this paper over [25] is that we can apply a multidimensional (m-D) DFT algorithm [3] to the generalized DFT and IDFT in order to reduce their computational complexities. Whereas both computational complexities are estimated as order \( nNq^N \) in [25], we reduce this to order \( Nq^{N+1} \); if \( n ≥ q \), then the order is actually improved. For practical use, a faster DFT algorithm, which has less complexity, is adopted. Thus, the results in [25] are sufficiently extended in this paper to enable us to implement it. On the other hand, if one adopts the conventional N-D DFT and IDFT over \( (F_q^n)^N \) in place of our generalized transforms, the results in [25] then correspond to the special cases of our Main Lemma and its application to a subclass of dual affine variety codes.

As mentioned above, because the isomorphic map of Main Lemma is equivalent to the inverse map of the proper transform in [34], the above applications to affine variety codes can also be performed by multiplying by the inverse matrix of the proper transform. Nevertheless, our IDFT-based expression of the inverse map enables us to reduce the computational complexity; moreover, this can be reduced further by applying an m-D DFT algorithm or FFT. Whereas the computational complexity of the error-value estimation with Gaussian elimination is of the order \( n^3 \), that with the proposed method has an upper bound of the order \( nq^N \), which is equivalent to \( qn^2 \) because \( N \) can be chosen as \( q^{N-1} < n ≤ q^N \). Thus, our generalized IDFT and Main Lemma are not only important in the theory of affine variety codes, but are also useful in reducing the computational complexity of their error-value estimation.

The rest of this paper is organized as follows. In Section II, we prepare some notation for the subsequent discussions. Section III gives a generalization of DFTs from \( (F_q^n)^N \) to \( F_q^N \). In Section IV, we state Main Lemma;
Subsection [IV-A] defines two vector spaces via Gröbner bases, Subsection [IV-B] defines the map from the linear 
feedback shift registers given by Gröbner bases, and Subsection [IV-C] gives an isomorphism between the two vector 
spaces. In Section [V], we apply the lemma to construct affine variety codes, reformulate erasure-and-error decoding 
algorithms, and determine the relation between systematic encoding and erasure-only decoding. In Section [VI], we 
estimate the number of finite-field operations in our algorithm; Subsection [VI-A] uses a simple count and Subsection 
[VI-B] applies an m-D DFT algorithm. Section [VII] concludes the paper.

II. NOTATION

Throughout this paper, the following notation is used. Let \( \mathbb{N}_0 \) be the set of non-negative integers. For two sets 
\( A \) and \( B \), a set \( A \setminus B \) is defined as \( \{ u \in A \mid u \notin B \} \). For an arbitrary finite set \( S \), the number of elements in \( S \) is 
represented by \( |S| \), and let \( V_S = \{(v_s)_S \mid s \in S, v_s \in \mathbb{F}_q \} \) denote an \( |S| \)-dimensional vector space over \( \mathbb{F}_q \) whose 
components are indexed by elements of \( S \). \(^2\) Although a vector \( (v_s)_S \in V_S \) is usually denoted as \( (v_s)_{s \in S} \), in this paper we use \( (v_s)_S \) in place of \( (v_s)_{s \in S} \) for simplicity. Because we have to treat different vectors, e.g., \( (r_s)_S \), \( (u_s)_S \), 
\( (v_s)_S \in V_S \), we judge from the index \( (s)_S \) if they belong to \( V_S \). Unless otherwise noted, for any arbitrary subset \( R \subseteq S \), the vector space \( V_R \) is considered to be a subspace of \( V_S \) given by \( V_R = \{(v_s)_S \in V_S \mid v_s = 0 \text{ for all } s \in S \setminus R \} \). 
A map \( f \) from a set \( A \) into a set \( B \) is represented by 
\[
f : A \rightarrow B \quad [a \mapsto f(a)].
\]

III. FOURIER-TYPE TRANSFORMS ON \( \mathbb{F}_q^N \)

A. Definitions

Let \( N \) be a positive integer and let 
\[
A = A_N = \{0, 1, \cdots, q - 1\}^N = \{a = (a_1, \cdots, a_N) \mid a_1, \cdots, a_N \in \{0, 1, \cdots, q - 1\}\},
\]
\[
\Omega = \Omega_N = \mathbb{F}_q^N = \{\omega = (\omega_1, \cdots, \omega_N) \mid \omega_1, \cdots, \omega_N \in \mathbb{F}_q\}.
\]

In this section, Fourier-type transforms are defined as maps between vector spaces, both of which have \( \dim \mathbb{F}_q^N \). \(^3\)

\[
V_A = \{(h_{\omega})_A \mid \omega \in A, h_{\omega} \in \mathbb{F}_q\},
\]
\[
V_\Omega = \{(c_{\omega})_\Omega \mid \omega \in \Omega, c_{\omega} \in \mathbb{F}_q\}.
\]

**Definition 1: (Generalization of the m-D DFT over \( \mathbb{F}_q \))** A linear map \( \mathcal{F} \) is defined by

\[
\mathcal{F} : V_\Omega \rightarrow V_A \quad \left[ (c_{\omega})_\Omega \mapsto \left( \sum_{\omega \in \Omega} c_{\omega} \omega^{-A} \right)_A \right],
\]

\(^1\)A list of main notation is given as Table III in appendix.

\(^2\)In [34], \( V_S \) is denoted by \( (\mathbb{F}_q)^S \), and \((v_s)_S \in V_S \) is denoted simply by \( c \in (\mathbb{F}_q)^S \); in this paper, because we must distinguish several 
types of vectors and indexes, we adopt \( (v_s)_S \in V_S \).

\(^3\)In Subsection III-A, the only vector spaces that we will use are \( V_A \) and \( V_\Omega \), whose vectors are represented by \( (h_{\omega})_A \in V_A \) and \( (c_{\omega})_\Omega \in V_\Omega \), 
respectively.
Then, we have

\[
\mathbf{C}_{(\omega_1, \omega_2)}^{a_1} \mathbf{C}_{(\omega_1, \omega_2)}^{a_2} = \mathbf{C}_{(\omega_1, \omega_2)}^{a_1 \cdot a_2} = \mathbf{C}_{(\omega_1, \omega_2)}^{a_1} \mathbf{C}_{(\omega_1, \omega_2)}^{a_2} \quad a_1, a_2 \neq 0
\]

\[
\mathbf{C}_{(\omega_1, \omega_2)}^{a_1} = \mathbf{C}_{(\omega_1, \omega_2)}^{a_2} = \mathbf{C}_{(\omega_1, \omega_2)}^{a_3} = \mathbf{C}_{(\omega_1, \omega_2)}^{a_4} = \mathbf{C}_{(\omega_1, \omega_2)}^{a_5} = \mathbf{C}_{(\omega_1, \omega_2)}^{a_6} = \mathbf{C}_{(\omega_1, \omega_2)}^{a_7} = 0 \quad a_1 = 0, a_2 = 0
\]

Assume \( N = 2 \). Then, for each \( \mathbf{a} = (a_1, a_2) \in A \), \( (h_{(a_1, a_2)})_A = \mathbf{F}((c_{(\omega_1, \omega_2)})_{\Omega}) \in V_A \) can be directly written as

\[
h_{(a_1, a_2)} = \begin{cases} 
\sum_{\omega \in \Omega} c_\omega \mathbf{C}_\omega^{a_1} \mathbf{C}_\omega^{a_2} = \sum_{\omega \in \Omega, \omega \neq 0} c_\omega \mathbf{C}_\omega^{a_1 \cdot a_2} & a_1, a_2 \neq 0 \\
\sum_{\omega \in \Omega} c_\omega & a_1 = 0, a_2 = 0 \\
\sum_{\omega \in \Omega} c_\omega \mathbf{C}_\omega^{a_1} & a_1 = 0, a_2 \neq 0 \\
\sum_{\omega \in \Omega} c_\omega \mathbf{C}_\omega^{a_2} & a_1 \neq 0, a_2 = 0 \\
\sum_{\omega \in \Omega} c_\omega \mathbf{C}_\omega^{a_1 a_2} & a_1 = a_2 = 0.
\end{cases}
\]

Remark 1: If we fix the orders of the elements in \( A \) and \( \Omega \), then the matrix representation of \( \mathbf{F} \) follows easily from (3). This matrix is used in Appendix B. Although the operation of \( \mathbf{F} \) by multiplying this matrix does not always give the minimum computational complexity as shown in Subsection VII-B, we use this matrix as a demonstration for the simple case of \( N = 1 \) and \( q = 8 \). Let \( \alpha \in \mathbb{F}_8 \) be \( \alpha^3 + \alpha + 1 = 0 \). Then, we have \( A = \{0, 1, \cdots, 7\} \) and \( \Omega = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^6\} \), and fix these orders. In this remark, we consider \( (h_\alpha)_A \) and \( (c_\omega)_{\Omega} \) as row vectors \( (h_\alpha)_A = (h_0, h_1, \cdots, h_7) \) and \( (c_\omega)_{\Omega} = (c_0, c_1, c_\alpha, \cdots, c_{\alpha^6}) \). According to (4), we can determine \( (h_\alpha)_A = \mathbf{F}((c_\omega)_{\Omega}) \) by

\[
(h_\alpha)_A = (c_\omega)_{\Omega} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & 1 \\
1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 & 1 \\
1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 & 1 \\
1 & \alpha^4 & \alpha^1 & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 & 1 \\
1 & \alpha^5 & \alpha^3 & \alpha^1 & \alpha^6 & \alpha^4 & \alpha^2 & 1 \\
1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 & 1 \\
\end{bmatrix}.
\]

Definition 2: (Generalization of the m-D IDFT over \( \mathbb{F}_q \)) For each \( \omega \in \Omega \), a subset \( I = I_\omega = \{i_1, \cdots, i_m\} \) of \( \{1, 2, \cdots, N\} \) is determined such that \( \omega_{i_1} \cdots \omega_{i_m} \neq 0 \) and \( \omega_i = 0 \) for all \( i \in \{1, 2, \cdots, N\} \setminus I \). A linear map \( \mathbf{F}^{-1} \) is then defined by

\[
\mathbf{F}^{-1} : V_A \to V_\Omega \quad [(h_\omega)_A \mapsto (c_\omega)_{\Omega}],
\]

(5)
where
\[ c_{\omega} = (-1)^m \sum_{l_1, \ldots, l_m=1}^{q-1} \left\{ \sum_{J \subseteq \{1, 2, \ldots, N\} \setminus I} (-1)^{|J|} h_{I,J} \right\} \omega_{l_1}^{-i_1} \cdots \omega_{l_m}^{-i_m}, \]
(6)

\( J \) in the sum runs over all subsets of \( \{1, 2, \ldots, N\} \setminus I \), and \( \omega(I,J) = (b_1, \ldots, b_N) \in A \) is defined by, for \( 1 \leq i \leq N \),
\[ b_i = \begin{cases} l_i & i \in I \\ q-1 & i \in J \\ 0 & i \in \{1, 2, \ldots, N\} \setminus (I \cup J). \end{cases} \]

The linear map \( F^{-1} : V_A \to V_\Omega \) of (5) is called a generalized IDFT on \( \mathbb{F}_q^N \). For example, if \( \omega_1 \cdots \omega_N \neq 0 \) for \( \omega = (\omega_1, \ldots, \omega_N) \in \Omega \), then \( I \) is equal to \( \{1, 2, \ldots, N\} \) and there is only one choice of \( J = \emptyset \). In this case, definition (5) implies
\[ c_{\omega} = (-1)^N \sum_{l_1, \ldots, l_N=1}^{q-1} h_{(l_1, \ldots, l_N)} \omega_{l_1}^{-i_1} \cdots \omega_{l_N}^{-i_N}, \]
in other words, \( F^{-1} \) agrees with the \( N \)-D IDFT if \( \Omega \) is restricted to \( (\mathbb{F}_q^N)^N \). In general, for each \( \omega \in \Omega \), the value \( c_{\omega} \) in (6) is equal to a linear combination of IDFTs whose dimensions do not exceed \( N \).

**Example 2:** Assume \( N = 1 \). If \( \omega \neq 0 \in \Omega \), then \( I = \{1\} \subseteq \{1\}, J = \emptyset \subseteq \{1\} \setminus I = \emptyset \), and \( \omega(I,J) = l_1 = i \).
If \( \omega = 0 \in \Omega \), then \( I = \emptyset \subseteq \{1\}, J = \emptyset \) or \( \{1\} \subseteq \{1\} \setminus I = \{1\} \), and \( \omega(I,J) = 0, q-1 \), respectively. Thus, \( F^{-1}((h_{a,})_A) = (c_{\omega})_\Omega \in V_\Omega \) can be directly written as
\[ c_{\omega} = \begin{cases} - \sum_{i=1}^{q-1} h_i \omega^{-i} & \omega \neq 0 \\ h_0 - h_{q-1} & \omega = 0. \end{cases} \]
(7)

Assume \( N = 2 \). For \( \omega = (\omega_1, \omega_2) \in \Omega \), e.g., if \( \omega_1 \omega_2 \neq 0 \), then \( I = \{1, 2\} \subseteq \{1, 2\}, J = \emptyset \subseteq \{1, 2\} \setminus I = \emptyset \), and \( \omega(I,J) = (l_1, l_2) = (i, j) \); if \( \omega_1 \neq 0 \) and \( \omega_2 = 0 \), then \( I = \{1\} \subseteq \{1, 2\}, J = \emptyset \) or \( \{2\} \subseteq \{1, 2\} \setminus I = \{2\} \), and \( \omega(I,J) = \omega(I) = (i, 0), (i, q-1) \), respectively. Thus, \( F^{-1}((h_{a,})_A) = (c_{(\omega_1, \omega_2)})_\Omega \in V_\Omega \) can be directly written as
\[ c_{(\omega_1, \omega_2)} = \begin{cases} \sum_{i,j=1}^{q-1} h_{(i,j)} \omega_1^{-i} \omega_2^{-j} & \omega_1 \omega_2 \neq 0 \\ - \sum_{i=1}^{q-1} (h_{(i,0)} - h_{(i,q-1)}) \omega_1^{-i} & \omega_1 \neq 0, \omega_2 = 0 \\ - \sum_{j=1}^{q-1} (h_{(0,j)} - h_{(q-1,j)}) \omega_2^{-j} & \omega_1 = 0, \omega_2 \neq 0 \\ h_{(0,0)} - h_{(0,q-1)} - h_{(q-1,0)} + h_{(q-1,q-1)} & \omega_1 = \omega_2 = 0. \end{cases} \]

In general, the summand in each condition of \( c_{\omega} \) consists of \( 2^{N-m} \) terms, where \( m \) is the number of non-zero components in \( \omega \).
B. Properties

Proposition 1: (Generalization of the Fourier inversion formulae) Two linear maps \( \mathcal{F} : V_\Omega \rightarrow V_A \) and \( \mathcal{F}^{-1} : V_A \rightarrow V_\Omega \) are the inverse of each other, i.e., \( \mathcal{F}^{-1} ( \mathcal{F} ( (c_\omega)_\Omega) ) = (c_\omega)_\Omega \) and \( \mathcal{F} ( \mathcal{F}^{-1} ( (h_\omega)_A) ) = (h_\omega)_A \). The proof is described in Appendix A. This proposition corresponds to one of the basic concepts in this paper.

Remark 2: (Continued from Remark 1) According to (7), we can determine \( (c_\omega)_\Omega = \mathcal{F}^{-1} ((h_\omega)_A) \) by

\[
(c_\omega)_\Omega = (h_\omega)_A
\]

As a consequence of Proposition 1, this matrix is equal to the inverse of the matrix that appeared in Remark 1; actually, this can be directly checked.

The next property is dimensional induction. The results obtained in the rest of this subsection are not used before Subsection VI-B. As observed in Examples 1 and 2, computing the values \( \mathcal{F} ( (c_\omega)_\Omega) \) and \( \mathcal{F}^{-1} ( (h_\omega)_A) \) according to their definitions is not simple. We will show in Section VI that computational complexities of these values are of the order \( Nq^{2N} \), which is significantly high among the other computational procedures. On the other hand, the m-D DFT algorithm \( [3] \) is applied to conventional DFT and IDFT over \( (F_q^N)^N \) and their complexities are reduced. We now show that the algorithm can also be applied to our generalized DFT and IDFT and that they can be computed inductively from low-dimensional DFTs and IDFTs. In the rest of this subsection, we index \( \mathcal{F}_N = \mathcal{F} : V_{\Omega_N} \rightarrow V_{A_N} \) and \( \mathcal{F}_N^{-1} = \mathcal{F}^{-1} : V_{A_N} \rightarrow V_{\Omega_N} \) because we will treat generalized DFTs and IDFTs in different dimensions.

Proposition 2: (Reduction to low dimensional DFTs) If \( N \geq 2 \), then the generalized DFT \( \mathcal{F}_N \) in (6) can be computed from \( \mathcal{F}_1 \) and \( \mathcal{F}_{N-1} \) as

\[
\mathcal{F}_N ( (c_{\omega\omega_N})_{\Omega_N} ) = (h_\omega a_N)_{A_N}, \quad \text{where}
\]

\[
(h_\omega a_N)_{A_1} = \mathcal{F}_1 ( (v_{\omega\omega_N})_{\Omega_1} ) \quad \text{for all } a \in A_{N-1},
\]

\[
(v_{\omega\omega_N})_{A_{N-1}} = \mathcal{F}_{N-1} ( (c_{\omega\omega_N})_{\Omega_{N-1}} ) \quad \text{for all } \omega_N \in \Omega_1,
\]

and, from \( (c_{\omega\omega_N})_{\Omega_{N-1}} \), we define \( (c_{\omega\omega_N})_{\Omega_N} \) by \( c_{\omega\omega_N} = c_{\omega_1, \cdots, \omega_{N-1}, \omega_N} \) with \( \omega = (\omega_1, \cdots, \omega_{N-1}) \in \Omega_{N-1} \) and fixed \( \omega_N \in \Omega_1 \).

The proof of this proposition is immediately obtained from Definition 1; we give an additional explanation in Subsection VI-B. Note that (8) is not the usual composition map of \( \mathcal{F}_1 \) and \( \mathcal{F}_{N-1} \); however, (9) and (10) mean to calculate \( \mathcal{F}_1 q^{N-1} \)-times after calculating \( \mathcal{F}_{N-1} q \)-times. It is also noted that, if \( N \geq 2 \), then there are many ways to decompose \( \mathcal{F}_N \) into the lower dimensional DFTs. Applying Proposition 2 repeatedly, it is possible to compute \( \mathcal{F}_N \) only by using \( \mathcal{F}_1 \), and achieve the least computational complexity as shown in Subsection VI-B.
Proposition 3: (Reduction to low dimensional IDFTs) If \( N \geq 2 \), then the generalized IDFT \( \mathcal{F}_N^{-1} \) in (5) can be computed from \( \mathcal{F}_1^{-1} \) and \( \mathcal{F}_{N-1}^{-1} \) as

\[
\mathcal{F}_N^{-1} \left( (h_{\mathbb{A},a_N})_{A_N} \right) = (c_{\omega,a_N})_{\Omega_N}, \quad \text{where}
\]

\[
(c_{\omega,a_N})_{\Omega_N} = \mathcal{F}_1^{-1} \left( (v_{\omega,a_N})_{A_1} \right) \quad \text{for all } \omega \in \Omega_N - 1,
\]

\[
(v_{\omega,a_N})_{\Omega_N-1} = \mathcal{F}_{N-1}^{-1} \left( (h_{\mathbb{A},a_N})_{A_{N-1}} \right) \quad \text{for all } a_N \in A_1,
\]

and, from \( (h_{\mathbb{A},a_N})_{A_N} \), we define \( (h_{\mathbb{A},a_N})_{A_{N-1}} \) by \( h_{\mathbb{A},a_N} = h(a_1, \ldots, a_{N-1}, a_N) \) with \( a = (a_1, \ldots, a_{N-1}) \in A_{N-1} \) and fixed \( a_N \in A_1 \).

The proof of this proposition is obvious because of Proposition [1] It is remarkable that \( \mathcal{F}_1^{-1} \) and \( \mathcal{F} \) have the same inductive expressions even though the summand of \( \mathcal{F}_1^{-1} \) is more complex than that of \( \mathcal{F} \). Similar to \( \mathcal{F}_N \), the complexity computing \( \mathcal{F}_N^{-1} \) is minimized by using only \( \mathcal{F}_1^{-1} \) in all available methods; these estimations will be performed in Section [VI]. As shown in Fig. [1], if we represent \( (h_{\mathbb{A}})_A \) two-dimensionally according to \( A = \{0, 1, \ldots, q - 2\}^2 \), then Proposition [3] in case \( N = 1 \) insists that \( \mathcal{F}_2^{-1} \) is decomposed to the vertical operation of \( \mathcal{F}_1^{-1} \) for all \( a_1 \) and the horizontal operation of \( \mathcal{F}_1^{-1} \) for all \( a_2 \), where \( (a_1, a_2) \in A_2 \) and the resulting value is trivially independent of the order of two operations.

Example 3: For a given \( (h_{(a_1,a_2)})_{A_2} \), all values of the m-D DFT algorithm are shown in Fig. [1], where the vertical and the horizontal axes \((0,1,\ldots,7)\) in \( (h_{(a_1,a_2)})_{A_2} \) denote \( a_1 \) and \( a_2 \) of \( a = (a_1, a_2) \in A_2 \), the vertical axis \((-1,0,\ldots,6)\) and the horizontal axis \((0,1,\ldots,7)\) in \( (v_{(\omega_1,a_2)})_{\Omega_1 \times A_1} \) denote \( \omega_1 \) and \( a_2 \) of \( (\omega_1, a_2) \in \Omega_1 \times A_1 \), and those axes \((-1,0,\ldots,6)\) in \( (c_{(\omega_1,\omega_2)})_{\Omega_2} \) denote \( \omega_1 \) and \( \omega_2 \). at \( \omega_2 = \omega_1 \in \Omega_2 \). At the first step, the first three values of \( \mathcal{F}_1^{-1} \left( (h_{(a_1,a_2)})_{A_1} \right) = (v_{(\omega_1,a_2)})_{\Omega_1} \) at \( a_2 = 0 \) are obtained as

\[
v_{(-1,0)} = h_{(0,0)} + h_{(1,0)} = \alpha^4 + \alpha^2 = \alpha,
\]

\[
v_{(0,0)} = h_{(1,0)} + h_{(2,0)} + h_{(3,0)} + h_{(4,0)} + h_{(5,0)} + h_{(6,0)} + h_{(7,0)}
\]

\[
= \alpha^5 + \alpha + \alpha^3 + 1 + 0 + \alpha^2 = \alpha^2,
\]

\[
v_{(1,0)} = h_{(1,0)} \alpha^6 + h_{(2,0)} \alpha^5 + h_{(3,0)} \alpha^4 + h_{(4,0)} \alpha^3 + h_{(5,0)} \alpha^2 + h_{(6,0)} \alpha + h_{(7,0)}
\]

\[
= \alpha^5 \alpha^6 + \alpha^5 \alpha + \alpha^4 \alpha^3 + \alpha^2 + 0 + \alpha^2 = \alpha^6.
\]

At the second step, the first three values of \( \mathcal{F}_1^{-1} \left( (v_{(\omega_1,a_2)})_{A_1} \right) = (v_{(\omega_1,\omega_2)})_{\Omega_1} \) at \( \omega_1 = 0 \) are obtained as

\[
c_{(-1,0)} = v_{(-1,0)} + v_{(-1,7)} = \alpha + \alpha^2 = \alpha^2,
\]

\[
c_{(-1,1)} = v_{(-1,1)} + v_{(-1,2)} + v_{(-1,3)} + v_{(-1,4)} + v_{(-1,5)} + v_{(-1,6)} + v_{(-1,7)}
\]

\[
= \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^6 + \alpha^5 + \alpha^4 = 0,
\]

\[
c_{(-1,1)} = v_{(-1,1)} \alpha^6 + v_{(-1,2)} \alpha^5 + v_{(-1,3)} \alpha^4 + v_{(-1,4)} \alpha^3 + v_{(-1,5)} \alpha^2 + v_{(-1,6)} \alpha + v_{(-1,7)}
\]

\[
= \alpha^3 \alpha^4 + \alpha^2 \alpha^5 + \alpha \alpha^4 + \alpha^3 + \alpha^6 \alpha + \alpha^5 \alpha + \alpha^4 = 0.
\]
Fig. 1. Numerical example of the m-D DFT algorithm; the details are described in Example 3. The non-zero elements of $F_8$ are represented by the number of powers of a primitive element $\alpha$ with $\alpha^3 + \alpha + 1 = 0$, i.e., $0, 1, \ldots, 6$ means $\alpha^0, \alpha^1, \ldots, \alpha^6$, respectively, and $-1$ means $0 \in F_8$. The first $F^{-1}_1$ and $F_1$ mean that the generalized IDFT and DFT are performed for all columns, and the second ones mean that they are performed for all rows. As a result, $F^{-1}_2 \left( \left( h_{(a_1,a_2)} \right)_{A_2} \right) = \left( c_{(\omega_1,\omega_2)} \right)_{\Omega_2}$ and $\left( h_{(a_1,a_2)} \right)_{A_2} = F_2 \left( \left( c_{(\omega_1,\omega_2)} \right)_{\Omega_2} \right)$ are verified.

In this numerical example, we first compute $F^{-1}_1$ vertically and then compute $F^{-1}_1$ horizontally; these two computations with the reverse order also give the same value. □

Remark 3: Because we deduce Propositions 2 and 3 from Definitions 1 and 2, we may conversely define our generalized DFT and IDFT by induction on dimension $N$. Then, the inductive step is performed using the formulae (8)–(13) in Propositions 2 and 3. Moreover, Fourier inversion formulae for general $N$ are deduced from these formulae only for $N = 1$, and the equalities (3) and (5) in Definitions 1 and 2 are also deduced from the simplest cases (4) and (7). Because Definitions 1 and 2 provide a procedure to compute each value point by point, one can compute the value on a part of $A$ and $\Omega$ using (3) and (5). On the other hand, if we adopt the inductive expressions, then we must compute the value on a whole $A$ or $\Omega$. These two methods will be compared in Section VI, and the latter one has less computational complexity in our applications. □
Another property of our generalized DFT is that its transposed map is equal to the evaluation map of $N$-variable polynomials; see Remark 4.

IV. MAIN LEMMA

A. Two vector spaces $V_D$ and $V_\Psi$

Let $\Psi \subseteq \Omega$ with $\Psi \neq \emptyset$ and $n = |\Psi|$. One of the two vector spaces in the lemma is given by

$$V_\Psi = \left\{ \left( c_\varphi \right)_\varphi \mid \varphi \in \Psi, c_\varphi \in \mathbb{F}_q \right\},$$

namely, $V_\Psi$ is the vector space over $\mathbb{F}_q$ indexed by the elements of $\Psi$ whose dimension is trivially $n$. The other of the two vector spaces is somewhat complicated to define, as it requires Gröbner basis theory [6]. Let $\mathbb{F}_q[x]$ be the ring of polynomials with coefficients in $\mathbb{F}_q$ whose variables are $x_1, \cdots, x_N$. Let $Z_\Psi$ be an ideal of $\mathbb{F}_q[x]$ defined by

$$Z_\Psi = \left\{ f(x) \in \mathbb{F}_q[x] \mid f(\psi) = 0 \text{ for all } \psi \in \Psi \right\}.$$  

Note that $x_i^q - x_i \in Z_\Psi$ for all $1 \leq i \leq N$, as $\Psi \neq \emptyset$. We fix a monomial order $\preceq$ of $\{ x^d \mid d \in \mathbb{N}_0^N \}$ [6], and then denote, for $f(x) \in \mathbb{F}_q[x]$,

$$\text{LM}(f) = \max \left\{ x^d \mid d \in \mathbb{N}_0^N, f_d \neq 0 \right\} \quad (14)$$

if $f(x) = \sum_{d \in \mathbb{N}_0^N, f_d \neq 0} f_d x^d \in \mathbb{F}_q[x]$ and $f(x) \neq 0$,

where $x^d = x_1^{d_1} \cdots x_N^{d_N}$ for $d = (d_1, \cdots, d_N) \in \mathbb{N}_0^N$, and $\text{LM}(f)$ is called the leading monomial of $f(x) \in \mathbb{F}_q[x]$. The delta set $D = D(\Psi) \subseteq \mathbb{N}_0^N$ of $Z_\Psi$ for $\Psi$ [54] is then defined by

$$D = D(\Psi) = \mathbb{N}_0^N \setminus \{ \text{mdeg (LM}(f)) \mid 0 \neq f(x) \in Z_\Psi \},$$

where $\text{mdeg } (x^d) = d \in \mathbb{N}_0^N$. Fortunately, $D(\Psi)$ has an intuitive description if a Gröbner basis $G_\Psi$ of $Z_\Psi$ is obtained; it corresponds to the area surrounded by $\text{LM}(G_\Psi)$. The delta set $D = D(\Psi) \subseteq \mathbb{N}_0^N$ of $Z_\Psi$ for $\Psi$ is equivalently defined by

$$\{ x^d \mid d \in D(\Psi) \} = \{ x^d \mid d \in \mathbb{N}_0^N \} \setminus \{ \text{LM}(f) \mid 0 \neq f(x) \in Z_\Psi \}.$$ 

The other of the two vector spaces is then given by

$$V_D = V_D(\Psi) = \left\{ \left( h_\Delta \right)_\Delta \mid \Delta \in D(\Psi), h_\Delta \in \mathbb{F}_q \right\},$$

Because we have used the vector notation $(c_\varphi)_{\varphi} \in V_D$ and $V_\Psi$ is a subspace of $V_D$ as noted in Section II, we represent a vector in $V_D$ as $(c_\varphi)_{\varphi}$ using the same $c$.

Because we have used the vector notation $(h_\Delta)_{\Delta} \in V_A$ and $V_D$ is a subspace of $V_A$ as noted in Section II, we represent a vector in $V_D$ as $(h_\Delta)_{\Delta}$ using the same $h$.
namely, the vector space over $\mathbb{F}_q$ indexed by the elements of $D(\Psi)$. It is known \[8\] that the evaluation map

$$ev : \mathbb{F}_q[x]/Z_\Psi \rightarrow V_\Psi \quad \left[ f(x) \mapsto (f(\psi))_{\Psi} \right]$$  \hspace{1cm} (15)

is isomorphic. Because $\{ x^d \mid d \in D(\Psi) \}$ is a basis of the quotient ring $\mathbb{F}_q[x]/Z_\Psi$ viewed as a vector space over $\mathbb{F}_q$, $\mathbb{F}_q[x]/Z_\Psi$ is isomorphic to $V_D$. Thus, the map (15) can also be written as

$$ev : V_D \rightarrow V_\Psi \quad \left[ (h_d)_D \mapsto \left( \sum_{d \in D} h_d x^d \right)_{\Psi} \right].$$  \hspace{1cm} (16)

In particular, it follows from the isomorphism (15) or (16) that $|D(\Psi)| = |\Psi|$ and $\dim_\mathbb{F}_q V_D = n$.

Because $V_D$ and $V_\Psi$ have the same dimension $n$, it is trivial that $V_D$ is isomorphic to $V_\Psi$ as a vector space over $\mathbb{F}_q$. However, this type of isomorphic maps depends on the choice of the bases of the vector spaces; additionally, in coding theory, the normal orthogonal basis is not always convenient for encoding and decoding. Our lemma asserts that there is a canonical isomorphic map that does not depend on the bases. As explained in Introduction, the isomorphic map $V_D \rightarrow V_\Psi$ of the lemma is given by the composition of the extension defined in the next subsection and the IDFT.

Consider another linear map $\mathcal{P}$ given by

$$\mathcal{P} : V_\Psi \rightarrow V_D \quad \left[ (c_\psi)_\Psi \mapsto \left( \sum_{\psi \in \Psi} c_\psi x^\omega \right)_D \right],$$  \hspace{1cm} (17)

which is called a proper transform \[34\].

**Proposition 4: (Relation between $ev$ and $\mathcal{P}$)** If the normal orthogonal bases are taken as those of $V_D$ and $V_\Psi$, then the two matrices that represent $ev : V_D \rightarrow V_\Psi$ in (16) and $\mathcal{P} : V_\Psi \rightarrow V_D$ in (17) are the transpose of each other. □

The proof is described in Appendix \[8\]. It follows from Proposition 4 that $\mathcal{P}$ is also isomorphic; this fact is noted in \[34\].

**Remark 4:** (Continued from Remark 2) In this remark, we consider the case $\Psi = \Omega$, and describe the relation among $ev$, $\mathcal{P}$, and $\mathcal{F}$. It follows from $\mathcal{G}_\Omega = \{ x_i^q - x_i \mid 1 \leq i \leq N \}$ that $D(\Omega) = A$. Then, $ev$ becomes the map between $V_A \rightarrow V_\Omega$. On the other hand, $\mathcal{P} : V_\Omega \rightarrow V_A$ is equivalent to $\mathcal{F}$. Thus, Proposition 4 implies that $ev : V_A \rightarrow V_\Omega$ is the transposed map of $\mathcal{F} : V_\Omega \rightarrow V_A$. We now demonstrate this fact for the simple case of $N = 1$ and $q = 8$. Because $\{ 1, x, x^2, \cdots, x^7 \}$ is a basis of the quotient ring $\mathbb{F}_8[x]/Z_\Omega$ viewed as a vector space over $\mathbb{F}_8$ isomorphic to $V_A$, the matrix representing $ev : V_A \rightarrow V_\Omega$ is equal to $[ x^{l-1}(\omega_m) ]$ with $(l, m)$-th entry $x^{l-1}(\omega_m) = x^{l-1} x = \omega_m$ for $1 \leq l, m \leq 8$, where $\omega_1 = 0$ and $\omega_m = \alpha^{m-2}$ with $1 < m \leq 8$ are in $\Omega$. Thus, we

9 The proof is quoted from \[8\]: the kernel of $ev$ is trivially $Z_\Psi$ and the image of $ev$ is $V_\Psi$ as, for $\phi \in \Psi$, $f_\phi(x) = \prod_{i=1}^{N} \left\{ 1 - (x_i - \phi_i)^q \right\}$ satisfies $f_\phi(\phi) = 1$ and $f_\phi(\psi) = 0$ for all $\psi \neq \phi$.
can determine \((c_\omega)_\Omega = ev ((h_\alpha)_A)\) by
\[
(c_\omega)_\Omega = (h_\alpha)_A = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\
0 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\
0 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \\
0 & \alpha^4 & \alpha^1 & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\
0 & \alpha^5 & \alpha^3 & \alpha^1 & \alpha^6 & \alpha^4 & \alpha^2 \\
0 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}.
\]

According to Proposition \[\text{Proposition 4}\] this matrix is equal to the transpose of the matrix that appeared in Remark \[\text{Remark 1}\]; actually, this can be directly checked. \(\square\)

B. Extension map \(E : V_D \to V_A\)

Let \(G_\Psi\) be a Gröbner basis with respect to \(\preceq\) for the ideal \(Z_\Psi\). We assume that \(G_\Psi\) consists of \(z\) elements \(\{g^{(w)}\}_0 \leq w < z\). According to Gröbner basis theory \[\text{[6]}\], we say that the Gröbner basis \(G_\Psi\) is reduced if and only if, for all distinct \(g_1, g_2 \in G_\Psi\), no monomial appearing in \(g_1\) is a multiple of \(LM(g_2)\), and the coefficient of the leading monomial in \(g \in G_\Psi\) is equal to one. Then, \(G_\Psi = \{g^{(w)}\}_0 \leq w < z\) becomes of the form
\[
g^{(w)} = g^{(w)}(x) = x^{a_w} + \sum_{d \in D(\Psi)} g_d^{(w)} x^d \in Z_\Psi \text{ with } a_w \in A \setminus D(\Psi).
\]

It is shown \[\text{[6]}\] that the reduced Gröbner basis can be computed from any Gröbner basis, and there exists a unique reduced Gröbner basis for each \(Z_\Psi\) with respect to a fixed monomial order \(\preceq\). However, we first do not assume that the Gröbner basis is reduced, and we deal with an arbitrary Gröbner basis for a while.

\textit{Definition 3: (Map from Gröbner bases)} A linear map \(E\) is defined by
\[
E : V_D \to V_A \quad \left[ (h_d)_D \mapsto (h_d)_A \right],
\]
where, for each \(\underline{a} \in A\), \(h_{\underline{a}}\) is determined by
\[
h_{\underline{a}} = \sum_{d \in D(\Psi)} v_{\underline{a}} h_d,
\]
if the division algorithm by \(G_\Psi\) produces the equality
\[
h_{\underline{a}} = \sum_{0 \leq w < z} u^{(w)}(\underline{x}) g^{(w)}(\underline{x}) + v(\underline{x})
\]
for some \(u^{(w)}(\underline{x}) \in \mathbb{F}_q[\underline{x}]\) for all \(0 \leq w < z\) and for some \(v(\underline{x}) \in \mathbb{F}_q[\underline{x}]\) with \(v(\underline{x}) = \sum_{d \in D(\Psi)} v_d \underline{x}^d\) \(\text{[10]}\). \(\square\)

\(\text{[10]}\) For an arbitrary \(\underline{a} \in A\), such \(u^{(w)}(\underline{x})\) and \(v(\underline{x})\) can be always computed through the division algorithm by \(G_\Psi\). Moreover, such \(v(\underline{x})\) is uniquely determined for each \(\underline{a} \in A\). For these facts from Gröbner basis theory, see, e.g., \[\text{[6]}\].
It follows from this definition that, for all \( a = b \in D \), each \( h_a \) of \( (h_a)_A = \mathcal{E} ((h_d)_D) \) is equal to \( h_d \) of \( (h_d)_D \), because \( v(x) = x^d \). This gives the consistency of notation \( (h_a)_A = \mathcal{E} ((h_d)_D) \) and implies the injectivity of \( \mathcal{E} \).

The map \( \mathcal{E} \) of Definition 3 enables us to extend syndrome values to DFT, for example, in the decoding of Reed–Solomon (RS) codes as stated below. If we represent a codeword of a RS code as \( c(x) \) and an error polynomial as \( e(x) \) as 7.2 of [3], we obtain syndrome values \( r(\alpha^i) = e(\alpha^i) \) by substituting the roots \( \alpha^i \) of the generator polynomial for \( r(x) = c(x) + e(x) \). Then, the syndrome values are equal to a part of DFT \( (e(\alpha^0), e(\alpha^1), \ldots, e(\alpha^{n-1})) \). The following Proposition 5 and diagram (23) indicate that the whole of DFT is obtained by \( \mathcal{E} \) for syndrome values, where more specific description is given at Algorithm 2 in V-C.

**Proposition 5:** (Prolongation via \( \mathcal{E} \) for the linear sum of monomial values) Let \( (h_a)_D \) = \( \left( \sum_{\omega \in \Psi} \omega \cdot \left[ c_\omega \right]_D \right)_D \in V_D \) for some \( \left( c_\omega \right)_\Psi \in V_\Psi \) according to the isomorphism \( \mathcal{P} : V_\Psi \rightarrow V_D \) of (17). Moreover, let \( (h_a)_A = \mathcal{E} ((h_d)_D) \in V_A \). Then, it follows that \( (h_a)_A = \left( \sum_{\omega \in \Psi} \omega \cdot \left[ c_\omega \right]_D \right)_A \). □

The proof of this proposition is described in Appendix C.

We denote by \( \mathcal{I} \) the inclusion map

\[
\mathcal{I} : V_\Psi \rightarrow V_\Omega \quad \left[ \left( c_\omega \right)_\Psi \mapsto \left( c_\omega \right)_\Omega \right],
\]

where \( c_\omega = c_\psi \) if \( \omega = \psi \in \Psi \) and \( c_\omega = 0 \) if \( \omega \not\in \Psi \). Then, Proposition 5 asserts that the following commutative diagram, i.e., \( \mathcal{E} \circ \mathcal{P} = \mathcal{F} \circ \mathcal{I} \), exists.

![Commutative Diagram](23)

Furthermore, if we also assume that the Gröbner basis \( G_\Psi \) is reduced, then we obtain an alternative description of the extension map \( \mathcal{E} : V_D \rightarrow V_A \). From now on, \( A = \{0, 1, \ldots, q - 1\}^N \) is considered as a semigroup by the component-wise addition \( a + b \) for \( a = (a_1, \ldots, a_N), b = (b_1, \ldots, b_N) \in A \), where the component \( a_i + b_i \) is viewed within \( 1 \leq (a_i + b_i \mod (q - 1)) < q \) if \( a_i + b_i \neq 0 \) for \( 1 \leq i \leq N \). For example, \((0, 0, 1, 2) + (0, 3, 1, 2) = (0, 3, 2, 1) \) in \( A \) if \( N = 4 \) and \( q = 4 \). This semigroup structure of \( A \) comes naturally from the multiplication of monomials in \( \mathbb{F}_q[x]/\mathbb{Z}_\Omega \), which is isomorphic to \( V_A \) as a vector space because \( D(\Omega) = A \). Moreover, for \( a, b \in A \), we denote \( a \geq b \) if \( a_i \geq b_i \) component-wise for all \( 1 \leq i \leq N \), or equivalently, if there is \( \epsilon \in A \) such that \( a = b + \epsilon \).

**Proposition 6:** (M-D linear feedback shift registers from Gröbner bases) Suppose that the Gröbner basis \( G_\Psi = \{ g^{(w)} \}_{0 \leq w < z} \) is reduced and of the form (18). If \( (h_a)_A = \mathcal{E} ((h_d)_D) \) for some \( (h_d)_D \in V_D \) with \( D = D(\Psi) \), then we have, for all \( a \in A \) and all \( 0 \leq w < z \),

\[
h_a = \begin{cases} 
  h_d & a = d \in D \\
  - \sum_{d \in D} g^{(w)}_d h_{a+d-\omega} & a \geq a_{\omega} 
\end{cases}
\]

Conversely, if \( (h_a)_A \in V_A \) satisfies that, for each \( a \in A \setminus D(\Psi) \), there exists at least one \( 0 \leq w < z \) such that (24), then we have \( (h_a)_A = \mathcal{E} ((h_d)_D) \) for \( (h_d)_D \in V_D \) with \( D = D(\Psi) \) and (24). □
The proof is described in Appendix [13] To actually compute the value of $E((h_d)_D) = (h_w)_A$ from a given $(h_d)_D$, we can generate $(h_w)_A$ inductively by (24), because, for each $a \in A \setminus D(\Psi)$, at least one $0 \leq w < z$ can be chosen such that $a \geq a_w$. Moreover, the induction to generate $(h_w)_A$ works because the monomial order is a total order [6] and we have $a \geq a + d - a_w$ and $a \neq a + d - a_w$ in case of $a \geq a_w$ in the right-hand side of (24). Then, the latter half of Proposition 6. asserts that the resulting value does not depend on the choice and order of the generation, and that $E((h_d)_D) = (h_w)_A$ is uniquely determined. In the rest of the paper, for simplicity, we adopt (24) to compute the value of $E((h_d)_D) = (h_w)_A$ in place of (23) and (21).

C. Isomorphic map $C : V_D \rightarrow V_\Psi$

From now on, we denote $R$ as the restriction map

$$R : V_\Omega \rightarrow V_\Psi \quad \left[ (c_{\omega})_\Omega \mapsto (c_{\omega})_\Psi \right].$$

(25)

It follows from (24) that $F^{-1} \circ E \circ P = I$. Moreover, $R \circ F^{-1} \circ E \circ P = R \circ I$ is the identity map on $V_\Psi$. This leads to the following lemma, which is frequently used in this paper.

**Main Lemma**: Let $G_\Psi$ be a Gröbner basis of $Z_\Psi$ for $\Psi \subseteq \Omega$, and let $E : V_D \rightarrow V_A$ be the extension map defined by (19). Then, the composition map $C = R \circ F^{-1} \circ E : V_D \rightarrow V_\Psi$ in the following commutative diagram gives an isomorphism between $V_D$ and $V_\Psi$.

Moreover, we have that

$$\left( c_{\omega} \right)_\Omega \in F^{-1} (E(V_D)) \quad \Rightarrow \quad c_{\omega} = 0 \quad \text{for all} \quad \omega \in \Omega \setminus \Psi.$$

(26)

**Remark 5**: As $C = P^{-1}$, our $C$ can also be obtained from the multiplication of the inverse matrix representing [17]. However, if $\Psi$ is changed, then the inverse matrix must be computed each time. As $\Psi$ takes, e.g., the set of erasure-and-error locations and $C$ has a lower computational complexity order than Gaussian elimination, there are many cases where $C$ outperforms computing the inverse matrix, as shown in Section [VI].

**Remark 6**: The above proof of our Main Lemma can also be applied to the non-zero indexed case [22], [26] where $A = \{0, 1, \cdots, q - 2\}_N$ has a cyclic structure mod $(q - 1)$ and $\Omega = (\mathbb{F}_q^\times)^N$. [\Box]

**Example 4**: Putting $N = 1$, $q = 8$, and $\alpha \in \mathbb{F}_8$ with $\alpha^3 + \alpha + 1 = 0$, consider the natural order $\preceq$ to be a monomial order, i.e., $0 \preceq 1 \preceq 2 \preceq \cdots \preceq 7$ on $A = \{0, 1, \cdots, 7\}$. Choose $\Psi \subseteq \Omega = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^6\}$ as $\Psi = \{0, \alpha, \alpha^3, \alpha^6\}$. Then, $D = D(\Psi) = \{0, 1, 2, 3\}$ and $G_\Psi = \{g(x)\}$, where

$$g(x) = \prod_{\psi \in \Psi} (x - \psi) = \alpha^3 x + \alpha^3 x^2 + \alpha^2 x^3 + x^4.$$
For \((h_d)_D = (h_0, h_1, h_2, h_3) = (\alpha^2, \alpha^3, \alpha^5, \alpha^0)\), \(E((h_d)_D) = (h_a)_A = (h_0, h_1, \ldots, h_7)\) is given by

\[
(h_0, h_1, \ldots, h_7) = (\alpha^2, \alpha^3, \alpha^5, \alpha^0, \alpha^4, \alpha^3, \alpha^2),
\]

where, e.g., \(h_4 = \alpha^3\alpha^3 + \alpha^3\alpha^5 + \alpha^2\alpha^0 = \alpha^3\), and \(F^{-1}(E((h_d)_D)) = (c_\omega)_\Omega\) is given by

\[
(c_0, c_1, c_\alpha, \ldots, c_{\alpha^6}) = (\alpha^5, 0, \alpha^2, 0, 1, 0, 0, \alpha^4).
\]

Note that \(c_\omega = 0\) if \(\omega \not\in \Psi\). Then, \(C((h_d)_D) = (c_\psi)_\Psi = (c_0, c_\alpha, c_\alpha^3, c_\alpha^6) = (\alpha^5, \alpha^2, 1, \alpha^4)\).

**Example 5:** Putting \(N = 2, q = 8\), and \(\alpha \in \mathbb{F}_8\) with \(\alpha^3 + \alpha + 1 = 0\), consider the lexicographic order \(\preceq\) to be a monomial order, i.e., \((0, 0) \preceq (1, 0) \preceq (2, 0) \preceq \cdots \preceq (7, 0) \preceq (0, 1) \preceq (1, 1) \preceq \cdots \preceq (7, 7)\) on \(A = \{0, 1, \ldots, 7\}^2\).

Choose \(\Psi \subseteq \Omega = \mathbb{F}_8^2\) as

\[
\Psi = \left\{ (0, 0), (0, \alpha^6), (\alpha^0, \alpha^0), (\alpha^0, \alpha^5), (\alpha^1, \alpha^1), (\alpha^1, \alpha^4), (\alpha^2, \alpha^2), (\alpha^2, \alpha^3), (\alpha^3, \alpha^2), (\alpha^3, \alpha^3), (\alpha^4, \alpha^1), (\alpha^4, \alpha^4), (\alpha^5, \alpha^0), (\alpha^5, \alpha^5), (\alpha^6, 0), (\alpha^6, \alpha^6) \right\},
\]

which, in order to show a pictorial example, is the cross pattern \((c_\omega)_\Omega\) in Fig. 2. We denote \(x = x_1\) and \(y = x_2\) in \(\mathbb{F}_8[x] = \mathbb{F}_8[x_1, x_2]\). An element \(g(x, y) \in \mathcal{G}_\Psi\) of the Gröbner basis can then be characterized as \(g(x, y) \in \mathbb{F}_8[x, y]\) with \(g(\omega_1, \omega_2) = 0\) for all \((\omega_1, \omega_2) \in \Psi\) that has the minimum \(\text{LM}(g)\) with respect to \(\preceq\). One of \(\mathcal{G}_\Psi\) is computed.
as
\[ g(x, y) = \alpha^6 x + \alpha^5 x^2 + \alpha^4 x^3 + \alpha^2 x^4 + \alpha x^5 + \alpha^4 x^6 + y (\alpha^6 + \alpha^5 x^2 + \alpha^4 x^3 + \alpha^3 x^4 + \alpha^4 x^5) + y^2. \]

The other elements of \( \mathcal{G}_\Psi \) are not necessary to extend \((h_d)_D\) because of the semigroup structure of \( A \). For a given \((h_d)_D\), all values of Main Lemma are shown in Fig. 2. For example, \( h_{(2, 2)} \) is generated as
\[ h_{(2, 2)} = - \sum_{d \in D(\Psi)} g_d h_{(2, 2) + d - (0, 2)}, \]
where it should be noted that \( h_{(2, 2) + (6, 0) - (0, 2)} = h_{(1, 0)}. \) Thus, we have
\[ h_{(2, 2)} = \alpha^6 \alpha^1 + \alpha^0 \alpha^4 + \alpha^1 \alpha^0 + \alpha^2 0 + \alpha^3 \alpha^2 + \alpha^4 \alpha^5 + (\alpha^6 \alpha^3 + \alpha^1 \alpha^5 + \alpha^2 \alpha^6 + \alpha^3 \alpha^3 + \alpha^4 \alpha^1) = \alpha^1. \]
The data of \( \mathcal{F}^{-1}(h_{(2, 2)}) = (c_{(2, 2)}) \) has already been treated in Example 3 and Fig. 1.

V. APPLICATIONS OF MAIN LEMMA

A. Affine variety codes

Let \( \Psi \subseteq \Omega \) with \( \Psi \neq \emptyset \) and \( n = |\Psi| \), as at the beginning of Subsection IV-A. Let \( U \) be a subspace of \( V_D(\Psi) \). Consider an affine variety code with code length \( n \)
\[ C(U, \Psi) = \text{ev}(U) \]
\[ = \left\{ (c_{(\cdot, \Psi)})_{\Psi} \in V_\Psi \left| \left( \sum_{d \in D} h_d \psi_d^{\Psi} \right)_{\Psi} = (c_{(\cdot)})_{\Psi} \right| \text{for some } (h_d)_D \in U \right\}, \]
where \( \psi_1^d \cdots \psi_N^d \) is as in [3]. Moreover, consider a dual affine variety code with code length \( n \)
\[ C^\perp(U, \Psi) = \text{ev}(U)^\perp \]
\[ = \left\{ (c_{(\cdot, \Psi)})_{\Psi} \in V_\Psi \left| \sum_{\psi \in \Psi} c_{\psi} \sum_{d \in D} h_d \psi_d^{\Psi} = 0 \right| \text{for all } (h_d)_D \in U \right\}, \]
where \( \sum_{\psi \in \Psi} c_{\psi} \sum_{d \in D} h_d \psi_d^{\Psi} \) in [29] is equal to the inner product of \( (c_{\psi})_{\Psi} \) and \( \text{ev} \left( (h_d)_D \right) = \left( \sum_{d \in D} h_d \psi_d^{\Psi} \right) \) in \( V_\Psi \). Thus, the dimension or number of information symbols \( k \) of \( C^\perp(U, \Psi) \) is equal to \( n - \dim_{F_q} U \); in other words, \( n - k = \dim_{F_q} U \). Note that, as vector spaces, these code definitions do not depend on the choice of monomial order; \( U \subseteq V_D(\Psi) \) is equivalent to \( U \subseteq F_q[x]/Z_\Psi \).

On the other hand, let \( U^\perp \) be the orthogonal complement of \( U \) in \( V_D \), i.e.,
\[ U^\perp = \left\{ (h_d)_D \in V_D \left| \sum_{d \in D} h_d h_d' = 0 \text{ for all } (h_d')_D \in U \right\}. \]
Thus, similarly to (28), we obtain
\[ C^\perp(U, \Psi) = C(U^\perp), \] (30)
a proof of which is given in Appendix E. Whereas the definition (29) of \( C^\perp(U, \Psi) \) is indirect and not constructive, the equality (30) provides a direct construction. Moreover, the equality (30) corresponds to the non-systematic encoding of \( C^\perp(U, \Psi) \). Actually, non-systematic encoding is obtained, for all \((h_d)_D \in U^\perp, \) by \( (c_v)_\Psi = C((h_d)_D) \in C^\perp(U, \Psi) \) as (30).

**Example 6:** (Continued from Example 4) Let \( U \subseteq V_D \) be a vector space generated by \((1, 0, \alpha^4, \alpha^5)\) and \((0, 1, 0, \alpha^6)\). If these are represented as polynomials \( f(x) = 1 + \alpha^4x^2 + \alpha^5x^3 \) and \( x + \alpha^6x^3 \), then \( ev(U) \subseteq V_\Psi \) is generated by
\[
(f(0), f(\alpha), f(\alpha^3), f(\alpha^6)) = (1, \alpha^4, \alpha^3, 1) \text{ and } (0, \alpha^3, 1, \alpha^4).
\]
Then, \( U^\perp \subseteq V_D \) is equal to a vector space generated by
\[
(h_0, h_1, h_2, h_3) = (\alpha^4, 0, 1, 0) \text{ and } (\alpha^5, \alpha^6, 0, 1).
\]
These extensions are equal to
\[
(h_4, h_5, h_6, h_7) = (\alpha^3, \alpha^2, \alpha^3, \alpha^6) \text{ and } (0, \alpha^3, \alpha^2, \alpha^3).
\]
Thus, \( C(U^\perp) \) is generated by
\[
(c_0, c_\alpha, c_{\alpha^3}, c_{\alpha^6}) = (\alpha^3, \alpha^5, \alpha^5, \alpha^6) \text{ and } (\alpha^2, \alpha^4, \alpha^2, 1).
\]
The orthogonality is valid, e.g., \( \alpha^3 + \alpha^2 + \alpha + \alpha^6 = 0. \)

**Remark 7:** A typical case of \( U \) is \( U = V_B \) for some \( B \subseteq D(\Psi) \). Then, \( U^\perp = V_{D \setminus B} \), where \( V_B \) and \( V_{D \setminus B} \) are considered subspaces of \( V_D \), as in Section II.

**Example 7:** Throughout the rest of Section III, we consider a Hermitian code, i.e., a code on the \( \mathbb{F}_9 \)-rational points of a Hermitian curve, in order to compare our method with conventional methods for algebraic geometry codes.

Putting \( N = 2, q = 9, \) and \( \alpha \in \mathbb{F}_9 \) with \( \alpha^2 + \alpha - 1 = 0 \), consider the weighted graded lexicographic order [6] to be a monomial order \( \preceq \) such that \( (a_1, a_2) \preceq (a_1', a_2') \Leftrightarrow 3a_1 + 4a_2 < 3a_1' + 4a_2' \) or \( 3a_1 + 4a_2 = 3a_1' + 4a_2' \), \( a_2 \leq a_2' \), i.e., \((0, 0) \preceq (1, 0) \preceq (0, 1) \preceq (2, 0) \preceq (1, 1) \preceq (0, 2) \preceq \cdots \preceq (1, 2) \preceq (4, 0) \preceq (0, 3) \preceq (3, 1) \preceq \cdots \preceq (8, 8) \) on \( A = \{0, 1, \cdots , 8\}^2 \). Choose \( \Psi \subseteq \Omega = \mathbb{F}_9^2 \) as
\[
\Psi = \{ (0, 0), (0, \alpha^2), (0, \alpha^6), (\alpha^0, \alpha^4), (\alpha^0, \alpha^5), (\alpha^0, \alpha^7), (\alpha^1, \alpha^0), (\alpha^1, \alpha^1), (\alpha^1, \alpha^3), (\alpha^2, \alpha^4), (\alpha^2, \alpha^5), (\alpha^2, \alpha^7), (\alpha^3, \alpha^0), (\alpha^3, \alpha^1), (\alpha^3, \alpha^3), (\alpha^4, \alpha^4), (\alpha^4, \alpha^5), (\alpha^4, \alpha^7), (\alpha^5, \alpha^0), (\alpha^5, \alpha^1), (\alpha^5, \alpha^3), (\alpha^6, \alpha^4), (\alpha^6, \alpha^5), (\alpha^6, \alpha^7), (\alpha^7, \alpha^0), (\alpha^7, \alpha^1), (\alpha^7, \alpha^3), \},
\] (31)
which agrees with \( \{ (\omega_1, \omega_2) \mid \omega_1^4 = \omega_2^3 + \omega_2 \} \), a set of \( \mathbb{F}_9 \)-rational points of a Hermitian curve with defining equation \( x^4 = y^3 + y \), where we denote \( x = x_1 \) and \( y = x_2 \). In this case, one of the elements in the Gröbner basis \( G_\Psi \) is equal to \( g(x, y) = y^3 - x^4 + y \) and the delta set \( D(\Psi) \) of \( G_\Psi \) is \( \{ (a_1, a_2) \mid a_1, a_2 \leq 2 \} \). The other elements of \( G_\Psi \) are not necessary to extend \( (h_\omega)_D \) because of the semigroup structure of \( A \). Let \( B \subseteq D(\Psi) \) be \( B = \{ (b_1, b_2) \mid (b_1 + b_2) \leq 11 \} \) and let \( U = V_B \). Then, \( C^\perp(U, \Psi) = C(V_D(\Psi) \setminus B) \) agrees with \( C_{Q_1}(D, mP_\infty) = C_{L_1}(D, mP_\infty)^\perp \) in the usual notation \[ \text{Eq.} \] for \( m = 11 \) and \( D = \sum_{(\omega_1, \omega_2) \in \Psi} P_{\omega_1, \omega_2} \) with \( P_{\omega_1, \omega_2} = (\omega_1, \omega_2) \). For a given \( (h_\omega)_D \), all values of Main Lemma are shown in Fig. 3, where the vertical axis and the horizontal axis \((0, 1, \cdots, 8)\) in \( (h_\omega)_A \) indicate \( a_1 \) and \( a_2 \) of \( \alpha = (a_1, a_2) \in A \), and those axes \((-1, 0, \cdots, 7)\) in \( (c_\omega)_\Omega \) indicate \( \omega_1 \) and \( \omega_2 \) of \( \omega = (\omega_1, \omega_2) \in \Omega \).

**Example 8:** Throughout the rest of Section \[ Eq. \] we consider an extended hyperbolic cascaded Reed–Solomon (HCRS) code, which is an example of affine variety codes that are not algebraic geometry codes. Putting \( N = 2 \), \( q = 9 \), and \( \alpha \in \mathbb{F}_q \) with \( \alpha^2 + \alpha - 1 = 0 \), choose \( \Psi = \Omega = \mathbb{F}_9^2 \) and \( A = \{ 0, 1, \cdots, 8 \} \); then, \( D = D(\Psi) = A \). Let \( B \subseteq D(\Psi) \) be \( B = \{ (b_1, b_2) \mid (b_1 + 1)(b_2 + 1) < 9 \} \), and let \( U = V_B \). Then, \( C^\perp(U, \Omega) = C(V_A \setminus B) \) is an extended HCRS code \[ Eq. \]. For a given \( (h_\omega)_D \), all values of Main Lemma are shown in Fig. 4.

In Subsection \[ Eq. \] it is shown that Main Lemma also gives the systematic encoding of a class of dual affine variety codes.
B. Erasure-and-error decoding: non-systematic case

Henceforth, consider the situation $U = V_B$ with some $B \subseteq D(\Psi)$ from Remark 7. In this subsection, suppose that $(h_d)_D \in V_D \setminus R$ is encoded into $(c_\psi)_\Psi = C((h_d)_D) \in C^\perp(V_B, \Psi)$, and consider the decoding problem for this non-systematic encoding.

Suppose also that erasure-and-error $(\tilde{e}_\psi)_\Psi \in V_\Psi$ has occurred in a received word $(\tilde{r}_d)_D = (c_\psi)_\Psi + (\tilde{e}_\psi)_\Psi \in V_\Psi$ from some channel. Let $\Phi_1 \subseteq \Psi$ be the set of erasure locations and $\Phi_2 \subseteq \Psi$ be the set of error locations with $\Phi_1 \cap \Phi_2 = \emptyset$; we suppose that $\Phi_1$ is known, but $\Phi_2$ and $(\tilde{e}_\psi)_\Psi$ are unknown, that $\tilde{e}_\psi \neq 0 \Rightarrow \psi \in \Phi_1 \cup \Phi_2$, and that $\psi \in \Phi_2 \Rightarrow e_\psi \neq 0$. We might permit $e_\psi = 0$ for some $\psi \in \Phi_1$. If $|\Phi_1| + 2|\Phi_2| < d_{FR}$ is valid, where $d_{FR}$ denotes the Feng–Rao minimum distance bound [1],[7],[27],[37], then it is known that the erasure-and-error version [17],[36] of the BMS algorithm [4],[7] or the multidimensional Berlekamp–Massey algorithm calculates the Gröbner basis $G_{\Phi_1 \cup \Phi_2}$. The main difference between the erasure-and-error and ordinary error-only algorithms is in the initialization; as $\Phi_1$ is known, $G_{\Phi_1}$ can be calculated in advance by the ordinary error-only version, and then $G_{\Phi_1 \cup \Phi_2}$ can be calculated by the erasure-and-error version from the syndrome and the initial value $G_{\Phi_1}$. Using the recurrence from $G_{\Phi_1 \cup \Phi_2}$ and Main Lemma, the erasure-and-error decoding algorithm is realized as follows.  

Algorithm 1: (Decoding of non-systematic codewords)

11 In the following algorithms, we use the auxiliary vector notation $(v_b)_B \in V_B$, $(\tilde{r}_d)_D \in V_D$, and $(k_d)_D \in V_D$. 
In Step 3, correction can be performed by Algorithm 1 if \( D(\Psi) \subseteq \Psi \). The input of Algorithm 1 consists of the received word \( \tilde{r}_B \). In Step 2, the Gröbner basis \( G_{\Phi_1} \) from syndrome \( \tilde{r}_B \). In Step 3, \( (\tilde{r}_d)_D = \left( \sum_{\psi \in \Psi} r_{\psi \tilde{d}} \right)_D \) \( \in \mathbb{D} \). In Step 4, calculate \( G_{\Phi_1 \cup \Phi_2} \) from \( (\tilde{r}_d)_B \) and \( G_{\Phi_1} \). In Step 5, \( (k_d)_D = E((\tilde{r}_d)_B) \in \mathbb{D} \) by \( G_{\Phi_1 \cup \Phi_2} \). In Step 6, \( (h_d)_D = (\tilde{r}_d)_D - (k_d)_D \in \mathbb{D} \).

At Step 5, \( (k_d)_D = E((\tilde{r}_d)_B) \) means that \( (k_d)_D(\Psi) = E((\tilde{r}_d)_D(\Phi_1 \cup \Phi_2)) \), where the values of \( E \) are only computed on \( D(\Psi) \subseteq \mathbb{A} \) by the recurrence relation (24).

The validity of this algorithm is proved by the following argument. It follows from Main Lemma that \( C((h_d)_D) = \left( c_{\tilde{r}_d} \right)_\Psi \iff (h_d)_D = C^{-1}(c_{\tilde{r}_d})_\Psi = \left( \sum_{\psi \in \Psi} c_{\psi \tilde{r}_d} \right)_D \). As \( (r_{\psi})_\Psi = (c_{\psi})_\Psi + (e_{\psi})_\Psi \), we have \( (\tilde{r}_d)_D = (h_d)_D + \left( \sum_{\psi \in \Psi} e_{\psi \tilde{r}_d} \right)_D \) by (29). It follows from the proof of Proposition 5 that \( E((\tilde{r}_d)_B) = \left( \sum_{\psi \in \Psi} e_{\psi \tilde{r}_d} \right)_D \) in Step 5, because \( U = V_B \) is assumed. Thus, we obtain \( (h_d)_D = (\tilde{r}_d)_D - (k_d)_D \) in Step 6.

**Example 9:** (Continued from Example 7) As it can be shown that \( d_{FR} = 7 \) for \( C^1(V_B, \Psi) \), the erasure-and-error correction can be performed by Algorithm 1 if \( |\Phi_1| + 2|\Phi_2| < 7 \). Erasure-and-error decoding of the non-systematic Hermitian codeword in Fig. 5 via Algorithm 1 is described as follows. The input of Algorithm 1 consists of the received word \( \tilde{r}_B \) in Fig. 5 and a set \( \Phi_1 \) of erasure locations \( \{(\alpha^6, \alpha^4), (\alpha^6, \alpha^7)\} \). Fig. 5 shows the values of vectors at each step in Algorithm 1. In Step 2, the Gröbner basis \( G_{\Phi_1} \) of \( Z_{\Phi_1} \) is obtained as \( G_{\Phi_1} = \{ g(0) = \alpha^2 + x, g(1) = \alpha^2 y + xy, g(2) = \alpha^3 + \alpha^5 y + y^2 \} \).

In Step 3, \( (\tilde{r}_d)_D = \left( \sum_{\psi \in \Psi} r_{\psi \tilde{d}} \right)_D \) is computed, e.g., \( (\tilde{r}_{(0,0)}) = \sum_{\psi \in \Psi} r_{\psi} = \alpha^2 \) according to the case \( N = 2 \) and
\[ a = b = 0 \text{ in Example 1. In Step 4, the Gröbner basis } \mathcal{G}_{\Phi_1 \cup \Phi_2} \text{ of } Z_{\Phi_1 \cup \Phi_2} \text{ is obtained as} \]

\[
\mathcal{G}_{\Phi_1 \cup \Phi_2} = \begin{cases} 
  g^{(0)} = \alpha x + \alpha^4 x^2 + x^3, \\
  g^{(1)} = 1 + \alpha^7 x + \alpha^2 y + \alpha^2 x^2 + xy, \\
  g^{(2)} = \alpha^5 + \alpha^7 x + \alpha^5 y + \alpha^2 x^2 + y^2
\end{cases}
\]

If we perform Chien search for \( \mathcal{G}_{\Phi_1 \cup \Phi_2} \), the set \( \Phi_1 \cup \Phi_2 \) of the erasure-and-error locations can be determined; however, the explicit set \( \Phi_1 \cup \Phi_2 \) may not be used in our algorithm. It can be seen in Fig. 5 that the erasure-and-error spectrum \( (k_d)_D \) is generated by \( \mathcal{G}_{\Phi_1 \cup \Phi_2} \) from \( \tilde{(r_d)}_D \) in Step 5, and \( (k_d)_D \) is then removed from \( \tilde{(r_d)}_D \) in Step 6. The resulting \( (h_d)_D \) agrees with the information given in Fig. 6.

**Example 10:** (Continued from Example 8) As it can be shown [15] that \( d_{\min} = d_{FR} = 9 \) for \( C_1(V_B, \Psi) \), where \( d_{\min} \) is the true minimum distance, the erasure-and-error correction can be performed by Algorithm 1 if \( |\Phi_1| + |\Phi_2| < 9 \). Fig. 6 shows the data at each step of Algorithm 1 for the erasure-and-error decoding of the non-systematic codeword in Fig. 4. The input of Algorithm 1 consists of the received word \( \tilde{(r_\psi)}_D \) in Fig. 6 and a set \( \Phi_1 \) of erasure locations \( \{(0, \alpha^4), (\alpha^2, 0)\} \). Consider the graded lexicographic order [6] to be a monomial order \( \leq \) such that \( (a_1, a_2) \leq (a_1', a_2') \Leftrightarrow a_1 + a_2 < a_1' + a_2' \) or \( a_1 + a_2 = a_1' + a_2' \) and \( a_2 \leq a_2' \), i.e., \( (0, 0) \leq (1, 0) \leq (0, 1) \leq (2, 0) \leq (1, 1) \leq (0, 2) \leq (3, 0) \leq \cdots \leq (0, 3) \leq (4, 0) \leq (3, 1) \leq \cdots \leq (8, 8) \) on \( A = \{0, 1, \cdots, 8\} \). In Step 2, the Gröbner basis \( \mathcal{G}_{\Phi_1} \) of \( Z_{\Phi_1} \) is obtained as

\[
\mathcal{G}_{\Phi_1} = \begin{cases} 
  g^{(0)} = \alpha^6 x + x^2, \\
  g^{(1)} = \alpha^6 + \alpha^2 y + \alpha^2 x^2 + xy + x^3,
\end{cases}
\]

where we denote \( x = x_1 \) and \( y = x_2 \). In Step 4, the Gröbner basis \( \mathcal{G}_{\Phi_1 \cup \Phi_2} \) of \( Z_{\Phi_1 \cup \Phi_2} \) is obtained as

\[
\mathcal{G}_{\Phi_1 \cup \Phi_2} = \begin{cases} 
  g^{(0)} = \alpha^6 + \alpha^6 y + \alpha^2 x^2 + xy + x^3, \\
  g^{(1)} = 1 + \alpha x + \alpha^5 y + \alpha^2 x^2 + \alpha^3 xy + y^2, \\
  g^{(2)} = 1 + \alpha x + \alpha^4 y + \alpha^5 x^2 + \alpha^3 xy + y^2
\end{cases}
\]

The resulting \( (h_d)_D \) agrees with the information given in Fig. 4.
the same as those in Example 9. Although only \((\tilde{r}_d)_{\Psi}\) is required, \((\tilde{r}_d)_{A}\) is shown for consistency and for the discussion in Subsection 6.5.1. The delta set \(D \in \mathcal{E}(\tilde{r}_d)\) indicates \(D(\Phi_1 \cup \Phi_2)\) and \(\mathcal{E}\) is formed from \(\mathcal{G}_{\Phi_1 \cup \Phi_2}\).

C. Erasure-and-error decoding: general case

In Algorithm 1 we removed the erasure-and-error spectrum from the received word spectrum without identifying \((e_\Psi)_{\Psi}\). In this subsection, we consider the problem of erasure-and-error decoding with identifying \((e_\Psi)_{\Psi}\) in the received word. It follows from Main Lemma that the value of \(C\) for the erasure-and-error spectrum is equal to \((e_\Psi)_{\Psi}\). Though \(F^{-1}\) was not used in Algorithm 1 the map \(C\) including \(F^{-1}\) is required in Algorithm 2.

Algorithm 2: (Finding erasures and errors)

Input: \(\Phi_1\) and a received word \((r_\psi)_{\Psi} \in V_{\Psi}\)

Output: \((e_\Psi)_{\Psi} \in C^1(V_B, \Psi)\)

Step 1. \((v_\Psi)_{B} = \left(\sum_{\psi \in \Phi_1} \omega_\Psi^e\right)_{B} \in V_B\)

Step 2. Calculate \(\mathcal{G}_{\Phi_1}\) from syndrome \((v_\Psi)_{B}\)

Step 3. \((\tilde{r}_d)_{B} = \left(\sum_{\psi \in \Psi} r_\psi \omega_\Psi^d\right)_{B} \in V_B\)

Step 4. Calculate \(\mathcal{G}_{\Phi_1 \cup \Phi_2}\) from \((\tilde{r}_d)_{B}\) and \(\mathcal{G}_{\Phi_1}\)

Step 5. \((e_\Psi)_{\Psi} = C ((\tilde{r}_d)_{B}) \in V_{\Psi}\)

Step 6. \((e_\Psi)_{\Psi} = (r_\psi)_{\Psi} - (e_\Psi)_{\Psi} \in C^1(V_B, \Psi)\)

In this algorithm, Main Lemma is used in Step 5, because \((\tilde{r}_d)_{B} = \left(\sum_{\psi \in \Psi} e_\psi \omega_\Psi^d\right)_{B} = C^{-1} ((e_\Psi)_{\Psi})\) from definition 29, and \(C ((\tilde{r}_d)_{B}) = (e_\Psi)_{\Psi}\) by Main Lemma, which is applied as \(C : V_D \to V_{\Phi_1 \cup \Phi_2}\) with \(D = D(\Phi_1 \cup \Phi_2)\). Note that \((e_\Psi)_{\Phi_1 \cup \Phi_2} = C ((\tilde{r}_d)_{B})\) is denoted as \((e_\Psi)_{\Psi} = C ((\tilde{r}_d)_{B})\) because \(V_{\Phi_1 \cup \Phi_2} \subseteq V_{\Psi}\) and \(D(\Phi_1 \cup \Phi_2) \subseteq B\).

Example 11: (Continued from Example 9) Erasure-and-error decoding of the codeword in Fig. 6 via Algorithm 2 is described as follows. The input of Algorithm 2 is the same as for Example 9. Fig. 7 shows the values of vectors at each step of Algorithm 2. The Gröbner basis \(\mathcal{G}_{\Phi_1}\) in Step 2 and the Gröbner basis \(\mathcal{G}_{\Phi_1 \cup \Phi_2}\) in Step 4 are the same as those in Example 9. Although \(C\) is used in Step 5 of Algorithm 2 the value of \(\mathcal{E}(\tilde{r}_d)\) is given in Fig. 7 in order to show the process.
for all $\phi \in \Phi$ of the codewords in Algorithm 2 are shown in Fig. 8. The Gröbner basis $G_{\Phi_1}$ in Step 2 and the Gröbner basis $G_{\Phi_1 \cup \Phi_2}$ in Step 4 are the same as those in Example 10.

**Example 12:** (Continued from Example 10) Erasure-and-error decoding of the codeword in Fig. 4 via Algorithm 2. As noted in Example 11, $E\left(\hat{r}_\Phi^t D\right)$ is the computational process of $C = F^{-1} o E$ in Step 5 of Algorithm 2. A received word $\left(r_\varphi\right)_\psi$ is decomposed into $\left(e_\varphi\right)_\psi$ and $\left(c_\varphi\right)_\psi$.

**Remark 8:** One might consider that, as the Gröbner basis $G_{\Phi_1 \cup \Phi_2}$ is obtained in Step 4 of Algorithms 1 and 2, and the set $\Phi_1 \cup \Phi_2$ of erasure-and-error locations can be calculated by Chien search, the erasure-and-error values $\left(e_\varphi\right)_{\Phi_1 \cup \Phi_2}$ can be computed from the system of linear equations $\left(\sum_{\psi \in \Phi_1 \cup \Phi_2} e_{\psi} \varphi x^{d_{\psi}}\right)_{D} = (\hat{r}_\varphi)_D$ with $D = D(\Phi_1 \cup \Phi_2)$, the matrix of which is invertible by (15) and Appendix B. If we use Gaussian elimination to solve this, then the computational complexity is of the order $(|\Phi_1| + |\Phi_2|)^3$, which is bounded by $n^3$. We will see in the next section that the computational complexity of Step 5 in Algorithm 1 or 2 for finding the erasure-and-error values or spectrum is bounded by the order $qn^{2+\varepsilon}$ with any $0 < \varepsilon < 1$. Consequently, we can choose an appropriate method according to $|\Phi_1| + |\Phi_2|$ and $n$.

**D. Systematic encoding regarded as erasure-only decoding**

Because, in practical use, error-correcting codes are usually encoded systematically, it is natural to consider the systematic encoding of $C\perp(V_B, \Psi)$. In this subsection, we show that the systematic encoding is equivalent to a certain type of erasure-only decoding under Algorithm 2.

Systematic encoding means that there exists at least one $\Phi$ with $\Phi \subseteq \Psi$ and $|\Phi| = |B|$ such that, for any given information $\left(h_\varphi\right)_{\Psi \setminus \Phi} \in V_{\Psi \setminus \Phi}$, we find $\left(c_\varphi\right)_{\Psi} \in C\perp(V_B, \Psi)$ with $c_{\varphi} = h_{\varphi}$ for all $\psi \in \Psi \setminus \Phi$. Thus, $\Phi$ corresponds to the set of redundant locations, and $\Psi \setminus \Phi$ corresponds to the set of information locations, in the codewords of $C\perp(V_B, \Psi)$. If $\Phi$ is fixed, then systematic encoding can be viewed as the erasure-only decoding of $\left(e_\varphi\right)_{\Phi} = \left(-c_\varphi\right)_{\Phi}$. However, as $|\Phi_1| = n - k = |\Phi|$ and $|\Phi_2| = 0$, the correctable erasure-and-error bound $|\Phi_1| + 2|\Phi_2| < d_{FR}$ is not generally valid.

**Example 13:** (Continued from Examples 9 and 10) In Examples 7 and 9 because $|B| = n - k = 9$ and $d_{FR} = 7$ for the Hermitian code, the correctable erasure-only bound $|B| = |\Phi_1| < d_{FR}$ is not valid. Similarly, in Examples...
follows from the surjectivity of (32) that, for any word \( v = (e_\phi) \_\psi \) from some channel, where \( (e_\phi) \_\psi \) is unknown, but \( \Phi \subseteq \Psi \) is known and \( e_\phi \neq 0 \Rightarrow \psi \in \Phi \). If the linear map \( \text{ev}|_{V_B,\Phi} \) given by

\[
\text{ev}|_{V_B,\Phi}: V_B \rightarrow V_\Phi
\]

is isomorphic, then the received word \( (r_\phi) \_\psi \) can be decoded by Algorithm 2. \( \Box \)

Note that this condition is equivalent to \( \det \left[ x_n (\varphi_m) \right] \neq 0 \), where \( \{ x_n^l | l \in B \} = \{ x_n^l | 1 \leq l \leq |B| \} \) and \( \Phi = \{ \varphi_n | 1 \leq m \leq |\Phi| \} \) are aligned in any order, and \( x_n (\varphi_m) \) is the \((l, m)\)-th entry. This matrix is considered in Appendix B. A non-zero determinant value \( \det \left[ x_n (\varphi_m) \right] \neq 0 \) is expected to occur with high probability \((q-1)/q\), because the values of \( \det \left[ x_n (\varphi_m) \right] \) are considered to occur equally in \( \mathbb{F}_q \) if we vary \( \Psi \subseteq \Phi \) and \( B \subseteq D(\Phi) \) randomly. At least when \( B = D(\Phi) \), this expectation is supported experimentally for Hermitian codes by [29], where \( \Phi \) with \( \det \left[ x_n (\varphi_m) \right] \neq 0 \) is said to be generic, and [16], where such a \( \Phi \) is said to be independent. Moreover, this expectation is supported theoretically for \( \mathbb{F}_q \)-rational points of algebraic curves by [13].

The validity of this Corollary can be described directly as follows. Let \( \Phi \subseteq \Psi \subseteq \Omega \), so that (32) is isomorphic. It follows from the surjectivity of (32) that, for any \( \phi \in A \setminus B \), there exists \( (h_\phi)_B \in V_B \) such that \( \left( \sum_{\phi \in B} h_\phi \phi \right) \_\Phi = (-\varphi^2)_\Phi \). We can then find \( f \in \mathbb{F}_q[x] \) such that \( f(\phi) = 0 \) for all \( \phi \in \Phi \); actually, \( f \) is given by

\[
f = f(x) = x^z + \sum_{\phi \in B} h_\phi \phi \in \mathbb{F}_q[x].
\]

Because \( a \in A \setminus B \) is arbitrary, a set of polynomials \( \mathcal{G}_\Phi = \{ f^{(w)} \}_{0 \leq w < z} \) is obtained and sufficient to extend \( V_B \) into \( V_A \) via \( E \) by (19) and (24); \( z \) can be taken as, at most, \( z \leq q^{N-1} \) if \( |A| = q^N \). The syndrome \( \left( \sum_{\phi \in \Phi} r_\phi \phi^2 \right)_B = \left( \sum_{\phi \in \Phi} e_\phi \phi \phi \right)_B \) can then be extended into \( E \left( \left( \sum_{\phi \in \Phi} e_\phi \phi \phi \right)_B \right) = \left( \sum_{\phi \in \Phi} e_\phi \phi \phi \right)_A \) by Proposition 5 and by function \( \mathcal{R} \circ \mathcal{F}^{-1} \), we obtain \( C \left( \left( \sum_{\phi \in \Phi} e_\phi \phi \phi \right)_B \right) = \left( e_\phi \phi \phi \right)_\Phi \) by Main Lemma.

The computation of \( \mathcal{G}_\Phi \) can be performed by the BMS algorithm; for systematic encoding, we calculate the \( \mathcal{G}_\Phi \) in advance—these play the role of generator polynomials in the case of Reed–Solomon codes. Although the following Algorithm 3 is equivalent to a special case of Algorithm 2 for \( \Phi_1 = \Phi \) and \( \Phi_2 = \emptyset \), we give it separately to describe systematic encoding.

\textbf{Algorithm 3: (DFT systematic encoding)}

\textbf{Input:} \( \Phi \) and an information word \( (h_\phi) \_\Phi \in V_\Phi \setminus \Phi \)

\textbf{Output:} \( (c_\phi) \_\Phi \in C^\perp(V_B, \Psi) \) with \( (c_\phi) \_\Phi = (h_\phi) \_\Phi \setminus \Phi \).
Step 2. (Continued from Example 13) Let

\[ \Phi = \left\{ (0, 0), (0, \alpha^2), (0, \alpha^6), (\alpha, 1), (\alpha, \alpha), (\alpha, \alpha^3), (\alpha^2, \alpha^4), (\alpha^2, \alpha^5), (\alpha^3, 1) \right\}. \]  

(33)

The Gröbner basis \( G_\Phi = \{ g^{(0)}, g^{(1)}, g^{(2)}, g^{(3)} \} \) is given by

\[
\begin{align*}
g^{(0)} &= \alpha^2 x + \alpha^7 x^2 + \alpha x^3 + x^4, \\
g^{(1)} &= \alpha^7 x + x^2 + \alpha^4 x^3 + y(\alpha^3 x + \alpha^4 x^2 + x^3), \\
g^{(2)} &= \alpha^4 x^2 + \alpha^7 x^3 + y(\alpha^4 x + \alpha^7 x^2) + y^2(\alpha^5 x + x^2), \\
g^{(3)} &= \alpha^2 x^2 + \alpha^7 x^2 + \alpha x^3 + y + y^3.
\end{align*}
\]

As \( D(\Phi) = B \), the isomorphy of (32) follows from (15). All values of Algorithm 3 are shown in Fig. 9.

---

**Example 14:** (Continued from Example 13) Let

\[ \Phi = \left\{ (0, 0), (0, \alpha^2), (0, \alpha^6), (\alpha, 1), (\alpha, \alpha), (\alpha, \alpha^3), (\alpha^2, \alpha^4), (\alpha^2, \alpha^5), (\alpha^3, 1) \right\}. \]  

(33)

The Gröbner basis \( G_\Phi = \{ g^{(0)}, g^{(1)}, g^{(2)}, g^{(3)} \} \) is given by

\[
\begin{align*}
g^{(0)} &= \alpha^2 x + \alpha^7 x^2 + \alpha x^3 + x^4, \\
g^{(1)} &= \alpha^7 x + x^2 + \alpha^4 x^3 + y(\alpha^3 x + \alpha^4 x^2 + x^3), \\
g^{(2)} &= \alpha^4 x^2 + \alpha^7 x^3 + y(\alpha^4 x + \alpha^7 x^2) + y^2(\alpha^5 x + x^2), \\
g^{(3)} &= \alpha^2 x^2 + \alpha^7 x^2 + \alpha x^3 + y + y^3.
\end{align*}
\]

As \( D(\Phi) = B \), the isomorphy of (32) follows from (15). All values of Algorithm 3 are shown in Fig. 9.
Example 15: (Continued from Example 13) Let
\[
\Phi = \begin{cases} 
(0, \alpha^3), (1, \alpha^2), (1, \alpha^4), (\alpha, \alpha), (\alpha, \alpha^5), \\
(\alpha^2, 1), (\alpha^2, \alpha^3), (\alpha^2, \alpha^6), (\alpha^3, 0), (\alpha^3, \alpha^2), \\
(\alpha^3, \alpha^4), (\alpha^3, \alpha^7), (\alpha^4, 1), (\alpha^4, \alpha^3), (\alpha^4, \alpha^6), \\
(\alpha^5, \alpha), (\alpha^5, \alpha^5), (\alpha^6, \alpha^2), (\alpha^6, \alpha^4), (\alpha^7, \alpha^3) 
\end{cases} 
\] ;
\tag{34}
\]
although we can choose \( \Phi \) as
\[
\Phi = \begin{cases} 
(0, 0), (1, 0), (\alpha, 0), (\alpha^2, 0), (\alpha^3, 0), \\
(\alpha^4, 0), (\alpha^5, 0), (\alpha^6, 0), (0, 1), (1, 1), \\
(\alpha, 1), (\alpha^2, 1), (0, \alpha), (1, \alpha), (0, \alpha^2), \\
(1, \alpha^2), (0, \alpha^3), (0, \alpha^4), (0, \alpha^5), (0, \alpha^6) 
\end{cases} 
\]
which has the same shape in \( \Omega \) as \( B \subseteq A \) because both \( \Phi \) lead to \( \det \left[ x \left( \frac{\partial \phi}{\partial x} \right) \right] \neq 0 \), we adopt (34) in order to
show Φ’s flexibility. The Gröbner basis \( G_Φ = \{ g^{(0)}, g^{(1)}, \ldots, g^{(8)} \} \) is then computed as

\[
g^{(0)} = \alpha^4 + \alpha^2 x + \alpha^2 x^2 + \alpha^6 x^3 + x^4 + x^5 + \alpha^6 x^6 + x^7 + \alpha^2 y + \alpha^6 y^2 + \alpha^6 y^3 + \alpha^4 y^4 + y^5 + \alpha^2 y^6 + y^7 + x^8,
g^{(1)} = \alpha^6 x + x^2 + \alpha^2 x^3 + \alpha^5 x^4 + \alpha^4 x^5 + \alpha x^6 + \alpha^3 x^7 + \alpha^6 y + \alpha^5 x^2 y + \alpha x^3 y + \alpha^4 y^2 + \alpha^5 x y^2 + \alpha^2 y^3 + \alpha^5 x y^3 + \alpha^4 y^4 + y^5 + \alpha^5 y^6 + \alpha^3 y^7 + x^4 y,
g^{(2)} = \alpha^4 x + \alpha^2 x^2 + \alpha^5 x^3 + \alpha^7 x^5 + \alpha^4 y + \alpha^6 x^2 y + \alpha^4 x^3 y + \alpha^2 y^2 + \alpha^6 x y^2 + \alpha^5 y^3 + \alpha^4 x y^3 + \alpha^7 y^5 + x^2 y^2,
g^{(3)} = \alpha^6 x + \alpha^5 x^2 + \alpha x^3 + \alpha^2 x^4 + \alpha^5 x^5 + \alpha^2 x^6 + \alpha^6 y + x^7 y + \alpha x^3 y + \alpha^3 y^2 + \alpha x y^2 + \alpha^3 y^3 + \alpha^5 x y^3 + \alpha^6 y^4 + \alpha^3 y^5 + \alpha^6 y^6 + x^2 y^3,
g^{(4)} = \alpha^6 x + \alpha^4 x^2 + \alpha^2 x^3 + \alpha x^4 + x^5 + \alpha^5 x^6 + \alpha^3 x^7 + \alpha^6 y + \alpha x^3 y + \alpha^5 x^3 y + y^2 + \alpha^5 x y^2 + \alpha^2 y^3 + \alpha x y^3 + \alpha^2 y^4 + \alpha^4 y^5 + \alpha y^6 + \alpha^3 y^7 + x y^4,
g^{(5)} = \alpha^3 x^2 + \alpha^7 x^2 + x^3 + \alpha^4 x^4 + \alpha^2 x^5 + \alpha^4 x^7 + \alpha^3 x y + \alpha^3 x^2 y + \alpha^3 x^3 y + \alpha^3 y^2 + \alpha^3 x y^2 + y^3 + \alpha^5 x y^3 + \alpha y^4 + \alpha^2 y^5 + y^6 + \alpha^4 y^7 + x y^5,
g^{(6)} = \alpha x + \alpha x^2 + \alpha^2 x^3 + \alpha^2 x^4 + \alpha^7 x^5 + \alpha^4 x^7 + \alpha^3 x^2 y + \alpha^3 x^3 y + \alpha^5 y^2 + \alpha^2 x y^2 + \alpha^5 y^3 + \alpha^7 x y^3 + \alpha^6 y^4 + \alpha^7 y^5 + x y^6,
g^{(7)} = 1 + \alpha x + \alpha^4 x^2 + \alpha^5 x^4 + \alpha^6 x^6 + \alpha^3 x^7 + \alpha y + \alpha^2 x y + \alpha^7 x^2 y + \alpha^7 x^3 y + \alpha^3 y^2 + \alpha^7 x y^2 + \alpha^3 x y^3 + \alpha^4 y^4 + \alpha^2 y^6 + \alpha^3 y^7 + x y^7,
g^{(8)} = \alpha^4 + \alpha^2 x + \alpha^6 x^2 + \alpha^6 x^3 + \alpha^4 x^4 + x^5 + \alpha^2 x^6 + x^7 + \alpha^2 y + \alpha^2 y^2 + \alpha^6 y^3 + y^4 + y^5 + \alpha^6 y^6 + y^7 + y^8.
\]

All values of Algorithm 3 are shown in Fig. 10.

Thus, the systematic encoding can be viewed as a special case of Algorithm 2 for \( (r_ψ, h_ψ) = (h_ψ) \) with \( h_ψ = 0 \) for all \( ψ \in Φ \). As there are many cases where the erasure-only correctable bound is exceeded, it is expected that both erasure-only and erasure-and-error can often be decoded beyond the erasure-and-error correcting bound.
TABLE I
NUMBER OF FINITE-FIELD OPERATIONS IN ALGORITHM 2

| Algorithm manipulation | order of bound |
|------------------------|----------------|
| Step 1                | \( (\sum_{\varphi \in \Phi_1} \varphi^b) \) \( B \) \( Nn^2 \) |
| Step 2                | BMS            | \( zn^2 \) |
| Step 3                | \( (\sum_{\varphi \in \Psi} \varphi \varphi^b) \) \( B \) \( Nn^2 \) |
| Step 4                | BMS            | \( zn^2 \) |
| Step 5a               | \( E \left( \left( \tilde{r}_{\varphi} \right) B \right) \) | \( nq^N \) |
| Step 5b               | \( R \circ \mathcal{F}^{-1} \left( \left( k_{\varphi} \right) A \right) \) | \( nNq^N \) |
| Step 6                | \( \left( r_{\varphi} \right) \!_{\psi} - \left( e_{\varphi} \right) \!_{\psi} \) | \( n \) |

| \( |\Phi_1|+2|\Phi_2| < d_{FR} \). In [24], the improvement and the necessary and sufficient condition for generic erasure-and-error decoding to succeed are obtained for Hermitian codes. |

**Remark 9:** If linear codes have non-trivial automorphism groups, then systematic encoding can also be performed by a division algorithm via Gröbner bases for modules [14], [19]. Indeed, there are cases where its computational complexity is less than that of Algorithm 3 as shown in [5], [39]. On the other hand, our method is more widely applicable to codes independent of automorphism groups. Another advantage of our method is that there are cases where encoding and erasure-and-error decoding are integrated, and thereby the overall size of the encoder and decoder is reduced; for the case of Reed–Solomon codes, see [23].

VI. ESTIMATION OF COMPLEXITY

**A. Simple counting**

We now estimate the number of finite-field operations, i.e., additions, subtractions, multiplications, and divisions, required by our method. We consider Algorithm 2 for the code \( C^+ (V_B, \Psi) \), as our systematic encoding algorithm corresponds to a special case of Algorithm 2. In this subsection, we simply count the operations in each step of the algorithm.

A summary of the results of our evaluation is given in Table I where \( n \) is the code length, \( N \) is the dimension of \( \Omega \), \( q \) is the finite-field size, \( z \) is the number of elements in the Gröbner bases, and Step 5 is decomposed into Step 5a of \( \left( k_{\varphi} \right) A = \mathcal{E} \left( \left( \tilde{r}_{\varphi} \right) B \right) \) and Step 5b of \( \left( e_{\varphi} \right) \!_{\psi} = R \circ \mathcal{F}^{-1} \left( \left( k_{\varphi} \right) A \right) \). We now consider the above estimation of each step.

Step 1) The calculation of DFT \( \sum_{\varphi \in \Phi_1} \varphi^b \) can be decomposed into updating \( \varphi^b \) and adding to the preserved value. This means that, at most, \( N+1 \) operations are repeated \( |\Phi_1| \) times, so \( (N+1)|\Phi_1| \) operations are required to compute one sum \( \sum_{\varphi \in \Phi_1} \varphi^b \). As there are at most \( |\Psi| = n \) values on \( B \subseteq D(\Psi) \), the total number of \( \mathbb{F}_q \)-operations in Step 1 has an upper bound of the order \( Nn^2 \).
Step 2) The computational complexity of the BMS algorithm \cite{4,7} is quoted as \(zn^2\).

Step 3) Similarly to Step 1, the calculation of DFT \(\sum_{\psi \in \Psi} r_{\psi} \psi^b\) can be decomposed into updating \(\psi^b\), multiplying by \(r_{\psi}\), and adding to the preserved value. As these three operations are repeated \(|\Psi|\) times, \((N + 2)|\Psi|\) operations are required to compute one sum \(\sum_{\psi \in \Psi} r_{\psi} \psi^b\). As there are at most \(n\) values on \(B\), the total number of \(\mathbb{F}_q\)-operations in Step 3 has an upper bound of the order \(Nn^2\).

Step 4) The order \(zn^2\) is quoted, as for Step 2.

Step 5a) For the extension of syndrome values, there are \(2|D(\Psi)| = 2|\Psi|\) additions and multiplications in the recurrence \cite{24}. Thus, the order of the upper bound for the extension is \(nq^N\).

Step 5b) Similarly to Step 3, the calculation of \(\mathcal{F}^{-1}\) can be decomposed into updating \(\omega_i^{l_1} \cdots \omega_i^{l_m}\), summing

\[
\sum_{J \subseteq \{1, 2, \ldots, N\} \setminus I} (-1)^{|J|} k_{2(I, J)}
\]

multiplying, and adding to the preserved value. The total number is \((m + 2^{N-m} + 2)q^m\), which is bounded by \((N + 3)q^N\). As these operations are repeated \(n\) times, the total number of \(\mathbb{F}_q\)-operations in Step 5b has an upper bound of the order \(nNq^N\).

Step 6) Exactly \(|\Psi| = n\) subtractions are performed.

Because \(N \leq z\), the total number of operations in Algorithm \cite{2} has an upper bound of the order \(zn^2 + nNq^N\). If \(N = 1\), then we have \(n \leq q\) and \(zn^2 + nNq^N \leq 2q^2\). Suppose that \(N > 1\). In the proof \cite{8} of \(|\text{linear codes}| = \{\text{affine variety codes}\}, \) \(q^N\) is chosen as \(q^{N-1} < n \leq q^N\), which leads to \(q^N < qn\) and \(N - 1 < \log_q n \leq N\). Then, \(zn^2 + nNq^N\) has an upper bound of the order \(n^2(z + q \log_q n)\); the factor \((z + q \log_q n)\) is comparatively less than \(n\). Thus, Algorithm \cite{2} improves the order \(n^3\) of the total computational complexity of the erasure-and-error decoding by the Gaussian elimination. Our method based on Main Lemma reduces the complexity of evaluating erasure-and-error values from \(O(n^3)\) to \(O(n^2q \log_q n)\).

B. Application of \(m\)-D DFT algorithm

In Steps 1, 3, and 5b of Algorithm \cite{2} the computations of DFT and IDFT are restricted to values on \(B\) and \(\Psi\), respectively. In this subsection, we consider the algorithm that enlarges their computations to \(A\) and \(\Omega\), i.e., the algorithm that replaces Steps 1, 3, and 5b with the following.

Step 1'. \((\tilde{v}_{\omega})_A = (\sum_{\psi \in \Phi} \psi^a\omega^b)_A \in V_A\)

Step 3'. \((\tilde{r}_{\omega})_A = (\sum_{\psi \in \Psi} r_{\psi} \omega^b\psi^a)_A \in V_A\)

Step 5b'. \((\tilde{e}_{\omega})_\Omega = \mathcal{F}^{-1}(k_2)_A \in V_\Omega\)

If the complexity of Steps 1', 3', and 5b' is estimated by the same method as for Steps 1, 3, and 5b, the result is an upper bound of the order \(Nq^{2N}\). It is well-known that the computational complexity of the ordinary FFT is of the order \(L \log L\), where \(L\) is the size of the data. As \(L = q^N\) in our case, \(L \log L\) is equal to \(Nq^N \log q\), though the ordinary FFT cannot be applied to our DFT and IDFT over the finite field. By applying the inductive expressions in Section \ref{sec:III-B} we find the computational complexities of Steps 1', 3', and 5b' to be as shown in Table \ref{table}.
Because of Propositions 2 and 3, we can argue DFT and IDFT identically, and focus on DFT. It is shown by induction that the computational complexity of calculating \( F((c_{\omega})_\Omega) = \left( \sum_{\omega \in \Omega} c_{\omega} \omega^a \right) \) is bounded by \( 3Nq^{N+1} \).

For \( N = 1 \), we obtain the bound \( 3q^2 \), as \( \sum_{\omega \in \Omega} c_{\omega} \omega^a \) is decomposed into updating \( \omega^a \), multiplying by \( c_{\omega} \), and adding to the preserved value for all \( \omega \in \Omega = \mathbb{F}_q \) and for all \( a \in A = \{0, 1, \ldots, q - 1\} \). Assume that, for \( N - 1 \), we obtain the bound \( 3(N-1)q^N \). The summation can be decomposed as

\[
\sum_{\omega_N \in \mathbb{F}_q} \omega_N^a \sum_{(\omega_1, \ldots, \omega_{N-1}) \in \mathbb{F}_q^{N-1}} c_{(\omega_1, \ldots, \omega_{N-1}, \omega_N)} \omega_1^{a_1} \cdots \omega_{N-1}^{a_{N-1}}.
\]

By induction hypothesis, the complexity of the interior summation in \((35)\) for all \( a_1, \ldots, a_{N-1} \in \{0, 1, \ldots, q - 1\} \) is bounded by \( 3(N-1)q^N \). For all \( \omega_N \in \mathbb{F}_q \), the values of the interior summation are calculated in advance. The complexity of the exterior summation in \((35)\) for all \( a_N \in \{0, 1, \ldots, q - 1\} \) is then bounded by \( 3q^2 \), from the case of \( N = 1 \). As the exterior summation is carried out for all \( a_1, \ldots, a_{N-1} \in \{0, 1, \ldots, q - 1\} \), the total complexity of computing \( F((c_{\omega})_\Omega) \) is bounded by

\[
3(N-1)q^N \times q + 3q^2 \times q^{N-1} = 3Nq^{N+1}.
\]

Thus, all DFT and IDFT parts of Algorithm 2 are bounded by the order \( Nq^{N+1} \). On the basis of the inductive expressions, the order \( nNq^N \) in the previous subsection is changed to the order \( Nq^{N+1} \), where the factor \( n \) in \( nNq^N \) is reduced to \( q \).

Finally, we show that the complexity \( O(n^2q \log_q n) \) of evaluating erasure-and-error values using the Main Lemma is improved by m-D DFT algorithm to \( O(qn^2) \). It follows from \( q^N < qn \) that the complexity of order \( nq^N \) for Step 5a is bounded by \( qn^2 \). Moreover, from \( q^{N-1} < n \leq q^N \), the complexity of order \( Nq^{N+1} \) for DFT and IDFT is

\[
Nq^{N+1} < (1 + \log_q n) q \cdot qn,
\]

where the factor \((1 + \log_q n) q \) is generally much lower than \( n \). Strictly, we have \((\log_q n) q \leq n \) for \( n \geq q \) and \( q \geq 3 \); if \( q = 2 \), then \((\log_q n) q \leq n \) is valid except for \( 2 \leq n \leq 4 \). Thus, the m-D DFT algorithm improves the complexity \( O(n^2q \log_q n) \) of evaluating erasure-and-error values to \( O(qn^2) \).

In the above estimation, the order \( nq^N \) for Step 5a is dominant in \( O(qn^2) \). However, note that the equality \( nq^N \) that defines the extension \( E \) is almost identical to that of the discrepancy of the BMS algorithm. Actually, in the
Concentrate on improving the error-correcting capability of generic erasure-and-error cases. Dual affine variety codes only after the Main Lemma has been used for error-value estimation. Future work will with Gaussian elimination affects the speed of the BMS algorithm, we have accomplished the fast decoding of encoding of a class of dual affine variety codes. We have improved the computational complexity of the error-value estimation application of our lemma, we have proposed a fast error-value estimation in the erasure-and-error decoding of the class of dual affine variety codes. We have described the construction of affine variety codes, and have shown that the systematic inverse transforms. This states that there is a canonical one-to-one linear map from a vector space indexed by \( \Omega \) from \( \mathbb{F}_q^N \). In this paper, we have generalized these to transforms between two vector spaces, each of which is indexed by \( \mathbb{F}_q^N \). Moreover, the Fourier inversion formulae of their transforms has also been generalized. We obtained a lemma using the linear recurrence relations from Gröbner bases and the generalized inverse transforms. This states that there is a canonical one-to-one linear map from a vector space indexed by the delta set of Gröbner bases onto another vector space indexed by an arbitrary subset of \( \mathbb{F}_q^N \). As an application of our lemma, we have described the construction of affine variety codes, and have shown that the systematic encoding of a class of dual affine variety codes is nothing but a special case of erasure-only decoding. As another application of our lemma, we have proposed a fast error-value estimation in the erasure-and-error decoding of the class of dual affine variety codes. We have improved the computational complexity of the error-value estimation from \( O(n^3) \) under Gaussian elimination to \( O(qn^2) \), where \( n \) is the code length. Because error-value estimation with Gaussian elimination affects the speed of the BMS algorithm, we have accomplished the fast decoding of dual affine variety codes only after the Main Lemma has been used for error-value estimation. Future work will concentrate on improving the error-correcting capability of generic erasure-and-error cases.

**Appendix A**

**Proof of Proposition 1**

It may be proved that, for \( \left( c_{\omega}' \right)_\Omega \in V_\Omega \), if \( \left( h_{\omega} \right)_A = \mathcal{F} \left( \left( c_{\omega}' \right)_\Omega \right) \) and \( \left( c_{\omega} \right)_\Omega = \mathcal{F}^{-1} \left( \left( h_{\omega} \right)_A \right) \) are defined, then \( \left( c_{\omega} \right)_\Omega = \left( c_{\omega}' \right)_\Omega \). Hence, we will show that, for all \( \omega \in \Omega \), \( c_{\omega} = c_{\omega}' \). Let \( I = I_\omega = \{ i_1, \ldots, i_m \} \) be as in Definition 2. We denote \( \overrightarrow{w} = (-1)^m \omega_{i_1}^{-1} \cdots \omega_{i_m}^{-1} \). First, note that

\[
\begin{align*}
\left( c_{\omega} \right)_\Omega &= \sum_{l_1, \ldots, l_m = 1}^{q-1} \left\{ \sum_{J \subseteq \{1, 2, \ldots, N\} \backslash I} (-1)^{|J|} h_j(I, J) \right\} \overrightarrow{w} \quad (\because \text{Definition 2}) \\
&= \sum_{l_1, \ldots, l_m = 1}^{q-1} \left\{ \sum_{J \subseteq \{1, 2, \ldots, N\} \backslash I} (-1)^{|J|} \sum_{\psi \in \Omega} c_{\psi}^{(I,J)} \right\} \overrightarrow{w} \quad (\because \text{assumption and Definition 1}) \\
&= \sum_{l_1, \ldots, l_m = 1}^{q-1} \left( \sum_{\psi \in \Omega} c_{\psi}^{(I,J)} \right) \overrightarrow{w} \quad (\because \text{changing the order of sums}) (35)
\end{align*}
\]

\(^{12}\)If \( \mathcal{F}^{-1} \circ \mathcal{F} = \text{id.} \), then \( \mathcal{F} \) is injective and \( \mathcal{F}^{-1} \) is surjective, and it follows from \( \dim V_A = \dim V_\Omega \) that \( \mathcal{F} \) and \( \mathcal{F}^{-1} \) are isomorphic and that \( \mathcal{F} \circ \mathcal{F}^{-1} = \text{id.} \).
Next, we compute the most interior sum in (36). It follows immediately from the development that

$$
\prod_{i \in \{1, 2, \ldots, N\} \setminus I_{\omega}} (1 - \psi_i^{q-1}) = \sum_{J \subseteq \{1, 2, \ldots, N\} \setminus I_{\omega}} (-1)^{|J|} \prod_{j \in J} \psi_j^{q-1}.
$$

(37)

On the other hand, because \( \psi_i^{q-1} = 1 \iff \psi \neq 0 \), we have

$$
\prod_{i \in \{1, 2, \ldots, N\} \setminus I_{\omega}} (1 - \psi_i^{q-1}) = \begin{cases} 
1 & \text{if } \psi_i = 0 \text{ for all } i \in \{1, 2, \ldots, N\} \setminus I_{\omega} \\
0 & \text{if } \exists i \in \{1, 2, \ldots, N\} \setminus I_{\omega} \text{ with } \psi_i \neq 0.
\end{cases}
$$

(38)

Then, the value \( \sum_{J \subseteq \{1, 2, \ldots, N\} \setminus I_{\omega}} (-1)^{|J|} \prod_{j \in J} \psi_j^{q-1} \) is equal to 1 or 0 according to the condition of (38). Moreover, it follows from Definition 2 that \( \omega^{(I_{\omega}, \cdot)} = \psi_1^{l_1} \cdots \psi_m^{l_m} \prod_{j \in J} \psi_j^{q-1} \). Thus, we have, for a given \( \omega \in \Omega \) and for all \( \psi \in \Omega \),

$$
\sum_{J \subseteq \{1, 2, \ldots, N\} \setminus I_{\omega}} (-1)^{|J|} \prod_{j \in J} \psi_j^{q-1} = \psi_1^{l_1} \cdots \psi_m^{l_m} \sum_{J \subseteq \{1, 2, \ldots, N\} \setminus I_{\omega}} (-1)^{|J|} \prod_{j \in J} \psi_j^{q-1}
$$

$$
= \begin{cases} 
\psi_1^{l_1} \cdots \psi_m^{l_m} & \text{if } \psi_i = 0 \text{ for all } i \in \{1, 2, \ldots, N\} \setminus I_{\omega} \\
0 & \text{if } \exists i \in \{1, 2, \ldots, N\} \setminus I_{\omega} \text{ with } \psi_i \neq 0.
\end{cases}
$$

Hence, we obtain

$$
c_{\omega} = \sum_{l_1, \ldots, l_m = 1}^{q-1} \left\{ \sum_{\omega \in \Omega, i \in I_{\omega}, \psi_i = 0} c_{\omega}^{l_1} \psi_1^{l_1} \cdots \psi_m^{l_m} \right\} \overline{\omega},
$$

where the inner sum runs over all \( \psi \in \Omega \) which satisfies \( \psi_i = 0 \) for all \( i \in \{1, 2, \ldots, N\} \setminus I_{\omega} \). This condition “\( i \notin I_{\omega} \implies \psi_i = 0 \)” of \( \psi \in \Omega \) is equivalent to “\( \psi_i \neq 0 \implies i \in I_{\omega} \)” Conversely, \( \psi \in \Omega \) with \( \psi_i = 0 \) for some \( i \in I_{\omega} \) is not contributed to the inner sum because of the factor \( \psi_1^{l_1} \cdots \psi_m^{l_m} \). Hence, we obtain

$$
c_{\omega} = \sum_{l_1, \ldots, l_m = 1}^{q-1} \left\{ \sum_{\omega \in \Omega, i \in I_{\omega}, \psi_i \neq 0} c_{\omega}^{l_1} \psi_1^{l_1} \cdots \psi_m^{l_m} \right\} \overline{\omega},
$$

where the inner sum runs over all \( \psi \in \Omega \) which satisfies \( \psi_i = 0 \) for all \( i \in \{1, 2, \ldots, N\} \setminus I_{\omega} \) and \( \psi_i \neq 0 \) for all \( i \in I_{\omega} \).

Finally, we change the order of the summations into

$$
c_{\omega} = (-1)^m \sum_{\omega \in \Omega, i \in I_{\omega}, \psi_i \neq 0} c_{\omega}^{l_1} \psi_1^{l_1} \cdots \psi_m^{l_m} \overline{\omega},
$$

and, because \( \sum_{i=1}^{q-1} (\psi_i/\omega_i)^l = 0 \) if \( \psi_i \neq \omega_i \) and \( q - 1 \) otherwise, we obtain \( c_{\omega} = (-1)^m (q - 1)^m c_{\omega}^{l_1} \overline{\omega} \). \( \square \)

**APPENDIX B**

**PROOF OF PROPOSITION 3**

Consider an \( n \times n \) matrix \( \Psi \left( \psi_{mn} \right) \) whose \((i, m)\)-th entry is equal to \( \omega_i \left( \psi_{mn} \right) \), where \( \left\{ \omega_i \mid d \in D(\Psi) \right\} = \left\{ \omega_i \mid 1 \leq i \leq n \right\} \) and \( \Psi = \left\{ \psi_{mn} \mid 1 \leq m \leq n \right\} \) are aligned by any order with \( n = |\Psi| = |D(\Psi)| \). The map

---

13 The equality (37) is also known as a variant of the inclusion-exclusion principal [21].
ev : V_D → V_{\Psi} of (16) can then be represented as
\[ (h_d)_{D} \mapsto \left( \sum_{d \in D} h_d \psi_d \right) \in \psi \]
\[ \iff \quad (h_i) \mapsto \left( h_i \right) \equiv \left( \psi_{i} \right) \]
where \((h_i)\) represents any row vector of length \(n\). Moreover, the map \(P : V_{\Psi} → V_D\) of (17) can be represented as
\[ (c_D)_{\Psi} \mapsto \left( \sum_{d \in D} c_D \psi_d \right) \in \Psi \]
\[ \iff \quad (c_i) \mapsto \left( c_i \right) \equiv \left( \psi_{i} \right) \]
where \((c_i)\) represents any row vector of length \(n\). These facts lead to Proposition 4 in case of the standard bases because \(x_{m} \equiv \left( \psi_{i} \right) \) indicates the transpose matrix whose \((l, m)\)-th entry is equal to \(x_{m} \equiv \left( \psi_{i} \right) \).

Suppose that \(\{v_1, \ldots, v_n\}\) and \(\{v'_1, \ldots, v'_n\}\) are any two normal orthogonal bases of \(V_D\) that consist of row vectors. Then there exists an \(n \times n\) matrix \(A\) with \(A^{-1} = A\) such that \([v_i] = A[v'_i]\), where \([v_i]\) and \([v'_i]\) represent the matrices whose \(i\)-th row are equal to \(v_i\) and \(v'_i\) for all \(1 \leq i \leq n\). Similarly, suppose that \(\{w_1, \ldots, w_n\}\) and \(\{w'_1, \ldots, w'_n\}\) are any two normal orthogonal bases of \(V_{\Psi}\) that consist of row vectors. Then there exists an \(n \times n\) matrix \(B\) with \(B^{-1} = B\) such that \([w_i] = B[w'_i]\). Thus, the conditions (39) and (40) indicate that
\[ (h_i) [ev(v_i)] = (h_i) X \quad \text{and} \quad (c_i) [P(w_i)] = (c_i) X \quad \text{with} \quad X = \left[ (\psi_{i}) \right] \]
if we take the standard bases \(\{v_i\}\) and \(\{w_i\}\) with the \(n\)-th identity matrix \([v_i] = [w_i]\). Suppose that \((h_i) [ev(v'_i)] = (h_i) Y[w'_i]\) and \((c_i) [P(w'_i)] = (c_i) Z[w'_i]\).

Because \([ev(v'_i)] = A^{-1}[ev(v_i)]\) and \([P(w'_i)] = B^{-1}[P(w_i)]\) follow from \([v'_i] = A^{-1}[v_i]\), \([w'_i] = B^{-1}[w_i]\), and the linearity of \(ev\) and \(P\), we have
\[ YB^{-1} = [ev(v'_i)] = A^{-1}[ev(v_i)] = A^{-1}X \]
\[ \text{and} \quad ZA^{-1} = [P(w'_i)] = B^{-1}[P(w_i)] = B^{-1}X. \]

Thus we have \(Y = A^{-1}X B, Z = B^{-1}X A,\) and \(Y = Z\), which leads to Proposition 4 in case of any normal orthogonal bases. □

**APPENDIX C**

**PROOF OF PROPOSITION 5**

From the assumption, we have
\[ h_d = \sum_{\psi \in \Psi} c_\psi \psi_d, \]
where \(\psi_d \in D = D(\Psi)\). We now show that (41) holds not only for \(d \in D\) but also for \(a \in A\) if \(h_a \equiv (h_a)_A \in E ((h_a)_D)\).

Actually, we have
\[ h_a = \sum_{d \in D} v_d h_a = \sum_{d \in D} v_d \sum_{\psi \in \Psi} c_\psi \psi_d \]
\[ = \sum_{\psi \in \Psi} c_\psi \sum_{d \in D} v_d \psi_d = \sum_{\psi \in \Psi} c_\psi \psi_a, \]
where we use \(\sum_{d \in D} v_d \psi_d = \psi_a\), which follows from (21) and \(g^{(w)}(a) \in Z_{\psi}\). Thus, (41) holds for all \(a \in A\); in other words, \((h_a = \sum_{\psi \in \Psi} c_\psi \psi_a)_A\) holds. □
APPENDIX D

PROOF OF PROPOSITION 6

Let \( c_i \in V_\Psi \) be \( (h_d)_D = \left( \sum_{\psi \in \Psi} c_{\psi} d \right)_D \in V_D \) according to the isomorphism \( P : V_\Psi \to V_D \) of (17). If \( (h_d)_A = \mathcal{E}(h_d)_D \), then we obtain \( (h_d)_{\Psi} = \left( \sum_{\psi \in \Psi} c_{\psi} \psi \right)_A \) by Proposition 5. On the other hand, because \( a^\gamma \mathbb{w}^v g(w) \in Z_\Psi \), we have, for all \( \psi \in \Psi \),

\[
\psi^{\omega} = - \sum_{d \in D} g_d(w) \psi^{\alpha + d - \mathbb{w}}.
\]

Thus, we have

\[
(h_d)_{\Psi} = \sum_{\psi \in \Psi} c_{\psi} \left\{ - \sum_{d \in D} g_d(w) \psi^{\alpha + d - \mathbb{w}} \right\}
= - \sum_{d \in D} g_d(w) \left\{ \sum_{\psi \in \Psi} c_{\psi} \psi^{\alpha + d - \mathbb{w}} \right\}
= - \sum_{d \in D} g_d(w) \psi^{\alpha + d - \mathbb{w}}.
\]

Conversely, suppose that \( (h_d)_{A} \in V_A \) satisfies that, for each \( a \in A \setminus D \), there exists at least one \( 0 \leq w < z \) such that (24). If there are \( a \in A \) and \( 0 \leq v \neq w < z \) such that \( a \geq a_v \) and \( a \geq a_w \), then it follows from \( x_a^v - x_a^w g(v) - x_a^v - x_a^w g(w) \in Z_\Psi \) that \( \sum_{d \in D} g_d(v) h_a + d - \mathbb{w} = \sum_{d \in D} g_d(w) h_a + d - \mathbb{w} \). By the same argument as above, Thus, \( h_d \) in the left-hand side of (24) does not depend on the choice and order of \( v, w \). \( \square \)

APPENDIX E

PROOF OF \( C^\perp(U, \Psi) = C \left( U^\perp \right) \)

We show that, for all \( (c_i')_{\Psi} \in \text{ev}(U) \) and all \( (c_i')_{\Psi} \in C \left( U^\perp \right) \), the value of the inner product \( \sum_{\psi \in \Psi} c_{\psi} c_{\psi} \) is equal to zero. Let \( (c_i) = (c_i')_{1 \leq i \leq n} \) be the aligned \( (c_i')_{\Psi} \), as in Appendix B. By (39), \( (c_i')_{\Psi} \in \text{ev}(U) \) is represented as

\[
(c_i') = (h_i') \left[ x_m \left( \psi_i \right) \right] \quad \text{for some } (h_i') \in U.
\]

Similarly, let \( (c_i) = (c_i')_{1 \leq i \leq n} \) be the aligned \( (c_i')_{\Psi} \). As \( C = P^{-1} \) and (40), \( (c_i')_{\Psi} \in C \left( U^\perp \right) \) is represented as

\[
(c_i) = (h_i) \left[ x_m \left( \psi_i \right) \right]^{-1} \quad \text{for some } (h_i) \in U^\perp.
\]

Because the transpose of the row vector \( (c_i') \) is equal to a column vector \( (c_i') = \left[ x_m \left( \psi_i \right) \right] (h_i'), \sum_{\psi \in \Psi} c_{\psi} c_{\psi} \) is equal to

\[
(c_i)(c_i') = (h_i) \left[ x_m \left( \psi_i \right) \right]^{-1} \left[ x_m \left( \psi_i \right) \right] (h_i') = 0. \quad \square
\]

ACKNOWLEDGMENT

The author would like to thank the anonymous referees for their useful comments that helped improve the final presentation of the paper.
REFERENCES

[1] H.E. Andersen, O. Geil, “Evaluation codes from order domain theory,” Finite Fields their Appl., vol.14, no.1, pp.92–123, Jan. 2008.
[2] M. Bras-Amorós, M.E. O’Sullivan, “The correction capability of the Berlekamp–Massey–Sakata algorithm with majority voting,” Appl. Algebra Eng. Commun. Comput., vol.17, no.5, pp.315–335, Oct. 2006.
[3] O. Geil, T. Høholdt, “Footprints or generalized Bezout’s theorem,” IEEE Trans. Inf. Theory, vol.46, no.2, pp.635–641, Mar. 2000.
[4] O. Geil, T. Høholdt, “On hyperbolic codes,” in Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes: Proc. AAECC-14, S. Boztaş and I.E. Shparlinski, eds., pp.227–235, Springer, 2001.
[5] H. Matsui, S. Mita, “Encoding via Gröbner bases and discrete Fourier transforms for several types of algebraic codes,” IEEE Int. Symp. Inf. Theory, pp.2656–2660, Nice, France, Jun. 24–29, 2007.
[6] H. Matsui, S. Mita, “Unified system of encoding and decoding erasures and errors for algebraic geometry codes,” Int. Symp. on Inf. Theory and its Applications, Taichung, Taiwan, pp.1001–1006, Oct. 17–20, 2010.
[7] H. Matsui, “Fast erasure-and-error decoding and systematic encoding of a class of affine variety codes,” The 34th Symp. on Inf. Theory and its Applications, Ousyuku, Iwate, Japan, pp.405–410, Nov. 29–Dec. 2, 2011. http://arxiv.org/abs/1208.5429
Hajime Matsui received a B.S. degree in 1994 from the Department of Mathematics, Shizuoka University, Japan, an M.S. degree in 1996 from the Graduate School of Science and Technology, Niigata University, Japan, and Ph.D. in 1999 from the Graduate School of Mathematics, Nagoya University, Japan. From 1999 to 2002, he was a Postdoctorate Fellow in the Department of Electronics and Information Science at the Toyota Technological Institute, Japan. From 2002 to 2006, he was a Research Associate at the same institute, where he has been working as an Associate Professor since 2006. His research interests include coding theory, computer science, and number theory.
### List of Main Notation

| Symbol | Description |
|--------|-------------|
| $d_{\text{min}}$ | minimum distance of the code |
| $d_{\text{FR}}$ | Feng–Rao bound of $d_{\text{min}}$ |
| $n$ | code length |
| $q$ | finite-field size |
| $z$ | size of Gröbner basis |
| $N$ | dimension of index set |
| $D = D(\Psi)$ | delta set |
| $\Psi$ | subset of $\mathbb{F}_q^N$ with size $n > 0$ |
| $N_0$ | set of non-negative integers |
| $A \setminus B$ | $\{u \in A | u \notin B\}$ for sets $A, B$ |
| $|S|$ | number of elements in $S$ |
| $V_S$ | $\{(v_s)_S | s \in S, v_s \in \mathbb{F}_q\}$ |
| $A = A_N$ | $\{0, 1, \ldots, q - 1\}^N$ in (1) |
| $\Omega = \Omega_N$ | $\mathbb{F}_q^N$ in (3) |
| $\hat{a}$ | an element of $A$ in (1) |
| $(h_{\hat{a}})_A$ | a vector in $V_A$ |
| $\omega$ | an element of $\Omega$ in (3) |
| $(c_{\omega})_{\Omega}$ | a vector in $V_{\Omega}$ |
| $F = F_N$ | $N$-D generalized DFT (4) |
| $\omega^k$ | $\omega_1^{k_1} \cdots \omega_N^{k_N}$ |
| $F_N^{-1} = F_N^{-1}$ | $N$-D generalized IDFT (5,6) |
| $\mathbb{F}_q[x]$ | ring of $N$-variable polynomials |
| $Z_\Psi$ | an ideal of $\mathbb{F}_q[x]$ |
| $\preceq$ | a fixed monomial order |
| $\text{LM}(f)$ | leading monomial (14) |
| $\text{mdeg}(x^d)$ | $d$ for $x^d \in \mathbb{F}_q[x]$ |
| $\text{ev}$ | evaluation map (15,16) |
| $\mathcal{P}$ | proper transform (17) |
| $\mathcal{G}_\Psi$ | a Gröbner basis of $Z_\Psi$ |
| $g^{(w)}$ | an element of $\mathcal{G}_\Psi$ |
| $\mathcal{E}$ | extension map (19) |
| $\mathcal{I}$ | inclusion map (22) |
| $\mathcal{G}_w$ | leading monomial $\text{LM}(g^{(w)})$ |
| $\hat{a} + \hat{b}$ | component-wise addition |
| $\hat{a} \geq \hat{b}$ | component-wise inequality |
| $\mathcal{R}$ | restriction map (25) |
| $C(U, \Psi)$ | $\text{ev}(U)$ in (28) |
| $C(U, \Psi)$ | $\text{ev}(U)$ in $C(U, \Psi)$ |
| $k$ | dimension of $C(U, \Psi)$ |
| $B$ | a subset of $D(\Psi)$ |
| $V_D \setminus B$ | $V_D^B$ in $V_D$ |
| $\mathbf{r}_\Psi$ | an erasure-and-error vector in $V_\Psi$ |
| $\mathbf{e}_\Psi$ | a received word $(\mathbf{e}_\Psi) + (\mathbf{e}_\Psi)$ |
| $\Phi_1$ | set of erasure locations |
| $\Phi_2$ | set of error locations |
| $\Phi$ | set of redundant locations |