Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
San Antonio, TX, USA - October 2009

A Note on the Relation between a Sampling Theorem for Functions over a $GF(q)^n$ Domain and Linear Codes

Yoshifumi Ukita*, Tomohiko Saito†, Toshiyasu Matsushima‡ and Shigeichi Hirasawa§
*Department of Management Information, Yokohama College of Commerce
4-11-1 Higashiterao, Tsurumi, Yokohama, Kanagawa 230-8577, Japan
Email: ukita@shodai.ac.jp
†College of Science and Engineering, Aoyama Gakuin University, Sagamihara, Kanagawa 229-8558, Japan
‡School of Fundamental Science and Engineering, Waseda University, Tokyo 169-8555, Japan
§Research Institute for Science and Engineering, Waseda University, Tokyo 169-8555, Japan,
and Cyber University, Tokyo 162-0853, Japan

***Abstract*—In this paper, we generalize the sampling theorem for bandlimited functions over the Boolean domain to a sampling theorem for bandlimited functions over a $GF(q)^n$ domain. We also present a theorem for the relation between the parity check matrix of a linear code and any distinct error vectors. Lastly, we clarify the relation between the sampling theorem for functions over a $GF(q)^n$ domain and linear codes.**

***Index Terms*—discrete Fourier transform, error-correcting codes, experimental designs, orthogonal designs**

I. Introduction

The Fourier series representation of a function is a classic representation which is widely used to approximate real functions. In digital signal processing[7], the sampling theorem states that any real valued function f can be reconstructed from a sequence of values of f that are discretely sampled with a frequency at least twice as high as the maximum frequency of the spectrum of f. This theorem can also be applied to functions over a finite domain[8], [12], [13]. Then, the range of frequencies of f can be expressed in more detail by using a bounded set instead of the maximum frequency. A function whose range of frequencies is confined to a bounded set I is referred to as bandlimited to I. Ukita et al.[13] obtained a sampling theorem for bandlimited functions over the Boolean domain.

However, it is important to obtain a sampling theorem for functions not only over the Boolean domain but also over a $GF(q)^n$ domain. For example, in experimental designs, the model can be expressed as a linear combination of the Fourier basis functions over the $GF(q)^n$ domain. However, the sampling theorem for bandlimited functions over the $GF(q)^n$ domain has not been obtained. On the other hand, the sampling points are closely related to the codewords of a linear code. In addition, it is known that there exist some relations between experimental designs and error-correcting codes[3], [9]. In coding theory, because the minimum distance of a code is important, the relation between the parity check matrix of a linear code and the minimum distance has been obtained[2], [5]. However, the relation between the parity check matrix of a linear code and any distinct error vectors has not been obtained, although it is necessary for understanding the meaning of the sampling theorem for bandlimited functions.

In this paper, we generalize the sampling theorem for bandlimited functions over the Boolean domain to a sampling theorem for bandlimited functions over a $GF(q)^n$ domain. We also present a theorem for the relation between the parity check matrix of a linear code and any distinct error vectors. Lastly, we clarify the relation between the sampling theorem for functions over a $GF(q)^n$ domain and linear codes.

II. Preliminaries

A. Basis Functions for the Class of Boolean Functions

Let $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$. Boolean functions of n variables can be considered as real valued functions, $f : \{0,1\}^n \to \{-1,+1\}$. An orthonormal basis for the class of Boolean functions can be given as follows. For each $\boldsymbol{z} = (z_1, z_2, \ldots, z_n) \in \{0,1\}^n$, define the function

$$\mathcal{X}_{\boldsymbol{z}}(\boldsymbol{x}) = (-1)^{\boldsymbol{z}\boldsymbol{x}^T}, \tag{1}$$

where the inner product $\boldsymbol{z}\boldsymbol{x}^T = z_1x_1 + z_2x_2 + \cdots + z_nx_n$ is to be performed modulo 2 and T denotes transposition. Then, the functions $\{\mathcal{X}_{\boldsymbol{z}} | \boldsymbol{z} \in \{0,1\}^n\}$ form an orthonormal basis. That is,

$$\frac{1}{2^n} \sum_{\boldsymbol{x}\in\{0,1\}^n} \mathcal{X}_{\boldsymbol{z}}(\boldsymbol{x})\mathcal{X}_{\boldsymbol{v}}(\boldsymbol{x}) = \begin{cases} 1, & \boldsymbol{z} = \boldsymbol{v}, \\ 0, & \boldsymbol{z} \neq \boldsymbol{v}. \end{cases} \tag{2}$$

Any real valued function of n Boolean inputs can then be uniquely expressed as a linear combination of the basis functions:

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{z}\in\{0,1\}^n} f_{\boldsymbol{z}}\mathcal{X}_{\boldsymbol{z}}(\boldsymbol{x}), \tag{3}$$

where the real number $f_{\boldsymbol{z}}$ is the $\boldsymbol{z}$-th *Fourier coefficient* of f,

$$f_{\boldsymbol{z}} = \frac{1}{2^n} \sum_{\boldsymbol{x}\in\{0,1\}^n} f(\boldsymbol{x})\mathcal{X}_{\boldsymbol{z}}(\boldsymbol{x}). \tag{4}$$

978-1-4244-2794-9/09/$25.00 ©2009 IEEE

B. Generalized Basis Functions

Suppose q is a prime power. Let $GF(q)$ be a Galois field of order q and let $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in GF(q)^n$. For each $\boldsymbol{a} = (a_1, a_2, \ldots, a_n) \in GF(q)^n$, define the *Fourier basis function* $\mathcal{X}_{\boldsymbol{a}}(\boldsymbol{x})$

$$\mathcal{X}_{\boldsymbol{a}}(\boldsymbol{x}) = e^{i2\pi \boldsymbol{a}\boldsymbol{x}^T/q}, \tag{5}$$

where $i^2 = -1$ and the inner product $\boldsymbol{a}\boldsymbol{x}^T$ is evaluated over $GF(q)$. Equation (1) is a special case ($q = 2$) of Equation (5).

The functions $\{\mathcal{X}_{\boldsymbol{a}} | \boldsymbol{a} \in GF(q)^n\}$ form an orthonormal system,

$$\frac{1}{q^n} \sum_{\boldsymbol{x} \in GF(q)^n} \mathcal{X}_{\boldsymbol{a}}(\boldsymbol{x}) \mathcal{X}^*_{\boldsymbol{b}}(\boldsymbol{x}) = \begin{cases} 1, & \boldsymbol{a} = \boldsymbol{b}, \\ 0, & \boldsymbol{a} \neq \boldsymbol{b}, \end{cases} \tag{6}$$

where $\mathcal{X}^*_{\boldsymbol{b}}(\boldsymbol{x})$ is the complex-conjugate of $\mathcal{X}_{\boldsymbol{b}}(\boldsymbol{x})$. Any complex valued function can be uniquely expressed as a linear combination of the Fourier basis functions:

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{a} \in GF(q)^n} f_{\boldsymbol{a}} \mathcal{X}_{\boldsymbol{a}}(\boldsymbol{x}), \tag{7}$$

where the complex number

$$f_{\boldsymbol{a}} = \frac{1}{q^n} \sum_{\boldsymbol{x} \in GF(q)^n} f(\boldsymbol{x}) \mathcal{X}^*_{\boldsymbol{a}}(\boldsymbol{x}) \tag{8}$$

is the $\boldsymbol{a}$-th *Fourier coefficient* of f.

III. Experimental Design

In this section, we provide a short introduction to experimental design. For a detailed explanation, refer to [11].

A. Model of Experimental Design

Let $F_1, F_2, \ldots, F_n$ denote the n factors to be included in the experiment. The levels of each factor can be represented by $GF(q)$, and the level combinations can be represented by the n-tuples $(x_1, x_2, \ldots, x_n) \in GF(q)^n$.

We use $y(\boldsymbol{x})$ to denote the response of the experiment with level combination $\boldsymbol{x}$ and assume the model

$$y(\boldsymbol{x}) = \sum_{\boldsymbol{a} \in I_A} f_{\boldsymbol{a}} \mathcal{X}_{\boldsymbol{a}}(\boldsymbol{x}) + \epsilon_{\boldsymbol{x}}. \tag{9}$$

where

$$I_A = \{(b_1 a_1, b_2 a_2, \ldots, b_n a_n) | \boldsymbol{a} \in A, b_i \in GF(q)\}. \tag{10}$$

The set $A \subseteq \{0,1\}^n$ represents the main and interactive factors included in the model. (For example, $A = \{000, 100, 010, 001, 110\}$ suggests main factors of F_1, F_2, F_3 and an interactive factor of $F_1 F_2$.) The effect of a main or interactive factor $\boldsymbol{a} \in I_A$ is represented by an unknown parameter $f_{\boldsymbol{a}}$. The model includes a random error $\epsilon_{\boldsymbol{x}}$ that has mean 0 and constant variance σ^2. In addition, we assume that the set A satisfies the following monotonicity condition.

Definition 1: Monotonicity

$$\boldsymbol{a} \in A \rightarrow \boldsymbol{b} \in A \qquad \forall \boldsymbol{b}\ (\boldsymbol{b} \sqsubseteq \boldsymbol{a}), \tag{11}$$

where $(b_1, b_2, \ldots, b_n) \sqsubseteq (a_1, a_2, \ldots, a_n)$ means that if $a_i = 0$ then $b_i = 0, i = 1, 2, \ldots, n$. □

Example 1:

$$\begin{aligned} A \;=\; & \{00000, 10000, 01000, 00100, 00010, 00001, \\ & 11000, 10100, 10010\}, \end{aligned}$$

is monotonic and, if $q = 3$, I_A is given by

$$\begin{aligned} I_A \;=\; & \{00000, 10000, 20000, 01000, 02000, 00100, 00200, \\ & 00010, 00020, 00001, 00002, 11000, 12000, 21000, \\ & 22000, 10100, 10200, 20100, 20200, 10010, 10020, \\ & 20010, 20020\}. \end{aligned}$$

□

In experimental design, we are given a model of experiment. That is, we are given a set $A \subseteq \{0,1\}^n$. First, we determine a set of level combinations $\boldsymbol{x}$, $X \subseteq GF(q)^n$, that is called a design. Then, we experiment according to the design X and estimate the effects, $f_{\boldsymbol{a}}$ ($\boldsymbol{a} \in I_A$), from the results of the experiments, $\{(\boldsymbol{x}, y(\boldsymbol{x})) | \boldsymbol{x} \in X\}$.

It is important to construct designs so that all effects in the model can be estimated, while the number of experiments is kept to a minimum.

B. Orthogonal Designs [11]

Definition 2: (Orthogonal Designs)

Define $v(\boldsymbol{a}) = \{i | a_i \neq 0, 1 \leq i \leq n\}$. For any $A \subseteq \{0,1\}^n$, let H_A be the $(n-k) \times n$ matrix

$$H_A = \begin{bmatrix} h_{1,1} & h_{1,2} & \ldots & h_{1,n} \\ h_{2,1} & h_{2,2} & \ldots & h_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k,1} & h_{n-k,2} & \ldots & h_{n-k,n} \end{bmatrix}. \tag{12}$$

The entries in this matrix, $h_{ij} \in GF(q) (1 \leq i \leq n-k, 1 \leq j \leq n)$, satisfy the following conditions.

1) The set $\{\boldsymbol{h}_{\cdot j} | j \in v(\boldsymbol{a}' + \boldsymbol{a}'')\}$[1], where $\boldsymbol{h}_{\cdot j}$ is the j-th column of H_A, is linearly independent over $GF(q)$ for any given $\boldsymbol{a}', \boldsymbol{a}'' \in A$.
2) The set $\{\boldsymbol{h}_{i\cdot} | 1 \leq i \leq n-k\}$, where $\boldsymbol{h}_{i\cdot}$ is the i-th row of H_A, is linearly independent over $GF(q)$.

An *orthogonal design* $C^\perp$ for main and interactive factors $A \subseteq \{0,1\}^n$ is defined by

$$C^\perp = \{\boldsymbol{x} | \boldsymbol{x} = \boldsymbol{r} H_A,\ \boldsymbol{r} \in GF(q)^{n-k}\} \tag{13}$$

and $|C^\perp| = q^{n-k}$. □

Example 2: We consider the case $n = 5$,

$$\begin{aligned} A \;=\; & \{00000, 10000, 01000, 00100, 00010, 00001, \\ & 11000, 10100, 10010\}, \end{aligned} \tag{14}$$

and $q = 3$. In this case,

$$H_A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 2 \end{bmatrix}, \tag{15}$$

[1] For $\boldsymbol{a}_1 = (a_{11}, a_{12}, \ldots, a_{1n}), \boldsymbol{a}_2 = (a_{21}, a_{22}, \ldots, a_{2n}) \in \{0,1\}^n$, the addition of vectors $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ is defined by $\boldsymbol{a}_1 + \boldsymbol{a}_2 = (a_{11} \oplus a_{21}, a_{12} \oplus a_{22}, \ldots, a_{1n} \oplus a_{2n})$, where $\oplus$ is exclusive or.

satisfies the conditions in Definition 2. Therefore,

$$\begin{aligned} C^{\perp} \;\; = \;\; & \{00000, 00112, 00221, 01011, 01120, 01202, 02022 \\ & 02101, 02210, 10000, 10112, 10221, 11011, 11120, \\ & 11202, 12022, 12101, 12210, 20000, 20111, 20221, \\ & 21011, 21120, 21202, 22022, 22101, 22210\}, \end{aligned}$$

is an orthogonal design for A. □

It is known that the unbiased estimators of $f_{\boldsymbol{a}}$ calculated from an orthogonal design $C^{\perp}$ are optimal compared to those from other designs that have the same number of experiments as $C^{\perp}$[11]. Therefore, many algorithms to construct H_A have been proposed [3], [9], [11], [13]. However, because the purpose of this paper is not to construct orthogonal designs, the algorithm is not included in this paper.

IV. Sampling Theorem for Functions over a $GF(q)^n$ domain

A. Bandlimited Functions

The range of frequencies of f is defined by a bounded set I. Then, $f_{\boldsymbol{a}} = 0$ for all $\boldsymbol{a} \in GF(q)^n \setminus I$. Any function whose range of frequencies is confined to a bounded set I is referred to as bandlimited to I.

B. A Sampling Theorem for Bandlimited Functions over a $GF(q)^n$ Domain

In this section, we consider the case of a bounded set[2] I_A defined by Equation (10), where the set A is monotonic.

Theorem 1: Suppose a set A is monotonic and $f(\boldsymbol{x})$ is expressed as

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{a} \in I_A} f_{\boldsymbol{a}} \mathcal{X}_{\boldsymbol{a}}(\boldsymbol{x}). \tag{16}$$

Then, the Fourier coefficients can be computed by

$$f_{\boldsymbol{a}} = \frac{1}{|C^{\perp}|} \sum_{\boldsymbol{x} \in C^{\perp}} f(\boldsymbol{x}) \mathcal{X}^*_{\boldsymbol{a}}(\boldsymbol{x}), \tag{17}$$

where $C^{\perp}$ is an orthogonal design as defined in Definition 2. □

Before proving Theorem 1, two lemmas needed for the proof are given.

Lemma 1: For an $(n-k) \times n$ matrix H and a vector $\boldsymbol{s} \in GF(q)^{n-k}$, define $C_{\boldsymbol{s}} = \{\boldsymbol{a} | \boldsymbol{s} = \boldsymbol{a}H^T, \boldsymbol{a} \in GF(q)^n\}$. Then, for any vector $\boldsymbol{a} \in C_{\boldsymbol{s}}$,

$$\sum_{\boldsymbol{c} \in C_{\boldsymbol{s}}} f_{\boldsymbol{c}} = \frac{1}{q^{n-k}} \sum_{\boldsymbol{x} \in C^{\perp}} f(\boldsymbol{x}) \mathcal{X}^*_{\boldsymbol{a}}(\boldsymbol{x}). \tag{18}$$

Proof: Using $f(\boldsymbol{x}) = \sum_{\boldsymbol{c} \in GF(q)^n} f_{\boldsymbol{c}} \mathcal{X}_{\boldsymbol{c}}(\boldsymbol{x})$, we see that the right-hand side of Equation (18) is given by

$$\begin{aligned} & \frac{1}{q^{n-k}} \sum_{\boldsymbol{x} \in C^{\perp}} \sum_{\boldsymbol{c} \in GF(q)^n} f_{\boldsymbol{c}} \mathcal{X}_{\boldsymbol{c}}(\boldsymbol{x}) \mathcal{X}^*_{\boldsymbol{a}}(\boldsymbol{x}) \\ & = \frac{1}{q^{n-k}} \sum_{\boldsymbol{c} \in GF(q)^n} \sum_{\boldsymbol{r} \in GF(q)^{n-k}} f_{\boldsymbol{c}} \mathcal{X}_{\boldsymbol{c}}(\boldsymbol{r}H) \mathcal{X}^*_{\boldsymbol{a}}(\boldsymbol{r}H) \\ & = \sum_{\boldsymbol{c} \in GF(q)^n} f_{\boldsymbol{c}} \left(\frac{1}{q^{n-k}} \sum_{\boldsymbol{r} \in GF(q)^{n-k}} \mathcal{X}_{\boldsymbol{c}H^T}(\boldsymbol{r}) \mathcal{X}^*_{\boldsymbol{a}H^T}(\boldsymbol{r}) \right) \\ & = \sum_{\boldsymbol{c} \in GF(q)^n} f_{\boldsymbol{c}} \left(\frac{1}{q^{n-k}} \sum_{\boldsymbol{r} \in GF(q)^{n-k}} \mathcal{X}_{\boldsymbol{c}H^T}(\boldsymbol{r}) \mathcal{X}^*_{\boldsymbol{s}}(\boldsymbol{r}) \right). \end{aligned} \tag{19}$$

Now if $\boldsymbol{c} \in C_{\boldsymbol{s}}$, then $\boldsymbol{c}H^T = \boldsymbol{s}$ holds. Therefore, using Equation (6), we have

$$\frac{1}{q^{n-k}} \sum_{\boldsymbol{r} \in GF(q)^{n-k}} \mathcal{X}_{\boldsymbol{c}H^T}(\boldsymbol{r}) \mathcal{X}^*_{\boldsymbol{s}}(\boldsymbol{r}) = \begin{cases} 1, & \boldsymbol{c} \in C_{\boldsymbol{s}}, \\ 0, & \boldsymbol{c} \notin C_{\boldsymbol{s}}. \end{cases} \tag{20}$$

Combining Equations (19) and (20), we obtain Equation (18). □

Lemma 2: Suppose $\boldsymbol{a} \in C_{\boldsymbol{s}}$ and that for all $\boldsymbol{b} \in C_{\boldsymbol{s}}(\boldsymbol{b} \neq \boldsymbol{a})$ we have $f_{\boldsymbol{b}} = 0$. Then, the following equation holds.

$$f_{\boldsymbol{a}} = \frac{1}{q^{n-k}} \sum_{\boldsymbol{x} \in C^{\perp}} f(\boldsymbol{x}) \mathcal{X}_{\boldsymbol{a}}(\boldsymbol{x}). \tag{21}$$

Proof: This is immediate from Lemma 1. □

We are now ready for the proof of Theorem 1.

Proof of Theorem 1: Let $\boldsymbol{a} \in C_{\boldsymbol{s}}(\boldsymbol{a} \in I_A)$. From Definition 2 and Equation (10), every set $\{\boldsymbol{h}_{\cdot j} | j \in v(\boldsymbol{a} - \boldsymbol{c})\}$ is linearly independent for all $\boldsymbol{c} \in I_A(\boldsymbol{c} \neq \boldsymbol{a})$. Hence

$$H_A(\boldsymbol{a} - \boldsymbol{c})^T \neq \boldsymbol{0}, \tag{22}$$

holds. This implies

$$H_A \boldsymbol{a}^T \neq H_A \boldsymbol{c}^T. \tag{23}$$

From $\boldsymbol{a} \in C_{\boldsymbol{s}}$ and Equation (23), we have $\boldsymbol{c} \notin C_{\boldsymbol{s}}$ for all $\boldsymbol{c} \in I_A(\boldsymbol{c} \neq \boldsymbol{a})$. Therefore, for all $\boldsymbol{b} \in C_{\boldsymbol{s}}(\boldsymbol{b} \neq \boldsymbol{a})$, $f_{\boldsymbol{b}} = 0$ holds. Hence, by Lemma 2, Equation (17) holds. □

C. Estimation of the parameters in experimental designs

When we experiment according to the orthogonal design $C^{\perp}$, we can use Theorem 1 to obtain unbiased estimators of the $f_{\boldsymbol{a}}$ in Equation (9):

$$\hat{f_{\boldsymbol{a}}} = \frac{1}{q^{n-k}} \sum_{\boldsymbol{x} \in C^{\perp}} y(\boldsymbol{x}) \mathcal{X}^*_{\boldsymbol{a}}(\boldsymbol{x}). \tag{24}$$

In particular, when $q = 2^m$ where m is a integer and $m \geq 1$, we can use the vector-radix fast Fourier transform (FFT), which is a multidimensional fast Fourier transform, to calculate Equation (24) for all $\boldsymbol{a} \in I_A$. The complexity of vector-radix FFT is $O(q^{n-k} \log q^{n-k})$.

[2] Of course it is not necessary to have $f_{\boldsymbol{a}} \neq 0$ for all $\boldsymbol{a} \in I_A$. It is similar to the sampling theorem[7] for the maximum frequency of the spectrum of f. In digital signal processing, frequency limitation by using a bounded set I_A has not been presented.

V. Relation between the parity check matrix of a linear code and any distinct error vectors

In data transmission over noisy communication channels, a desired level of error control is ensured through the use of error-correcting codes[5]. Linear codes are the most important for practical applications in error-correcting codes.

Sampling points are closely related to the codewords of a linear code.

A. Linear Codes

Linear codes are defined as follows.

Definition 3: (Linear Code)

Let H be an $(n-k)\times n$ matrix with entries from $GF(q)$, having $n-k$ linear independent rows. The linear code C with parity check matrix H is defined by

$$C=\{\boldsymbol{x}|H\boldsymbol{x}^T=\boldsymbol{0}^T,\boldsymbol{x}\in GF(q)^n\} \tag{25}$$

and $|C|=q^k$. □

Now, it is always possible to find a matrix of the form

$$H=[I_{n-k},P] \tag{26}$$

where I_{n-k} is the $(n-k)\times(n-k)$ unit matrix and P is some $(n-k)\times k$ matrix. The linear code C can then be expressed as

$$C=\{\boldsymbol{x}|\boldsymbol{u}G=\boldsymbol{x},\boldsymbol{u}\in GF(q)^k\}, \tag{27}$$

where

$$G=[-P^T,I_k] \tag{28}$$

and

$$GH^T=\boldsymbol{0}, \tag{29}$$

with $\boldsymbol{0}$ being the $k\times(n-k)$ zero matrix.

Example 3: Consider a ternary code with parity check matrix

$$H=\begin{bmatrix}1&0&0&0&0\\0&1&0&1&1\\0&0&1&1&2\end{bmatrix}. \tag{30}$$

Then,

$$G=\begin{bmatrix}0&2&2&1&0\\0&2&1&0&1\end{bmatrix}, \tag{31}$$

and

$$C=\{00000,02101,01202,02210,01011,00112,01120,00221,00022\}.$$

□

A code $C^{\perp}=\{\boldsymbol{x}|\boldsymbol{x}=\boldsymbol{r}H,\ \boldsymbol{r}\in GF(q)^{n-k}\}$ is called the dual code of C.

The *Hamming weight* $w(\boldsymbol{a})$ of a vector $\boldsymbol{a}$ is defined as the number of nonzero components.

The *Hamming distance* $d_H(\boldsymbol{u},\boldsymbol{v})$ between two vectors $\boldsymbol{u},\boldsymbol{v}$ is defined to be the number of positions where they differ,

$$d_H(\boldsymbol{u},\boldsymbol{v})=w(\boldsymbol{u}-\boldsymbol{v}). \tag{32}$$

We define the *minimum distance* of a code C to be the minimum Hamming distance between distinct codewords in C.

B. Parity check matrix H of a linear code C

We begin by stating two lemmas concerning the relation between the parity check matrix H and the minimum distance.

The first lemma, which establishes the relationship between the parity check matrix H of a linear code C and the minimum distance, is taken from [5].

Lemma 3: If H is the parity check matrix of a linear code C, then the minimum distance of the code is greater than or equal to $2t+1$ if and only if every set of $2t$ columns of H is linearly independent. □

The second lemma, which establishes the relationship between the parity check matrix H of a linear unequal error protection (UEP) code[3] C and the minimum distance, is taken from [2].

Lemma 4: If H is the parity check matrix of a linear UEP code C, then the minimum distance of codewords which differ in the i-th digit of the code is greater than or equal to $2t_i+1$ for all i $(1\leq i\leq n)$ if and only if every set of $2t_i$ columns of H which include the i-th column is linearly independent for all i $(1\leq i\leq n)$. □

Now, from the viewpoint of coding theory, I_A in Equation (10) is considered to be the set of error vectors that can be corrected. Defining I_A means that the error vectors are specified individually. Since specifying the error vectors in such detail is not realistic in coding theory, the relation between the parity check matrix of a linear code and the distances between any distinct error vectors has not been clarified up to now. However, in experimental design, machine learning and similar problems, it is important to specify the vectors individually.

Now, we give our second main theorem which generalizes Lemma 3 and Lemma 4.

Theorem 2: If H is the parity check matrix of a linear code C, then $\boldsymbol{e}-\boldsymbol{e}'\notin C$ for all $\boldsymbol{e},\boldsymbol{e}'\in I_A(\boldsymbol{e}\neq\boldsymbol{e}')$, if and only if every set $\{\boldsymbol{h}_{\cdot j}|j\in v(\boldsymbol{e}-\boldsymbol{e}')\}$ is linearly independent for all $\boldsymbol{e},\boldsymbol{e}'\in I_A(\boldsymbol{e}\neq\boldsymbol{e}')$.

Proof: $(\leftarrow)$ Let $\{\boldsymbol{h}_{\cdot j}|j\in v(\boldsymbol{e}-\boldsymbol{e}')\}$ be linearly independent for all $\boldsymbol{e},\boldsymbol{e}'\in I_A(\boldsymbol{e}\neq\boldsymbol{e}')$ and suppose $\boldsymbol{e}-\boldsymbol{e}'\in C$. From the supposition $H(\boldsymbol{e}-\boldsymbol{e}')^T=\boldsymbol{0}$ must hold. This is a contradiction, since the set $\{\boldsymbol{h}_{\cdot j}|j\in v(\boldsymbol{e}-\boldsymbol{e}')\}$ is linearly independent. Therefore, $\boldsymbol{e}-\boldsymbol{e}'\notin C$.

$(\rightarrow)$ Let $\boldsymbol{e}-\boldsymbol{e}'\notin C$ for all $\boldsymbol{e},\boldsymbol{e}'\in I_A(\boldsymbol{e}\neq\boldsymbol{e}')$ and suppose the set $\{\boldsymbol{h}_{\cdot j}|j\in v(\boldsymbol{e}-\boldsymbol{e}')\}$ is not linearly independent for some $\boldsymbol{e},\boldsymbol{e}'\in I_A(\boldsymbol{e}\neq\boldsymbol{e}')$. From the supposition and the monotonicity of A, there are vectors $\boldsymbol{d}$ and $\boldsymbol{d}'$ $(\boldsymbol{d}\sqsubseteq\boldsymbol{e},\boldsymbol{d}'\sqsubseteq\boldsymbol{e}',\boldsymbol{d}\neq\boldsymbol{d}')$ satisfying $H(\boldsymbol{d}-\boldsymbol{d}')^T=\boldsymbol{0}$ and $\boldsymbol{d},\boldsymbol{d}'\in I_A$.

Now from $H(\boldsymbol{d}-\boldsymbol{d}')^T=\boldsymbol{0}$, we have $\boldsymbol{d}-\boldsymbol{d}'\in C$. This is a contradiction, since $\boldsymbol{e}-\boldsymbol{e}'\notin C$ for all $\boldsymbol{e},\boldsymbol{e}'\in I_A(\boldsymbol{e}\neq\boldsymbol{e}')$. Therefore, every set $\{\boldsymbol{h}_{\cdot j}|j\in v(\boldsymbol{e}-\boldsymbol{e}')\}$ is linearly independent. □

Corollary 1: Lemma 3 is a special case of Theorem 2.

Proof: In Theorem 2, we consider the case $A=\{\boldsymbol{a}|w(\boldsymbol{a})\leq$

[3] UEP codes are codes in which some information digits are protected against a greater number of errors than other information digits[6].

$t, \boldsymbol{a} \in \{0,1\}^n\}$. Then,

$$\begin{aligned} &\{\boldsymbol{e}-\boldsymbol{e}'|\boldsymbol{e},\boldsymbol{e}' \in I_A(\boldsymbol{e} \neq \boldsymbol{e}')\} \\ &\quad = \{\boldsymbol{a}|w(\boldsymbol{a}) \leq 2t, \boldsymbol{a} \in GF(q)^n\} \end{aligned} \tag{33}$$

holds. From Equation (33) and the fact that $\boldsymbol{e}-\boldsymbol{e}' \notin C$ for all $\boldsymbol{e},\boldsymbol{e}' \in I_A(\boldsymbol{e} \neq \boldsymbol{e}')$, the minimum distance of C is greater than or equal to $2t+1$. Using Equation (33) and the fact that every set $\{\boldsymbol{h}_{\cdot j}|j \in v(\boldsymbol{e}-\boldsymbol{e}')\}$ is linearly independent for all $\boldsymbol{e},\boldsymbol{e}' \in I_A(\boldsymbol{e} \neq \boldsymbol{e}')$, we also have every set of $2t$ columns of H is linearly independent. Hence, Corollary 1 is obtained. □

Corollary 2: Lemma 4 is a special case of Theorem 2.

Proof: In Theorem 2, we consider the case that

$$\begin{aligned} &\{\boldsymbol{e}-\boldsymbol{e}'|\boldsymbol{e},\boldsymbol{e}' \in I_A(\boldsymbol{e} \neq \boldsymbol{e}')\} \\ &\quad = \bigcup_{i=1}^{n} \{\boldsymbol{a}|a_i \neq 0, w(\boldsymbol{a}) \leq 2t_i, \boldsymbol{a} \in GF(q)^n\}. \end{aligned} \tag{34}$$

Then, from Equation (34) and the fact that $\boldsymbol{e}-\boldsymbol{e}' \notin C$ for all $\boldsymbol{e},\boldsymbol{e}' \in I_A(\boldsymbol{e} \neq \boldsymbol{e}')$, the minimum distance between codewords which differ in the i-th digit of the code is greater than or equal to $2t_i+1$ for all i $(1 \leq i \leq n)$. Using Equation (34) and the fact that every set $\{\boldsymbol{h}_{\cdot j}|j \in v(\boldsymbol{e}-\boldsymbol{e}')\}$ is linearly independent for all $\boldsymbol{e},\boldsymbol{e}' \in I_A(\boldsymbol{e} \neq \boldsymbol{e}')$, we also have every set of $2t_i$ columns of H including the i-th column is linearly independent for all i $(1 \leq i \leq n)$. Hence, Corollary 2 is obtained. □

Next, we consider the meaning of Theorem 2 from the viewpoint of coding theory.

If, for any two distinct codewords $\boldsymbol{c}',\boldsymbol{c}'' \in C(\boldsymbol{c}' \neq \boldsymbol{c}'')$ and any two error vectors $\boldsymbol{e}',\boldsymbol{e}'' \in I_A$,

$$\boldsymbol{c}'+\boldsymbol{e}' \neq \boldsymbol{c}''+\boldsymbol{e}'' \tag{35}$$

holds, then any error in I_A can be corrected.

Now, if $\boldsymbol{c}'$ and $\boldsymbol{c}''$ belong to a linear code C, then $\boldsymbol{c}''-\boldsymbol{c}'$ is also a codeword. That is, $\boldsymbol{c}''-\boldsymbol{c}' \in C$. Hence Equation (35) is equivalent to

$$\boldsymbol{e}'-\boldsymbol{e}'' \notin C \tag{36}$$

for any two distinct error vectors $\boldsymbol{e}',\boldsymbol{e}'' \in I_A$.

VI. Relation between the Sampling Theorem for Functions over a $GF(q)^n$ Domain and Linear Codes

Combining Theorem 1 and Theorem 2, we obtain the following corollary.

Corollary 3: Suppose a set A is monotonic and $f(\boldsymbol{x})$ is expressed as

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{a} \in I_A} f_{\boldsymbol{a}} \mathcal{X}_{\boldsymbol{a}}(\boldsymbol{x}), \tag{37}$$

then the Fourier coefficients can be computed by

$$f_{\boldsymbol{a}} = \frac{1}{|C^{\perp}|} \sum_{\boldsymbol{x} \in C^{\perp}} f(\boldsymbol{x}) \mathcal{X}^*_{\boldsymbol{a}}(\boldsymbol{x}), \tag{38}$$

where $C^{\perp}$ is the dual code of a linear code C satisfying $\boldsymbol{e}-\boldsymbol{e}' \notin C$ for all $\boldsymbol{e},\boldsymbol{e}' \in I_A(\boldsymbol{e} \neq \boldsymbol{e}')$. □

Let us consider the meaning of Corollary 3. The following description is based on the method of proof used in [12].

First, the following equation holds.

$$\frac{1}{q} \sum_{l \in GF(q)} \mathcal{X}_{l\boldsymbol{a}}(\boldsymbol{x}) = \begin{cases} 1, & \boldsymbol{a}\boldsymbol{x}^T = 0, \\ 0, & \boldsymbol{a}\boldsymbol{x}^T \neq 0, \end{cases} \tag{39}$$

where the scalar multiple $l\boldsymbol{a} = (la_1, la_2, \ldots, la_n)$, and la_i is evaluated over $GF(q)$.

Next, we define $f_G(\boldsymbol{x})$ by

$$f_G(\boldsymbol{x}) = f(\boldsymbol{x}) \prod_{i=1}^{k} \left(\frac{1}{q} \sum_{l \in GF(q)} \mathcal{X}_{l\boldsymbol{g}_{i\cdot}}(\boldsymbol{x}) \right), \tag{40}$$

where $\boldsymbol{g}_{i\cdot}$ is the i-th row of the $k \times n$ matrix G defined in Equation (28).

From Equations (13) and (29), we have

$$f_G(\boldsymbol{x}) = \begin{cases} f(\boldsymbol{x}), & \boldsymbol{x} \in C^{\perp}, \\ 0, & \boldsymbol{x} \in GF(q)^n \setminus C^{\perp}. \end{cases} \tag{41}$$

Hence $f_G(\boldsymbol{x})$ can be determined by the collection of values that it takes on $C^{\perp}$.

Lemma 5: The equality

$$f_G(\boldsymbol{x}) = \frac{1}{q^k} \sum_{\boldsymbol{c} \in C} f(\boldsymbol{x}) \mathcal{X}_{\boldsymbol{c}}(\boldsymbol{x}). \tag{42}$$

holds.

Proof: From Equation (27), we see that the right-hand side of Equation (40) equals

$$\begin{aligned} &\frac{1}{q^k} f(\boldsymbol{x}) \prod_{i=1}^{k} \left(\sum_{l \in GF(q)} \mathcal{X}_{l\boldsymbol{g}_{i\cdot}}(\boldsymbol{x}) \right) \\ &\quad = \frac{1}{q^k} f(\boldsymbol{x}) \left(\sum_{\boldsymbol{c} \in C} \mathcal{X}_{\boldsymbol{c}}(\boldsymbol{x}) \right) \\ &\quad = \frac{1}{q^k} \sum_{\boldsymbol{c} \in C} f(\boldsymbol{x}) \mathcal{X}_{\boldsymbol{c}}(\boldsymbol{x}). \end{aligned} \tag{43}$$

□

Now, I_A is the bounded set of the original function $f(\boldsymbol{x})$. Let $I_{\boldsymbol{c}}$ be the bounded set of $f(\boldsymbol{x})\mathcal{X}_{\boldsymbol{c}}(\boldsymbol{x})$. Using the fact that $f(\boldsymbol{x})\mathcal{X}_{\boldsymbol{c}}(\boldsymbol{x})$ is a function which only causes a shift $\boldsymbol{c}$ of $f(\boldsymbol{x})$ in the frequency domain,

$$I_{\boldsymbol{c}} = \{\boldsymbol{a}-\boldsymbol{c}|\boldsymbol{a} \in I_A\} \tag{44}$$

holds.

It is clear that if $I_A \cap I_{\boldsymbol{c}} = \emptyset$ (the empty set) for all $\boldsymbol{c} \in C$ then the original function can be reconstructed from only $\{(\boldsymbol{x}, f(\boldsymbol{x}))|\boldsymbol{x} \in C^{\perp}\}$. Now, $\boldsymbol{e}-\boldsymbol{e}' \notin C$ for all $\boldsymbol{e},\boldsymbol{e}' \in I_A(\boldsymbol{e} \neq \boldsymbol{e}')$ in Corollary 3 is equivalent to $I_A \cap I_{\boldsymbol{c}} = \emptyset$ for all $\boldsymbol{c} \in C$. Hence, Corollary 3 states that the original function can be reconstructed by using $I_A \cap I_{\boldsymbol{c}} = \emptyset$ for all $\boldsymbol{c} \in C$ in the frequency domain.

VII. Conclusion

In this paper, we have generalized the sampling theorem for bandlimited functions over the Boolean domain to a sampling theorem for bandlimited functions over a $GF(q)^n$ domain. We have also provided a theorem for the relation between the parity check matrix of a linear code and any distinct error vectors. Lastly, we have clarified the relation between the sampling theorem for functions over a $GF(q)^n$ domain and linear codes.

Acknowledgment

This research was partially supported by Grant-in-Aid for Scientific Research on Innovative Areas of Japan Society for the Promotion of Science (No:20200044), Waseda University Grant for Special Research Project No:2009A-058 and the Academic Committee of Yokohama College of Commerce. The research leading to this paper was partially supported by Waseda University Grant for Special Research Project No: 2008B-198.

References

[1] D. Angluin, “Queries and concept learning,” Machine Learning, vol.2, no.4, pp.319–342, April 1988.

[2] I.M. Boyarinov and G.L. Katsman, “Linear Unequal Error Protection Codes,” IEEE Trans. Inf. Theory, vol.IT-27, no.2, pp.168–175, 1981.

[3] A.S. Hedayat, N.J.A. Sloane and J. Stufken, Orthogonal Arrays: Theory and Applications, Springer, New York, 1999.

[4] S. Hirasawa and T. Nishijima, Introduction to coding theory (in Japanese), Baifukan, 1999.

[5] F.J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes, North-Holland, 1977.

[6] B. Masnick and J. Wolf, “On Linear Unequal Error Protection Codes,” IEEE Trans. Inf. Theory, vol.IT-13, no.4, pp.600–607, 1967.

[7] A.V. Oppenheim and R.W. Schafer, Digital Signal Processing, Prentice-Hall, 1975.

[8] R.S. Stankovic and J. Astola, “Reading the Sampling Theorem in Multiple-Valued Logic: A journey from the (Shannon) sampling theorem to the Shannon decomposition rule,” Proc. 37th Int. Symp. on Multiple-Valued Logic, Oslo, Norway, May 14-15, 2007.

[9] T. Saito, T. Matsushima and S. Hirasawa, “A Note on Construction of Orthogonal Arrays with Unequal Strength from Error-Correcting Codes, ” IEICE Trans. Fundamentals, Vol.E89-A, pp.1307–1315, May 2006.

[10] E.M. Stein, R. Shakarchi, Fourier Analysis: An Introduction (Princeton Lectures in Analysis, Volume 1), Princeton University Press, 2003.

[11] I. Takahashi, Combinatorial Theory and its Application (in Japanese), Iwanami Syoten, 1979.

[12] E. Takimoto and A. Maruoka, “A Sampling Theorem for Functions over the Boolean Domain” (in Japanese), Technical Report of IEICE, vol.COMP97–56, 1997.

[13] Y. Ukita, T. Matsushima and S. Hirasawa, “A Note on Learning Boolean Functions Using Orthogonal Designs” (in Japanese), IEICE Trans. Fundamentals, Vol.J86-A, no.4, pp.482–490, Apr. 2003.