Hiroshima Math. J.
45 (2015), 341–364

WAFOM over abelian groups for quasi-Monte Carlo point sets

Kosuke Suzuki

(Received January 20, 2015)

Abstract. In this paper, we study quasi-Monte Carlo (QMC) rules for numerical integration. J. Dick proved a Koksma-Hlawka type inequality for α-smooth integrands and gave an explicit construction of QMC rules achieving the optimal rate of convergence in that function class. From this inequality, Matsumoto, Saito and Matoba introduced the Walsh figure of merit (WAFOM) $\mathrm{WF}(P)$ for an $\mathbf{F}_2$-digital net P as a quickly computable quality criterion for P as a QMC point set. The key ingredient for obtaining WAFOM is the Dick weight, a generalization of the Hamming weight and the Niederreiter-Rosenbloom-Tsfasman (NRT) weight.

We extend the notions of the Dick weight and WAFOM over a general finite abelian group G, and show that this version of WAFOM satisfies Koksma-Hlawka type inequality when G is cyclic. We give a MacWilliams-type identity on weight enumerator polynomials for the Dick weight, by which we can compute the minimum Dick weight as well as WAFOM. We give a lower bound on WAFOM of order $N^{-C_G'(\log N)/s}$ and an upper bound on lowest WAFOM of order $N^{-C_G(\log N)/s}$ for given (G, N, s) if $(\log N)/s$ is sufficiently large, where C_G' and C_G are constants depending only on the cardinality of G and N is the cardinality of quadrature rules in $[0,1)^s$. These bounds generalize the bounds given by Yoshiki and others given for $G = \mathbf{F}_2$.

1. Introduction

Quasi-Monte Carlo (QMC) integration is a method for numerical integration using the average of function evaluations as an approximation of the true integration value. In QMC integration, sample points are chosen deterministically, while in Monte-Carlo integration they are chosen randomly. Thus, how to construct point sets has been a major concern in QMC theory. One of the known good construction frameworks is digital nets, which is based on linear algebra over finite fields (or more generally over finite rings).

A strong analogy between coding theory and QMC point sets is well known (see, e.g., [2, 13, 17]). In coding theory, the minimum Hamming weight is used for a criterion for linear codes. Analogically, Niederreiter-

The work of the first author was supported by the Program for Leading Graduate Schools, MEXT, Japan.

2010 *Mathematics Subject Classification*. Primary 11K45, 65D30, 11K38.

Key words and phrases. numerical integration, Quasi-Monte Carlo, WAFOM, Dick weight, digital net, MacWilliams-type identity.

Rosenbloom-Tsfasman (NRT) weight is a criterion for digital nets in QMC theory [12, 15]. More precisely, the minimum NRT weight is essentially equivalent to t-value and gives an upper bound on the star-discrepancy, which are important criteria for QMC point sets. Recently, based on Dick's work [3], Matsumoto, Saito and Matoba defined the Dick weight μ on digital nets over $\mathbf{F}_2$ and related it to a criterion called the Walsh figure of merit (WAFOM) in [10]. In this paper, as a generalization of [10], we extend the notions of the Dick weight and WAFOM for digital nets over $\mathbf{Z}_b$, and more generally, for subgroups of $G^{s\times n}$ where G is a finite abelian group. Furthermore, we establish a MacWilliams-type identity for the Dick weight, which gives a computable formula of the minimum Dick weight and WAFOM.

Let us recall the notion of QMC integration. For an integrable function $f : [0,1)^s \to \mathbf{R}$ and a finite point set in an s-dimensional unit cube $\mathscr{P} \subset [0,1)^s$, quasi Monte-Carlo (QMC) integration of f by $\mathscr{P}$ is an approximation value

$$I_{\mathscr{P}}(f) := \frac{1}{N}\sum_{\boldsymbol{x}\in\mathscr{P}} f(\boldsymbol{x})$$

of the actual integration

$$I(f) := \int_{[0,1)^s} f(\boldsymbol{x})d\boldsymbol{x},$$

where $N := |\mathscr{P}|$ is the cardinality of $\mathscr{P}$. The QMC integration error is defined as $\mathrm{Err}(f;\mathscr{P}) := |I_{\mathscr{P}}(f) - I(f)|$. If the integrand f has bounded variation in the sense of Hardy and Krause, the Koksma-Hlawka inequality shows that $\mathrm{Err}(f;\mathscr{P}) \le V(f)D(\mathscr{P})$, where $V(f)$ is the total variation of f and $D(\mathscr{P})$ is the star-discrepancy of $\mathscr{P}$. There have been many studies on the construction of low-discrepancy point sets, i.e., point sets with $D(\mathscr{P}) \in O(N^{-1+\varepsilon})$. In particular, digital nets and sequences are a general framework for the construction of good point sets. We refer to [6] and [13] for the general information on QMC integration and digital nets and sequences.

Recently, higher order convergence results for digital nets, i.e., $\mathrm{Err}(f;\mathscr{P})$ converges faster than N^{-1}, has been established. For a given integer $\alpha > 1$, Dick gave quadrature rules for α-smooth integrands which achieve $\mathrm{Err}(f;\mathscr{P}) \in O(N^{-\alpha+\varepsilon})$ [3]. He introduced a weight which gives a bound on a criterion $\mathrm{WF}_\alpha(\mathscr{P})$ (he did not give a name and we use the name in [10]) for a digital net $\mathscr{P}$ over a finite field with cardinality b, and proved a Koksma-Hlawka type inequality $\mathrm{Err}(f;\mathscr{P}) \le C_{b,s,\alpha}\|f\|_\alpha \cdot \mathrm{WF}_\alpha(\mathscr{P})$, where $\|f\|_\alpha$ is a norm of f for a Sobolev space and $C_{b,s,\alpha}$ is a constant depend only on b, s, and α. Later he improved the constant factor of the lowest WF_α for digital nets over a finite cyclic group [4].

As a discretized version of Dick's method, Matsumoto, Saito and Matoba introduced the Dick weight μ and a related criterion WAFOM $\mathrm{WF}(P)$ for an $\mathbf{F}_2$-digital net P [10]. WAFOM also satisfies a Koksma-Hlawka type inequality (with some errors due to discretization). One remarkable merit of WAFOM is that WAFOM is easily computable by the inversion formula [10, (4.2)], which is easier to implement than the formula of WF_α derived from [1, Section 4]. Using this merit, they executed a random search of low-WAFOM point sets and showed that such point sets perform better than some standard low-discrepancy point sets. There are several studies on low-WAFOM point sets. The existence of low-WAFOM point sets was shown by Matsumoto and Yoshiki [11]. The author proved that the interlacing construction for higher order QMC point sets with Niederreiter-Xing sequences over a finite field gives low-WAFOM point sets [18].

In this paper, as a generalization of [10] we propose the Dick weight and WAFOM for digital nets over $\mathbf{Z}_b$ and for subgroups of $G^{s\times n}$ where G is a finite abelian group. WAFOM over $\mathbf{Z}_b$ is also a discretized version of Dick's method and thus satisfies a Koksma-Hlawka type inequality. Moreover, we give a MacWilliams-type identity of weight enumerator polynomials for the Dick weight. Using this identity we obtain a computable formula of the minimum Dick weight as well as WAFOM, which is a generalization of the inversion formula for WAFOM in the dyadic case. Furthermore, we give generalizations of known properties of WAFOM over $\mathbf{F}_2$ in [11] and [19]. More precisely, we give a lower bound on WAFOM and prove the existence of low-WAFOM point sets. In particular, we improve some of the results in [11]. These results imply that there exist positive constants C, D, D' and F depending only on b and independent of s, n and N such that $N^{-C\log N/s} \le \min\{\mathrm{WF}(P) \mid P \text{ is a digital net}, |P| \le N\} \le FN^{-D(\log N)/s+D'}$, if $(\log N)/s$ is sufficiently large.

These results are similar to the works of Dick, but there is no implication between them. Dick fixed the smoothness α, while our method requires n-smoothness on the function where n is as above. Thus, in our case, the function class is getting smaller for n being increased.

The rest of the paper is organized as follows. In Section 2, we introduce the necessary background and notation, such as the discretization scheme of QMC integration, the discrete Fourier transform, and Walsh functions. In Section 3, we define the Dick weight and WAFOM over a general finite abelian group G, and prove a Koksma-Hlawka type inequality in the case that G is cyclic. In Section 4, we define the weight enumerator polynomial, give the MacWilliams-type identity for the Dick weight, and give a computable formula of WAFOM. In Section 5, we give a lower bound on WAFOM, prove the existence of low-WAFOM point sets, and study the order of WAFOM.

2. Preliminaries

Throughout this paper, we use the following notation. Let $\mathbf{N}$ be the set of positive integers and $\mathbf{N}_0 := \mathbf{N} \cup \{0\}$. Let b be an integer greater than 1. Let $\mathbf{Z}_b = \mathbf{Z}/b\mathbf{Z}$ be the residue class ring modulo b. We identify $\mathbf{Z}_b$ with the set $\{0, 1, \dots, b-1\} \subset \mathbf{Z}$. For a set S, we denote by $|S|$ the cardinality of S. For a group or a ring R and positive integers s and n, we denote by $R^{s\times n}$ the set of $s \times n$ matrices with components in R. We denote by O the zero matrix. We denote by e the base of the natural logarithm.

2.1. Discretized QMC in base b. In this subsection, we explain discretized QMC in base b. This discretization is a straightforward generalization of the $b = 2$ case in [10].

Let s be a positive integer. Let $\mathscr{P} \subset [0,1)^s$ be a point set in an s-dimensional unit cube with finite cardinality $|\mathscr{P}| = N$, and let $f : [0,1)^s \to \mathbf{R}$ be an integrable function. Recall that quasi-Monte Carlo integration by $\mathscr{P}$ is an approximation value

$$I_{\mathscr{P}}(f) := \frac{1}{N}\sum_{\boldsymbol{x}\in\mathscr{P}} f(\boldsymbol{x})$$

of the actual integration

$$I(f) := \int_{[0,1)^s} f(\boldsymbol{x})d\boldsymbol{x}.$$

The QMC integration error is $\mathrm{Err}(f;\mathscr{P}) := |I_{\mathscr{P}}(f) - I(f)|$.

Here, we fix a positive integer n, which is called the degree of discretization or the precision. We consider an n-digit discrete approximation in base b. We associate a matrix $B := (b_{i,j}) \in \mathbf{Z}_b^{s\times n}$ with a point $\boldsymbol{x}_B = (x_B^1, \dots, x_B^s) = (\sum_{j=1}^n b_{1,j}b^{-j}, \dots, \sum_{j=1}^n b_{s,j}b^{-j}) \in [0,1)^s$, and with an s-dimensional cube $\mathbf{I}_B := \prod_{i=1}^s I_i \subset [0,1)^s$, where each edge $I_i := [x_B^i, x_B^i + b^{-n})$ is a half-open interval with length b^{-n}. We define n-digit discrete approximation f_n of f as

$$f_n : \mathbf{Z}_b^{s\times n} \to \mathbf{R}, \qquad B := (b_{i,j}) \mapsto \frac{1}{\mathrm{Vol}(\mathbf{I}_B)}\int_{\mathbf{I}_B} f(\boldsymbol{x})d\boldsymbol{x}.$$

Let P be a subset of $\mathbf{Z}_b^{s\times n}$. We define n-th discretized QMC integration of f by P as

$$I_{P,n}(f) := \frac{1}{|P|}\sum_{B\in P} f_n(B)$$

and define the n-th discretized QMC integration error as

$$\mathrm{Err}(f;P,n) := |I_{P,n}(f) - I(f)|.$$

For each $B \in P$, we take the center point of the cube I_B. Let $\mathscr{P} \subset [0,1)^s$ be the set of such center points given by P. By a slight extension of [10, Lemma 2.1], if f is continuous with Lipschitz constant K then we have $|I_{P,n}(f) - I_{\mathscr{P}}(f)| \le K\sqrt{s}b^{-n}$. We take n large enough so that $K\sqrt{s}b^{-n}$ is negligibly small compared to the order of QMC integration error $|I_{\mathscr{P}}(f) - I(f)|$ by $\mathscr{P}$. Then we may regard the n-th discretized QMC integration error $\mathrm{Err}(f;P,n)$ as an approximation of the QMC integration error $\mathrm{Err}(f;P)$.

As point sets, in this paper we consider subgroups of $\mathbf{Z}_b^{s\times n}$ as well as digital nets. The definition of digital nets over finite rings is given in [7], we adopt an equivalent definition of digital nets, which is proposed as digital nets with generating matrices in [5, Definition 4.3].

Definition 1. Let $C_1, \dots, C_s \in \mathbf{Z}_b^{n\times d}$ be matrices and let $X_1, \dots, X_d \in \mathbf{Z}_b^{s\times n}$ be defined by the j-th row of X_i is the transpose of the i-th column of C_j. Assume that $X_1, \dots, X_d$ are a free basis of $\mathbf{Z}_b^{s\times n}$ as a $\mathbf{Z}_b$-module. For an integer k with $0 \le k \le b^d - 1$, we define a matrix $\boldsymbol{x}_k \in \mathbf{Z}_b^{s\times n}$ as $\boldsymbol{x}_k = \sum_{i=1}^d \kappa_{i-1} X_i$, where $k = \kappa_0 + \kappa_1 b^1 + \cdots + \kappa_{d-1} b^{d-1}$ $(0 \le \kappa_i \le b-1)$ is the b-adic expansion of k. We call the set $\{\boldsymbol{x}_0, \dots, \boldsymbol{x}_{b^d-1}\}$ the digital net generated by the matrices $C_1, \dots, C_s$.

It is easy to see that digital nets become subgroups of $\mathbf{Z}_b^{s\times n}$.

2.2. Discrete Fourier transform. In this subsection, we recall the notion of character groups and the discrete Fourier transform. We refer to [16] for general information on character groups. Let G be a finite abelian group. Let $T := \{z \in \mathbf{C} \mid |z| = 1\}$ be the multiplicative group of complex numbers of absolute value one. Let $\omega_b = \exp(2\pi\sqrt{-1}/b)$.

Definition 2. We define the character group of G by $G^\vee := \mathrm{Hom}(G, T)$, namely $G^\vee$ is the set of group homomorphisms from G to T.

There is a natural pairing $\bullet : G^\vee \times G \to T$, $(h,g) \mapsto h \bullet g := h(g)$.

We can see that $\mathbf{Z}_b^\vee$ is isomorphic to $\mathbf{Z}_b$ as an abstract group. Throughout this paper, we identify $\mathbf{Z}_b^\vee$ with $\mathbf{Z}_b$ through a pairing $\bullet : \mathbf{Z}_b \times \mathbf{Z}_b \to T$, $(h,g) \mapsto h \bullet g := \omega_b^{hg}$, where hg is the product in $\mathbf{Z}_b$.

Let R be a commutative ring containing $\mathbf{C}$. Let $f : G \to R$ be a function. We define the discrete Fourier transform of f as below.

Definition 3. The discrete Fourier transform of f is defined by $\hat{f} : G^\vee \to R$, $h \mapsto \frac{1}{|G|}\sum_{g\in G} f(g)(h \bullet g)$. Each value $\hat{f}(h)$ is called a discrete Fourier coefficient.

We assume that $P \subset G$ is a subgroup. We define $P^{\perp} := \{h \in G^{\vee} \mid h \bullet g = 1$ for all $g \in P\}$. Since $P^{\perp}$ is the kernel of the restriction map $G^{\vee} \to P^{\vee}$, we have $|P^{\perp}| = |G|/|P|$. We recall the orthogonality of characters.

LEMMA 1. *Suppose that $P \subset G$ is a subgroup and $g \in G$. Then we have*

$$\sum_{h \in P^{\perp}} h \bullet g = \begin{cases} |P^{\perp}| & \text{if } g \in P, \\ 0 & \text{if } g \notin P. \end{cases}$$

This lemma implies the Poisson summation formula and the Fourier inversion formula.

THEOREM 1 (Poisson summation formula).

$$\frac{1}{|P|}\sum_{g \in P} f(g) = \sum_{h \in P^{\perp}} \hat{f}(h).$$

PROOF.

$$\begin{aligned}
\sum_{h \in P^{\perp}} \hat{f}(h) &= \sum_{h \in P^{\perp}} \frac{1}{|G|}\sum_{g \in G} f(g)(h \bullet g) \\
&= \sum_{g \in G} \frac{1}{|G|} f(g) \sum_{h \in P^{\perp}} h \bullet g \\
&= \frac{1}{|G|}\sum_{g \in P} f(g) \cdot |P^{\perp}| \quad (\because \text{ Lemma } 1) \\
&= \frac{1}{|P|}\sum_{g \in P} f(g).
\end{aligned}$$

□

THEOREM 2 (Fourier inversion formula). *For a complex-valued function $f : G \to \mathbf{C}$, we have $f(g) = \sum_{h \in G^{\vee}} \hat{f}(-h)(h \bullet g)$ for any $g \in G$. Moreover, if f is real-valued, we have $f(g) = \sum_{h \in G^{\vee}} \overline{\hat{f}(h)(h \bullet g)}$.*

PROOF. By Lemma 1, we have $\sum_{h \in G^{\vee}} h \bullet g = 0$ if $g \neq 0$ and $\sum_{h \in G^{\vee}} h \bullet g = |G|$ if $g = 0$. Thus we have

$$\begin{aligned}
\sum_{h \in G^{\vee}} \hat{f}(-h)(h \bullet g) &= \sum_{h \in G^{\vee}} \frac{1}{|G|} \sum_{g' \in G} f(g')((-h) \bullet g')(h \bullet g) \\
&= \frac{1}{|G|} \sum_{g' \in G} f(g') \sum_{h \in G^{\vee}} (h \bullet (g - g')) \\
&= f(g),
\end{aligned}$$

which proves the complex-valued case. If f is real-valued, we have $\hat{f}(-h) = \overline{\hat{f}(h)}$, and thus the complex-valued case implies the real-valued case. □

2.3. Walsh functions. In this subsection, we recall the notion of Walsh functions and Walsh coefficients, and see the relationship between Walsh coefficients and discrete Fourier coefficients. As a corollary, we prove that the n-digit discrete approximation f_n of f is essentially equal to the appropriate approximation of the Walsh series of f. We refer to [6, Appendix A] for general information on Walsh functions.

First, we define Walsh functions for the one dimensional case.

Definition 4. Let $k \in \mathbf{N}_0$ with b-adic expansion $k = \kappa_0 + \kappa_1 b^1 + \kappa_2 b^2 + \cdots$ (this expansion is actually finite), where $\kappa_j \in \{0, 1, \dots, b-1\}$ for all $j \in \mathbf{N}_0$. The k-th b-adic Walsh function ${}_b\mathrm{wal}_k : [0,1) \to \{0, \omega_b, \dots, \omega_b^{b-1}\}$ is defined as

$${}_b\mathrm{wal}_k(x) := \omega_b^{\kappa_0 x_1 + \kappa_1 x_2 + \cdots},$$

for $x \in [0,1)$ with b-adic expansion $x = x_1 b^{-1} + x_2 b^{-2} + x_3 b^{-3} + \cdots$ with $x_j \in \{0, 1, \dots, b-1\}$, which is unique in the sense that infinitely many of the x_j must be different from $b-1$.

This definition is generalized to the higher-dimensional case.

Definition 5. For dimension $s \geq 1$, let $\boldsymbol{k} = (k_1, \dots, k_s) \in \mathbf{N}_0^s$. The $\boldsymbol{k}$-th b-adic Walsh function ${}_b\mathrm{wal}_{\boldsymbol{k}} : [0,1)^s \to \{0, \omega_b, \dots, \omega_b^{b-1}\}$ is defined as

$${}_b\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}) = \prod_{i=1}^{s} {}_b\mathrm{wal}_{k_i}(x_i).$$

for $\boldsymbol{x} = (x_1, \dots, x_s) \in [0,1)^s$.

Walsh coefficients are defined as follows.

Definition 6. Let $f : [0,1)^s \to \mathbf{R}$. The $\boldsymbol{k}$-th b-adic Walsh coefficient of f is defined as

$$\mathscr{F}(f)(\boldsymbol{k}) := \int_{[0,1)^s} f(\boldsymbol{x}) \overline{{}_b\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x})} d\boldsymbol{x}.$$

We see the relationship between Walsh coefficients and discrete Fourier coefficients in the following. Let $A = (a_{i,j}) \in \mathbf{Z}_b^{s \times n}$. We define maps $\phi_i : \mathbf{Z}_b^{s \times n} \to \mathbf{N}_0$ as $\phi_i(A) = \sum_{j=1}^{n} a_{i,j} b^{j-1}$ and $\phi : \mathbf{Z}_b^{s \times n} \to \mathbf{N}_0^s$ as $\phi(A) = (\phi_1(A), \dots, \phi_s(A))$. Note that $\phi_i(A) < b^n$ holds for all $1 \leq i \leq s$ and $A \in \mathbf{Z}_b^{s \times n}$.

Lemma 2. *Let $f : [0,1)^s \to \mathbf{R}$ and $A = (a_{i,j}) \in \mathbf{Z}_b^{s \times n}$. Then we have*

$$\overline{\mathscr{F}(f)(\phi(A))} = \widehat{f_n}(A).$$

PROOF. Since $\phi_i(A) < b^n$ holds for all $1 \leq i \leq s$, for all $\boldsymbol{x} = (x_1, \dots, x_s) \in \mathbf{I}_B$ we have

$$ {}_b\mathrm{wal}_{\phi(A)}(\boldsymbol{x}) = \prod_{i=1}^{s} {}_b\mathrm{wal}_{\phi_i(A)}(x_i) = \prod_{i=1}^{s} \omega_b^{a_{i,1}b_{i,1}+\cdots+a_{i,n}b_{i,n}} = B \bullet A. $$

Therefore we have

$$ \begin{aligned} \overline{\mathscr{F}(f)(\phi(A))} &= \int_{[0,1)^s} f(\boldsymbol{x})\ {}_b\mathrm{wal}_{\phi(A)}(\boldsymbol{x}) d\boldsymbol{x} \\ &= \sum_{B \in \mathbf{Z}_b^{s\times n}} \int_{\mathbf{I}_B} f(\boldsymbol{x})\ {}_b\mathrm{wal}_{\phi(A)}(\boldsymbol{x}) d\boldsymbol{x} \\ &= \sum_{B \in \mathbf{Z}_b^{s\times n}} \int_{\mathbf{I}_B} f(\boldsymbol{x})(B \bullet A) d\boldsymbol{x} \\ &= \sum_{B \in \mathbf{Z}_b^{s\times n}} (B \bullet A) \int_{\mathbf{I}_B} f(\boldsymbol{x}) d\boldsymbol{x} \\ &= \sum_{B \in \mathbf{Z}_b^{s\times n}} (B \bullet A) \cdot \mathrm{Vol}(\mathbf{I}_B) f_n(B) \\ &= \sum_{B \in \mathbf{Z}_b^{s\times n}} (B \bullet A) \cdot b^{-sn} f_n(B) = \widehat{f_n}(A), \end{aligned} $$

which proves the lemma. □

Let $f \sim \sum_{\boldsymbol{k} \in \mathbf{N}_0^s} \mathscr{F}(f)(\boldsymbol{k})\ {}_b\mathrm{wal}_{\boldsymbol{k}}$ be the Walsh expansion of a real valued function $f : [0,1)^s \to \mathbf{R}$. Lemma 2 implies that considering n-digit discrete approximation f_n of f is the same as considering the Walsh polynomial $\sum_{\boldsymbol{k} < b^n} \mathscr{F}(f)(\boldsymbol{k}) \cdot {}_b\mathrm{wal}_{\boldsymbol{k}}$, where $\boldsymbol{k} = (k_1, \dots, k_s) < b^n$ means that $k_i < b^n$ holds for every $i = 1, \dots, s$, namely we have the following.

PROPOSITION 1. *Let* $f : [0,1)^s \to \mathbf{R}$. *For* $B \in \mathbf{Z}_b^{s\times n}$, *we have* $f_n(B) = \sum_{\boldsymbol{k} < b^n} \mathscr{F}(f)(\boldsymbol{k})\ {}_b\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_B)$.

PROOF.

$$ \begin{aligned} f_n(B) &= \sum_{A \in \mathbf{Z}_b^{s\times n}} \overline{\widehat{f_n}(A)} B \bullet A \quad (\because \text{ Theorem 2}) \\ &= \sum_{A \in \mathbf{Z}_b^{s\times n}} \mathscr{F}(f)(\phi(A))\ {}_b\mathrm{wal}_{\phi(A)}(\boldsymbol{x}_B) \quad (\because \text{ Lemma 2}) \\ &= \sum_{\boldsymbol{k} < b^n} \mathscr{F}(f)(\boldsymbol{k})\ {}_b\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_B). \end{aligned} $$

□

3. WAFOM over a finite abelian group

In this section, we expand the notion of WAFOM defined in [10], more precisely, we define WAFOM over a finite abelian group with b elements.

First, we evaluate the n-th discretized QMC integration error of f with its discrete Fourier coefficients. Let $P \subset \mathbf{Z}_b^{s\times n}$ be a subgroup. We have $I(f) = \widehat{f_n}(O)$ by the definition of the discrete Fourier inversion, and we have $I_{P,n}(f) = \sum_{A\in P^\perp} \widehat{f_n}(A)$ by the Poisson summation formula (Theorem 1). Hence we have

$$\mathrm{Err}(f; P, n) = |I_{P,n}(f) - I(f)| = \left|\sum_{A\in P^\perp\setminus\{O\}} \widehat{f_n}(A)\right| \le \sum_{A\in P^\perp\setminus\{O\}} |\widehat{f_n}(A)|,$$

and thus we would like to bound the value $|\widehat{f_n}(A)|$. Dick gives an upper bound of the $\boldsymbol{k}$-th b-adic Walsh coefficient $\mathscr{F}(f)(\boldsymbol{k})$ for n-smooth function f (for the definition of n-smoothness, see [3] or [6, §14]).

Theorem 3 ([6], Theorem 14.23). *There is a constant $C_{b,s,n}$ depending only on b, s and n such that for any n-smooth function $f : [0,1)^s \to \mathbf{R}$ and any $\boldsymbol{k} \in \mathbf{N}^s$ it holds that*

$$|\mathscr{F}(f)(\boldsymbol{k})| \le C_{b,s,n}\|f\|_n \cdot b^{-\mu_n(\boldsymbol{k})},$$

where $\|f\|_n$ is a norm of f for a Sobolev space and $\mu_n(\boldsymbol{k})$ is the n-weight of $\boldsymbol{k}$, which are defined in [6, (14.6) and Theorem 14.23] *(we do not define them here).*

Instead of μ_n, we define the Dick weight μ on dual groups of general finite abelian groups below, which is a generalization of the Dick weight over $\mathbf{F}_2$ defined in [10]. Actually, μ is a special case of $\mu_n \circ \phi$. More precisely, if $G = \mathbf{Z}_b$ and $\alpha \ge n$ hold, then we have $\mu = \mu_\alpha \circ \phi$ as a function from $(\mathbf{Z}_b^\vee)^{s\times n} (\simeq \mathbf{Z}_b^{s\times n})$ to $\mathbf{N}_0$.

Definition 7. Let G be a finite abelian group and let $A \in (G^\vee)^{s\times n}$. The Dick weight $\mu : (G^\vee)^{s\times n} \to \mathbf{N}_0$ is defined as

$$\mu(A) := \sum_{i,j} j \times \delta(a_{i,j}),$$

with $\delta(h) = 0$ for $h = 0$ and $\delta(h) = 1$ for $h \ne 0$.

We obtain the next corollary.

Corollary 1. *There exists a constant $C_{b,s,n}$ depending only on b, s and n such that for any n-smooth function $f : [0,1)^s \to \mathbf{R}$ and any $A \in (\mathbf{Z}_b)^{s\times n}$ it holds that*

$$|\hat{f_n}(A)| \le C_{b,s,n}\|f\|_n \cdot b^{-\mu(A)}.$$

PROOF. This is the direct corollary of Theorem 3, Lemma 2, and the equality $\mu(A) = \mu_n \circ \phi(A)$. □

By the above corollary, we have a bound on the n-th discretized QMC integration error

$$\mathrm{Err}(f; P, n) := |I(f) - I_{P,n}(f)| \leq C_{b,s,n} \|f\|_n \times \sum_{A \in P^{\perp} \setminus \{O\}} b^{-\mu(A)},$$

for a subgroup P of $\mathbf{Z}_b^{s \times n}$.

Hence, as a generalization of [10], we define a kind of figure of merit (the Walsh figure of merit or WAFOM).

DEFINITION 8. Let s, n be positive integers. Let G be a finite abelian group with b elements. Let $P \subset G^{s \times n}$ be a subgroup of $G^{s \times n}$. We define the Walsh figure of merit of P by

$$\mathrm{WF}(P) := \sum_{A \in P^{\perp} \setminus \{O\}} b^{-\mu(A)}.$$

In order to stress the role of the precision n, we sometimes denote $\mathrm{WF}^n(P)$ instead of $\mathrm{WF}(P)$.

Then, as we have seen, we have the Koksma-Hlawka type inequality

$$\mathrm{Err}(f; P, n) := |I(f) - I_{P,n}(f)| \leq C_{b,s,n} \|f\|_n \times \mathrm{WF}(P)$$

for a subgroup $P \subset \mathbf{Z}_b^{s \times n}$. This shows that $\mathrm{WF}(P)$ is a quality measure of the point set P for quasi-Monte Carlo integration when $G = \mathbf{Z}_b$.

4. MacWilliams identity over an abelian group

In this section, we assume that s, n are positive integers. Recall that G is a finite abelian group and $G^{\vee}$ its character group. We consider an abelian group $G^{s \times n}$. Let $P \subset G^{s \times n}$ be a subgroup.

We are interested in the weight enumerator polynomial of $P^{\perp}$

$$W_{P^{\perp}}(x, y) := \sum_{A \in P^{\perp}} x^{M - \mu(A)} y^{\mu(A)} \in \mathbf{C}[x, y],$$

where $M := n(n+1)s/2$.

Let $R := \mathbf{C}[x_{i,j}(h)]$, where $x_{i,j}(h)$ is a family of indeterminates for $1 \leq i \leq s$, $1 \leq j \leq n$, and $h \in G^{\vee}$. We define functions $f_{i,j} : G^{\vee} \to R$ as $f_{i,j}(h) = x_{i,j}(h)$ and $f : (G^{s \times n})^{\vee} = (G^{\vee})^{s \times n} \to R$ as

$$f(A) := \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} f_{i,j}(a_{i,j}) = \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq n}} x_{i,j}(a_{i,j}).$$

Now the complete weight enumerator polynomial of $P^{\perp}$, in a standard sense [8, Chapter 5], is defined by

$$GW_{P^{\perp}}(x_{i,j}(h)) := \sum_{A \in P^{\perp}} \prod_{\substack{1 \le i \le s \\ 1 \le j \le n}} x_{i,j}(a_{i,j}),$$

and similarly, the complete weight enumerator polynomial of P is defined by

$$GW_P^*(x_{*i,j}(g)) := \sum_{B \in P} \prod_{\substack{1 \le i \le s \\ 1 \le j \le n}} x_{*i,j}(b_{i,j})$$

in $R^* := \mathbf{C}[x_{*i,j}(g)]$ where $x_{*i,j}(g)$ is a family of indeterminates for $1 \le i \le s$, $1 \le j \le n$, and $g \in G$. We note that if we substitute

$$x_{i,j}(0) \leftarrow x^j, \qquad x_{i,j}(h) \leftarrow y^j \quad \text{for } h \neq 0, \tag{1}$$

we have an identity

$$GW_{P^{\perp}}(x_{i,j}(h))|_{\text{above substitution}} = W_{P^{\perp}}(x, y).$$

A standard formula of the Fourier transform tells that, if $f_1 : G_1 \to R$, $f_2 : G_2 \to R$ are functions and $f_1 f_2 : G_1 \times G_2 \to R$ is their multiplication at the value, then

$$\widehat{f_1 f_2} = \widehat{f_1}\widehat{f_2}$$

holds. This implies that

$$\hat{f}(B) = \prod_{\substack{1 \le i \le s \\ 1 \le j \le n}} \widehat{f_{i,j}}(b_{i,j}) = \frac{1}{|G|^{sn}} \prod_{\substack{1 \le i \le s \\ 1 \le j \le n}} \sum_{h \in G^{\vee}} f_{i,j}(h)(h \bullet b_{i,j}).$$

Hence, by the Poisson summation formula (Theorem 1), we have

$$\begin{aligned} GW_{P^{\perp}}(x_{i,j}(h)) &= \sum_{A \in P^{\perp}} f(A) \\ &= |P^{\perp}| \sum_{B \in P} \hat{f}(B) \\ &= \frac{1}{|P|} \prod_{\substack{1 \le i \le s \\ 1 \le j \le n}} \sum_{h \in G^{\vee}} f_{i,j}(h)(h \bullet b_{i,j}). \end{aligned}$$

Thus we have the MacWilliams identity below, which is a variant of Generalized MacWilliams identity [8, Chapter 5 §6]:

Proposition 2 (MacWilliams identity).

$$GW_{P^\perp}(x_{i,j}(h)) = \frac{1}{|P|} GW_P^* \ \ (\textit{substituted}),$$

where in the right hand side every $x_{*i,j}(g)$ *is substituted by*

$$x_{*i,j}(g) \leftarrow \sum_{h \in G^\vee} (h \bullet g) x_{i,j}(h).$$

We consider specializations of this identity. First, we consider a specialization $\overline{GW}_{P^\perp}(x_1, \dots, x_n, y_1, \dots, y_n)$ of $GW_{P^\perp}(x_{i,j}(h))$ obtained by the substitution

$$x_{i,j}(0) \leftarrow x_j, \qquad x_{i,j}(h) \leftarrow y_j \quad \text{for } h \neq 0.$$

We have

$$\begin{aligned} \sum_{h \in G^\vee} (h \bullet g) x_{i,j}(h) \Big|_{\text{above substitution}} &= (0 \bullet g) x_j + \sum_{h \in G^\vee \setminus \{0\}} (h \bullet g) y_j \\ &= x_j - y_j + \sum_{h \in G^\vee} (h \bullet g) y_j \\ &= x_j - y_j + \begin{cases} b y_j & (\text{if } g = 0) \\ 0 & (\text{otherwise}) \end{cases} \\ &= \begin{cases} x_j + (b-1) y_j & (\text{if } g = 0) \\ x_j - y_j & (\text{otherwise})' \end{cases} \end{aligned}$$

where we use Lemma 1 for the third equality. Thus, we have the following formula.

Corollary 2.

$$\overline{GW}_{P^\perp}(x_1, \dots, x_n, y_1, \dots, y_n) = \frac{1}{|P|} \sum_{B \in P} \prod_{\substack{1 \le i \le s \\ 1 \le j \le n}} (x_j + \eta(b_{i,j}) y_j),$$

where $\eta(b_{i,j}) = b - 1$ *if* $b_{i,j} = 0$ *and* $\eta(b_{i,j}) = -1$ *if* $b_{i,j} \neq 0$.

Second, we consider the specialization (1) of $GW_{P^\perp}$. We have already seen that $GW_{P^\perp}|_{(\text{substitution (1)})} = W_{P^\perp}(x, y)$ holds. Since

$$W_{P^\perp}(x, y) = \overline{GW}_{P^\perp}(x^1, \dots, x^n, y^1, \dots, y^n)$$

follows, Corollary 2 implies the following formula:

Theorem 4.

$$W_{P^{\perp}}(x, y) = \frac{1}{|P|} \sum_{B \in P} \prod_{\substack{1 \le i \le s \\ 1 \le j \le n}} (x^j + \eta(b_{i,j}) y^j),$$

where $\eta(b_{i,j}) = b - 1$ *if* $b_{i,j} = 0$ *and* $\eta(b_{i,j}) = -1$ *if* $b_{i,j} \neq 0$.

Using Theorem 4, we can compute $\mathrm{WF}(P)$ and $\delta_{P^{\perp}}$, the minimum Dick weight of $P^{\perp}$. The minimum Dick weight of $P^{\perp}$ is defined as

$$\delta_{P^{\perp}} := \min_{B \in P^{\perp} \setminus \{O\}} \mu(B),$$

which is used for bounding WAFOM (see Section 5.3). First, we introduce how to compute $\mathrm{WF}(P)$. The following formula to compute WAFOM is a generalization of [10, Corollary 4.2], which treats the case $G = \mathbf{F}_2$.

Corollary 3. *Let* $P \subset \mathbf{Z}_b^{s \times n}$ *be a subgroup. Then we have*

$$\mathrm{WF}(P) = -1 + \frac{1}{|P|} \sum_{B \in P} \prod_{\substack{1 \le i \le s \\ 1 \le j \le n}} (1 + \eta(b_{i,j}) b^{-j}).$$

Proof.

$$\begin{aligned}
\mathrm{WF}(P) &= \sum_{A \in P^{\perp} \setminus \{O\}} b^{-\mu(A)} \\
&= -1 + \sum_{A \in P^{\perp}} b^{-\mu(A)} \\
&= -1 + W_{P^{\perp}}(1, b^{-1}) \\
&= -1 + \frac{1}{|P|} \sum_{B \in P} \prod_{\substack{1 \le i \le s \\ 1 \le j \le n}} (1 + \eta(b_{i,j}) b^{-j}). \qquad \square
\end{aligned}$$

The merit of Theorem 4 and Corollary 3 is that the number of summation depends only on $|P|$ linearly, not $|P^{\perp}| = b^{sn}/|P|$. We can calculate weight enumerator polynomials by sn times multiplication between an integer polynomial with a binomial, and $|P|$ times addition of such polynomials of degree $n(n+1)/2$. In the case of computing WAFOM, we need sn times of multiplication of real numbers and $|P|$ times of summation of such real numbers, thus we need $O(sn|P|)$ times of operations of real numbers. On the other hand, to calculate weight enumerator polynomials based on the definition, we need $|P^{\perp}|$ times of summations of monomials, and to calculate weight WAFOM based on the definition, we need $|P^{\perp}|$ times of summations of real numbers.

For QMC, the size $|P|$ cannot exceed a reasonable number of computer operations, so $|P^{\perp}| = b^{sn}/|P|$ can be large if sn is sufficiently large. This implies that the computational complexity of calculating weight enumerator polynomials or WAFOM using Theorem 4 or Corollary 3 is smaller if sn is large.

Second, we introduce how to compute $\delta_{P^{\perp}}$. The minimum Dick weight $\delta_{P^{\perp}}$ is equal to the degree of leading nonzero term of $-1 + W_{P^{\perp}}(1, y)$, namely:

Lemma 3. *Let* $W_{P^{\perp}}(1, y) = 1 + \sum_{i=1}^{\infty} a_i y^i$. *Then we have* $\delta_{P^{\perp}} = \min\{i \mid a_i \neq 0\}$.

Thus we can obtain the minimum Dick weight of $P^{\perp}$ by calculating the weight enumerator polynomial of $P^{\perp}$.

Remark 1. *Because of Lemma* 8 *in Section* 5.5, *in order to compute* $\delta_{P^{\perp}}$ *it is sufficient to compute* $W_{P^{\perp}}(1, y)$ *only up to degree* $\delta_{P^{\perp}} \leq d^2/(2s) + 3d/2 + s$.

5. Estimation of WAFOM

The following arguments from Section 5.1 to Section 5.4 are generalizations of [11] which deals with the case $G = \mathbf{F}_2$, and arguments in Section 5.5 are generalizations of [19], which deals with the case $G = \mathbf{F}_2$. The methods for proofs are similar to [11] and [19]. In this section, we suppose that s and n are positive integers and that G is a finite abelian group.

5.1. Geometry of the Dick weight. Recall that G is a finite abelian group with $b \geq 2$ elements, $G^{\vee}$ its character group. The Dick weight $\mu : (G^{\vee})^{s \times n} \to \mathbf{N}_0$ induces a metric

$$d(A, B) := \mu(A - B) \qquad \text{for } A, B \in (G^{\vee})^{s \times n}$$

and thus $(G^{\vee})^{s \times n}$ can be regarded as a metric space.

Let $S_{s,n}(m) := |\{A \in (G^{\vee})^{s \times n} \mid \mu(A) = m\}|$, namely $S_{s,n}(m)$ is the cardinality of the sphere in $(G^{\vee})^{s \times n}$ with center 0 and radius m. A combinatorial interpretation of $S_{s,n}(m)$ is as follows. One has $s \times n$ dice. Each die has b faces. For each value $i = 1, \dots, n$, there exist exactly s dice with value 0 on one face and i on the other $b - 1$ faces. Then, $S_{s,n}(m)$ is the number of ways that the summation of the upper surfaces of $s \times n$ dice is m. This combinatorial interpretation implies the following identity:

$$\prod_{k=1}^{n} (1 + (b-1)x^k)^s = \sum_{m=0}^{\infty} S_{s,n}(m) x^m.$$

You can also see this identity from Theorem 4 for $P = \{O\}$, $x \leftarrow 1$, and $y \leftarrow x$. Note that the right hand side is a finite sum. It is easy to see that $S_{s,n}(m)$ is monotonically increasing with respect to s and n, and $S_{s,m}(m) = S_{s,m+1}(m) = S_{s,m+2}(m) = \cdots$ holds.

Definition 9. $S_s(m) := S_{s,m}(m)$.

We have the following identity between formal power series:

$$\prod_{k=1}^{\infty}(1 + (b-1)x^k)^s = \sum_{m=0}^{\infty} S_s(m)x^m. \tag{2}$$

For any positive integer M, we define

$$\mathscr{B}_{s,n}(M) := \{A \in (G^\vee)^{s\times n} \mid \mu(A) \le M\}, \qquad \mathrm{vol}_{s,n}(M) := |\mathscr{B}_{s,n}(M)|,$$

namely $\mathscr{B}_{s,n}(M)$ is the ball in $G^{s\times n}$ with center 0 and radius M, and $\mathrm{vol}_{s,n}(M)$ is its cardinality. We have $\mathrm{vol}_{s,n}(M) = \sum_{m=0}^{M} S_{s,n}(m)$, and thus $\mathrm{vol}_{s,n}(M)$ inherits properties of $S_{s,n}(m)$, namely, $\mathrm{vol}_{s,n}(M)$ is also monotonically increasing with respect to s and n, and $\mathrm{vol}_{s,M}(M) = \mathrm{vol}_{s,M+1}(M) = \mathrm{vol}_{s,M+2}(M) = \ldots$ holds.

Definition 10. $\mathrm{vol}_s(M) := \mathrm{vol}_{s,M}(M)$.

5.2. Combinatorial inequalities.

Lemma 4.

$$\mathrm{vol}_{s,n}(M) \le \mathrm{vol}_s(M) \le \exp(2\sqrt{(b-1)sM}).$$

Proof. We have already seen the first inequality. We prove the next inequality along [9, Exercise 3(b), p. 332], which treats only $S = 1$ and $b = 2$ case. If $M = 0$ it is trivial, and so we assume that $M > 0$. Define a polynomial with non-negative integer coefficients by

$$f_{s,M}(x) := \prod_{k=1}^{M}(1 + (b-1)x^k)^s.$$

Since $f_{s,M}(x)$ has only non-negative coefficients, from Identity (2) we have $\sum_{m=0}^{M} S_s(m)x^m \le f_{s,M}(x)$ $(x \in (0,1))$. Hence we have

$$\mathrm{vol}_s(M) = \sum_{m=0}^{M} S_s(m) \le \sum_{m=0}^{M} S_s(M)x^{m-M} \le f_{s,M}(x)/x^M \qquad (x \in (0,1)).$$

By taking the logarithm of the both sides and using the well-known inequality $\log(1+X) \le X$, for all $x \in (0,1)$ we have

$$\begin{aligned}\mathrm{vol}_{s,n}(M) &\le s\sum_{k=1}^{M}\log(1+(b-1)x^k) + M\log(1/x)\\ &< s(b-1)\sum_{k=1}^{M}x^k + M\log\left(1+\frac{1-x}{x}\right)\\ &< s(b-1)\frac{x}{1-x} + M\frac{1-x}{x}.\end{aligned}$$

By comparison of the arithmetic mean and the geometric mean, the last expression attains the minimum value $2\sqrt{(b-1)sM}$ when $s(b-1)x/(1-x) = M(1-x)/x$ holds, namely $x = (1+\sqrt{(b-1)s/M})^{-1} \in (0,1)$. □

LEMMA 5.

$$S_{s,n}(M) \le S_s(M) \le \exp(2\sqrt{(b-1)sM}).$$

PROOF. It follows from Lemma 4 and the inequality $S_s(M) \le \mathrm{vol}_s(M)$. □

5.3. Bounding WAFOM by the minimum weight.

DEFINITION 11. Let $P \subset G^{s\times n}$ be a subgroup. The minimum Dick weight of $P^\perp$ is defined by

$$\delta_{P^\perp} := \min_{B\in P^\perp\setminus\{O\}} \mu(B)$$

The next lemma bounds $\mathrm{WF}(P)$ by the minimum weight of $P^\perp$.

LEMMA 6. *For a positive integer M, define*

$$C_{s,n}(M) := \sum_{A\in (G^\vee)^{s\times n}\setminus\mathscr{B}_{s,n}(M-1)} b^{-\mu(A)} = \sum_{m=M}^{\infty} S_{s,n}(m)b^{-m}$$

and

$$C_s(M) := \sum_{m=M}^{\infty} S_s(m)b^{-m}.$$

Then we have

$$\mathrm{WF}^n(P) = \sum_{A\in P^\perp\setminus\{O\}} b^{-\mu(A)} \le C_{s,n}(\delta_{P^\perp}) \le C_s(\delta_{P^\perp}).$$

Proof. The last inequality is trivial, so it suffices to prove the first inequality. Since $P^{\perp}\backslash\{O\} \subset (G^{\vee})^{s\times n}\backslash\mathscr{B}_{s,n}(\delta_{P^{\perp}}-1)$ holds, we have

$$\begin{aligned}\mathrm{WF}^n(P) = \sum_{A \in P^{\perp}\backslash\{O\}} b^{-\mu(A)} &\le \sum_{A \in (G^{\vee})^{s\times n}\backslash\mathscr{B}_{s,n}(\delta_{P^{\perp}}-1)} b^{-\mu(A)} \\ &= C_{s,n}(\delta_{P^{\perp}}). \qquad \square\end{aligned}$$

We shall estimate $C_s(\lceil M'\rceil)$ (C for the Complement of the ball) for rather general real number M': from Lemma 5 it follows that

$$\begin{aligned}C_s(\lceil M'\rceil) &= \sum_{m=\lceil M'\rceil}^{\infty} S_s(m) b^{-m} \\ &\le \sum_{m=\lceil M'\rceil}^{\infty} b^{-m} e^{2\sqrt{(b-1)sm}} \\ &= b^{-\lceil M'\rceil} e^{2\sqrt{(b-1)s\lceil M'\rceil}} + \sum_{m=\lceil M'\rceil+1}^{\infty} b^{-m} e^{2\sqrt{(b-1)sm}}. \qquad (3)\end{aligned}$$

First, we estimate the second term of the above. The function

$$\exp(2\sqrt{(b-1)sm})b^{-m} = \exp(2\sqrt{(b-1)sm} - m\log b)$$

is monotonically decreasing with respect to m if

$$\begin{aligned}\frac{d}{dm}(2\sqrt{(b-1)sm} - m\log b) \le 0 &\Leftrightarrow \frac{2(b-1)s}{2\sqrt{(b-1)sm}} - \log b \le 0 \\ &\Leftrightarrow \sqrt{\frac{(b-1)s}{m}} \le \log b \\ &\Leftrightarrow m \ge (\log b)^{-2}(b-1)s,\end{aligned}$$

hence we assume that $M' \ge (\log b)^{-2}(b-1)s$. Then, we have

$$\begin{aligned}&\sum_{m=\lceil M'\rceil+1}^{\infty} b^{-m} e^{2\sqrt{(b-1)sm}} \\ &\quad\le \int_{m=\lceil M'\rceil}^{\infty} e^{-m\log b} e^{2\sqrt{(b-1)sm}}\, dm \\ &\quad= \int_{m=\lceil M'\rceil}^{\infty} \exp\left(-(\log b)\left(\sqrt{m} - \frac{\sqrt{(b-1)s}}{\log b}\right)^2 + \frac{(b-1)s}{\log b}\right) dm\end{aligned}$$

$$\leq \int_{m=M'}^{\infty} \exp\left(-(\log b)\left(\sqrt{m} - \frac{\sqrt{(b-1)s}}{\log b}\right)^2 + \frac{(b-1)s}{\log b}\right) dm$$

$$= \int_{x=\sqrt{M'}}^{\infty} \exp\left(-(\log b)\left(x - \frac{\sqrt{(b-1)s}}{\log b}\right)^2 + \frac{(b-1)s}{\log b}\right) 2x\, dx.$$

In order to bound the last integral from above, for a positive number c we assume that $\sqrt{M'} \geq (1+c)\sqrt{(b-1)s}/\log b$ or equivalently $M' \geq (1+c)^2(\log b)^{-2}(b-1)s$. This assumption is stronger than the previous assumption $M' \geq (\log b)^{-2}(b-1)s$. Then, on the domain of integration $x \geq \sqrt{M'} \geq (1+c)\sqrt{(b-1)s}/\log b$, we have $cx \leq (1+c)(x - \sqrt{(b-1)s}/\log b)$. Hence the estimation continues:

$$\sum_{m=\lceil M' \rceil + 1}^{\infty} b^{-m} e^{2\sqrt{(b-1)sm}}$$

$$\leq \int_{x=\sqrt{M'}}^{\infty} \exp\left(-(\log b)\left(x - \frac{\sqrt{(b-1)s}}{\log b}\right)^2 + \frac{(b-1)s}{\log b}\right)$$

$$\times 2\frac{1+c}{c}\left(x - \frac{\sqrt{(b-1)s}}{\log b}\right) dx$$

$$= \frac{1+c}{c}\frac{1}{\log b}\left[-\exp\left(-(\log b)\left(x - \frac{\sqrt{(b-1)s}}{\log b}\right)^2 + \frac{(b-1)s}{\log b}\right)\right]_{x=\sqrt{M'}}^{\infty}$$

$$= \frac{1+c}{c}\frac{1}{\log b} \exp\left(-(\log b)\left(\sqrt{M'} - \frac{\sqrt{(b-1)s}}{\log b}\right)^2 + \frac{(b-1)s}{\log b}\right)$$

$$= \frac{1+c}{c}\frac{1}{\log b} \exp(-(\log b)M' + 2\sqrt{(b-1)sM'})$$

$$= \frac{1+c}{c}\frac{1}{\log b} b^{-M'} e^{2\sqrt{(b-1)sM'}}.$$

Second, we consider the first term of (3). We have already proved that $\exp(2\sqrt{(b-1)sm})b^{-m}$ is monotonically decreasing if $m \geq (\log b)^{-2}(b-1)s$, and thus the assumption $M' \geq (\log b)^{-2}(b-1)s$ implies

$$b^{-\lceil M' \rceil} e^{2\sqrt{(b-1)s\lceil M' \rceil}} \leq b^{-M'} e^{2\sqrt{(b-1)sM'}}.$$

Therefore we have

$$
\begin{aligned}
C_s(\lceil M' \rceil) &\le b^{-\lceil M' \rceil} e^{2\sqrt{(b-1)s\lceil M' \rceil}} + \sum_{m=\lceil M' \rceil+1}^{\infty} b^{-m} e^{2\sqrt{(b-1)sm}} \\
&\le b^{-M'} e^{2\sqrt{(b-1)sM'}} + \frac{1+c}{c} \frac{1}{\log b} b^{-M'} e^{2\sqrt{(b-1)sM'}} \\
&= \left(1 + \frac{1+c}{c} \frac{1}{\log b}\right) b^{-M'} e^{2\sqrt{(b-1)sM'}}.
\end{aligned}
$$

Now we proved:

Proposition 3. *Let c be a positive real number. Let M' be a real number with $M' \ge (1+c)^2 (\log b)^{-2} (b-1)s$. Then we have the following bound*

$$
C_{s,n}(\lceil M' \rceil) \le C_s(\lceil M' \rceil) \le \left(1 + \frac{1+c}{c} \frac{1}{\log b}\right) b^{-M'} e^{2\sqrt{(b-1)sM'}}.
$$

5.4. Existence of low-WAFOM point sets. We denote the probability of the event A by $\mathrm{prob}[A]$. Let p_b be the smallest prime factor of b. Let d be a positive integer. Choose d matrices $B_1, \ldots, B_d \in G^{s \times n}$ independently and uniformly at random. Let $P = \langle B_1, \ldots, B_d \rangle \subset G^{s \times n}$ be the G-linear span of $B_1, \ldots, B_d$, namely $P = \{g_1 B_1 + \cdots + g_d B_d \mid g_1, \ldots, g_d \in G\}$ where $g \in G$ acts on $B = (b_{ij})$ by $gB = (gb_{ij})$. Note that $|P| \le b^d$.

Remark 2. *If $G = \mathbf{Z}_b$, by the theory of invariant factor decomposition, we can say that there exist matrices $B'_1, \ldots, B'_d$ such that $P' := \langle B'_1, \ldots, B'_d \rangle$ includes P and becomes a free $\mathbf{Z}_b$-module of rank d. Thus if $G = \mathbf{Z}_b$, we can replace "subgroup P" in this subsection with a "digital net P," since in this subsection we consider only the existence of a subgroup which has large minimum Dick weight, and $P \subset P'$ implies that $\delta_{P^\perp} \le \delta_{P'^\perp}$.*

First, we evaluate $\mathrm{prob}[\mathrm{perp}_L]$, where we define perp_L as the event that $B_1, \ldots, B_d$ are all perpendicular to $L \in (G^\vee)^{s \times n}$.

Lemma 7. *Let $L \in (G^\vee)^{s \times n}$ be a nonzero matrix. Then we have* $\mathrm{prob}[L \perp B] \le 1/p_b$. *Especially we have* $\mathrm{prob}[\mathrm{perp}_L] \le p_b^{-d}$.

Proof. We consider the map $(L\bullet) : G^{s \times n} \to \mathbf{C}, B \mapsto L \bullet B$. Then we have the surjective group homomorphism $G^{s \times n} \to \mathrm{Im}(L\bullet)$, and thus $|\mathrm{Im}(L\bullet)|$ divides $G^{s \times n}$. Moreover, since L is nonzero, $|\mathrm{Im}(L\bullet)|$ is larger than 1. Hence we have $|\mathrm{Im}(L\bullet)| \ge p_b$. Therefore we have $\mathrm{prob}[L \perp B] = |\mathrm{Im}(L\bullet)|^{-1} \le 1/p_b$, and especially we have $\mathrm{prob}[\mathrm{perp}_L] = \mathrm{prob}[L \perp B]^d \le p_b^{-d}$. □

Let M be a positive integer. We evaluate the probability of the event that $\delta_{P^\perp} \ge M$. We have

$$
\begin{aligned}
\mathrm{prob}[\delta_{P^\perp} \geq M] &= 1 - \mathrm{prob}[\delta_{P^\perp} \leq M-1] \\
&= 1 - \mathrm{prob}[\exists L \in \mathscr{B}_{s,n}(M-1)\backslash\{O\} \ \text{ s.t. } \ L \in P^\perp] \\
&= 1 - \mathrm{prob}[\exists L \in \mathscr{B}_{s,n}(M-1)\backslash\{O\} \ \text{ s.t. } \ L \perp B_1, \dots, L \perp B_d] \\
&= 1 - \mathrm{prob}[\textstyle\bigcup_{L \in \mathscr{B}_{s,n}(M-1)\backslash\{O\}} \mathrm{perp}_L] \\
&\geq 1 - \sum_{L \in \mathscr{B}_{s,n}(M-1)\backslash\{O\}} \mathrm{prob}[\mathrm{perp}_L] \\
&\geq 1 - (\mathrm{vol}_{s,n}(M-1) - 1) \cdot p_b^{-d} \\
&> 1 - \mathrm{vol}_{s,n}(M-1) \cdot p_b^{-d}.
\end{aligned}
$$

This shows:

PROPOSITION 4. *If* $\mathrm{vol}_{s,n}(M-1) \leq p_b^d$ *holds, then there exists a subgroup* $P \subset G^{s\times n}$ *with* $|P| \leq b^d$ *satisfying* $\delta_{P^\perp} \geq M$.

By Lemma 4, the condition of this proposition is satisfied if it holds that

$$
e^{2\sqrt{(b-1)s(M-1)}} \leq p_b^d \Leftrightarrow M \leq \frac{(\log p_b)^2 d^2}{4(b-1)s} + 1. \tag{4}
$$

Therefore we have the following sufficient condition on the existence of M.

PROPOSITION 5. *If* $M \leq (\log p_b)^2 d^2/(4(b-1)s) + 1$ *holds, then Inequality* (4) *is satisfied, and hence there exists a subgroup* $P \subset G^{s\times n}$ *with* $|P| \leq b^d$ *satisfying* $\delta_{P^\perp} \geq M$.

From now on, we define $\alpha_b := (\log p_b)/2$ and $M' := A^2 d^2/((b-1)s)$ where $A \leq \alpha_b$ and we take M to be $\lfloor M'+1 \rfloor$ so that P with $|P| \leq b^d$ and $\delta_{P^\perp} \geq M$ exists. Then, by Proposition 3, we have the following upper bound of $\mathrm{WF}(P)$:

PROPOSITION 6. *Let* $\alpha_b := (\log p_b)/2$. *Take a real number* A *with* $A \leq \alpha_b$ *and an arbitrary real number* $c > 0$. *Then for any positive integers* s, n, *and* $d \geq (1+c)(b-1)s/(A \log b)$, *there exists a subgroup* $P \subset G^{s\times n}$ *with* $|P| \leq b^d$ *satisfying*

$$
\mathrm{WF}^n(P) \leq \left(1 + \frac{1+c}{c}\frac{1}{\log b}\right) b^{-A^2 d^2/((b-1)s)} e^{2Ad}.
$$

PROOF. Define $M' := A^2 d^2/((b-1)s)$ and $M := \lfloor M'+1 \rfloor$. By Proposition 5, there exists a subgroup $P \subset G^{s\times n}$ with $|P| \leq b^d$ and $\delta_{P^\perp} \geq M$. For this P, from Lemma 6 and Proposition 3 we have

$$\begin{aligned}\mathrm{WF}(P) &\le C_s(M)\\ &= C_s(\lceil M' \rceil)\\ &\le \left(1+\frac{1+c}{c}\frac{1}{\log b}\right)b^{-M'}e^{2\sqrt{(b-1)sM'}}\\ &= \left(1+\frac{1+c}{c}\frac{1}{\log b}\right)b^{-A^2d^2/((b-1)s)}e^{2Ad},\end{aligned}$$

which proves the proposition. □

In particular, take $A = \alpha_b$ and we have the next theorem.

THEOREM 5. *Let* $\alpha_b := (\log p_b)/2$ *and take an arbitrary real number* $c > 0$. *Then for any* s, n, *and* $d \ge (1+c)(b-1)s/(\alpha_b \log b)$, *there exists a subgroup* $P \subset G^{s\times n}$ *with* $|P| \le b^d$ *satisfying*

$$\mathrm{WF}(P) \le \left(1+\frac{1+c}{c}\frac{1}{\log b}\right)b^{-\alpha_b^2d^2/((b-1)s)}e^{2\alpha_b d}.$$

Applying Theorem 5 to the case $G = \mathbf{F}_2$, we can improve [11, Theorem 2 and Remark 5].

COROLLARY 4. *Let* $\alpha := \alpha_2 = (\log 2)/2$ *and take an arbitrary real number* $c > 0$. *Then for any* n *and* $d \ge (1+c)s/(\alpha \log 2)$, *there exists a linear subspace* $P \subset \mathbf{F}_2^{s\times n}$ *with* $\dim P \le d$ *satisfying*

$$\mathrm{WF}(P) \le \left(1+\frac{1+c}{c}\frac{1}{\log 2}\right)2^{-\alpha^2d^2/s}e^{2\alpha d}.$$

REMARK 3. *Suzuki* [18] *proved that the construction of higher order digital nets on* $\mathbf{F}_p$ *given in* [3] *combined with some Niederreiter-Xing point sets* [14] *yields an explicit construction of low-WAFOM point sets, whose order of WAFOM is almost the same with the order obtained in this paper.*

5.5. A lower bound of WAFOM. In this subsection, we show a lower bound on WAFOM(P), as a generalization of [19]. The next lemma gives an upper bound on the minimum Dick weight of $P^\perp$ for given $P \subset G^{s\times n}$, which implies a lower bound of WAFOM(P).

LEMMA 8. *Suppose that* s *and* n *are positive integers. Let* $P \subset G^{s\times n}$ *be a subgroup with* $|P| \le b^d$. *Let* q, r *be nonnegative integers which satisfy* $d = qs + r$ *and* $0 \le r < s$. *Then we have the following:*

(1) $\delta_{P^\perp} \le sq(q+1)/2 + (q+1)(r+1) \le d^2/2s + 3d/2 + s$.

(2) *Let* C *be an arbitrary positive real number greater than* $1/2$. *If* $d/s \ge (\sqrt{C+1/16}+3/4)/(C-1/2)$ *holds, then we have* $\delta_{P^\perp} \le Cd^2/s$.

PROOF. We define a subgroup $Q := \{A = (a_{ij}) \in (G^{\vee})^{s\times n} \mid a_{ij} = 0$ if $(q+2 \leq j \leq n)$ or $(j = q+1$ and $r+2 \leq i \leq s)\}$. We have $|Q| = b^{qs+r+1} = b^{d+1}$. There is a $\mathbf{Z}$-module isomorphism $P^{\perp}/(P^{\perp} \cap Q) \simeq (P^{\perp} + Q)/Q$, and thus we have

$$|P^{\perp} \cap Q| = \frac{|P^{\perp}| \cdot |Q|}{|P^{\perp} + Q|} \geq \frac{b^{sn-d} \cdot b^{d+1}}{|(G^{\vee})^{s\times n}|} = b,$$

especially there exists a non-zero matrix $A' \in (P^{\perp} \cap Q)$. Therefore we have

$$\delta_{P^{\perp}} \leq \mu(A') \leq \max\{\mu(A) \mid A = (a_{ij}) \in Q\} = sq(q+1)/2 + (q+1)(r+1),$$

where the last equality holds if the components of A is as follows:

$$\begin{cases} a_{ij} = 0 \text{ if } (q+2 \leq j \leq n) \text{ or } (j = q+1 \text{ and } r+2 \leq i \leq s) \\ a_{ij} \neq 0 \text{ if } (1 \leq j \leq q) \text{ or } (j = q+1 \text{ and } 1 \leq i \leq r+1) \end{cases}.$$

In particular, since $q \leq d/s$ and $r+1 \leq s$, we have

$$\begin{aligned} \delta_{P^{\perp}} &\leq sq(q+1)/2 + (q+1)(r+1) \\ &\leq \frac{d}{2}\left(\frac{d}{s}+1\right) + \left(\frac{d}{s}+1\right)s = \frac{d^2}{s}\left(\frac{1}{2} + \frac{3s}{2d} + \frac{s^2}{d^2}\right), \end{aligned}$$

which proves the first statement.

Let C be a real number greater than $1/2$ and we assume $d/s \geq (\sqrt{C + 1/16} + 3/4)/(C - 1/2)$. Then we have $1/2 + 3s/2d + s^2/d^2 \leq C$. Thus we obtain

$$\delta_{P^{\perp}} \leq \frac{d^2}{s}\left(\frac{1}{2} + \frac{3s}{2d} + \frac{s^2}{d^2}\right) \leq Cd^2/s,$$

which proves the second statement. □

The above lemma gives a lower bound of $\mathrm{WF}(P)$.

THEOREM 6. *Suppose that s and n are positive integers. Let G be a finite abelian group with $b \geq 2$ elements. Let $P \subset G^{s\times n}$ be a subgroup with $|P| \leq b^d$. Let C be an arbitrary positive real number greater than $1/2$. If $d/s \geq (\sqrt{C + 1/16} + 3/4)/(C - 1/2)$ holds, then we have*

$$\mathrm{WF}^n(P) \geq b^{-Cd^2/s}.$$

PROOF.

$$\mathrm{WF}^n(P) = \sum_{A \in P^{\perp}\setminus\{O\}} b^{-\mu(A)} \geq b^{-\delta_{P^{\perp}}} \geq b^{-Cd^2/s}.$$ □

5.6. Order of WAFOM. In this subsection, we consider the order of $\mathrm{WF}(P)$ where P is a subgroup of $G^{s\times n}$ with $|P| = b^d$.

We fix the base b. Let $D := \alpha_b = (\log p_b)/2$. We fix a positive integer E satisfying $E > (b-1)/(D\log b)$. Let c be the real number such that $E = (1+c)(b-1)/(D\log b)$ (by the assumption that $E > (b-1)/(D\log b)$, c is positive). Note that c, D and E depend only on b.

We assume that $d/s \geq E$. Then, by Proposition 6, there exists a subgroup $P \subset G^{s\times n}$ with $|P| \leq b^d$ satisfying

$$\mathrm{WF}^n(P) \leq \left(1 + \frac{1+c}{c}\frac{1}{\log b}\right) b^{-D^2 d^2/((b-1)s)} e^{2Dd}.$$

Moreover, by Theorem 6, for every P with $|P| \leq b^d$ we have $\mathrm{WF}^n(P) \geq b^{-Cd^2/s}$ where $C = (1/2 + 3/(2E) + 1/E^2)$. Thus we have the following lemma.

LEMMA 9. *If $d/s \geq E$, we have*

$$\begin{aligned} -Cd^2/s &\leq \min\{\log_b(\mathrm{WF}^n(P)) \mid P \subset G^{s\times n} \ \textit{subgroup},\ |P| \leq b^d\} \\ &\leq -D^2 d^2/((b-1)s) + 2Dd/\log b + \log_b\left(1 + \frac{1+c}{c}\frac{1}{\log b}\right). \end{aligned}$$

Especially, let $N = b^d$ and we have the following.

THEOREM 7. *Let G be a finite abelian group with $|G| = b$. Let $P \subset G^{s\times n}$ be a subgroup with $|P| \leq N$. Let c, C, D, and E are constants as Lemma 9, which depend only on b. Suppose that $(\log N)/s \geq E$. Then we have*

$$\begin{aligned} N^{-C(\log N)/s} &\leq \min\{\mathrm{WF}^n(P) \mid P \subset G^{s\times n} \ \textit{subgroup},\ |P| \leq N\} \\ &\leq \left(1 + \frac{1+c}{c}\frac{1}{\log b}\right) N^{-D^2(\log N)/((\log b)(b-1)s) + 2D/\log b}. \end{aligned}$$

Acknowledgement

The author would like to express his gratitude to his supervisor Professor Makoto Matsumoto for the patient guidance, encouragement and many helpful discussions and comments.

References

[1] Jan Baldeaux, Josef Dick, Gunther Leobacher, Dirk Nuyens, and Friedrich Pillichshammer. Efficient calculation of the worst-case error and (fast) component-by-component construction of higher order polynomial lattice rules. Numer. Algorithms, 59(3):403–431, 2012.

[2] W. W. L. Chen and M. M. Skriganov. Explicit constructions in the classical mean squares problem in irregularities of point distribution. J. Reine Angew. Math., 545:67–95, 2002. translation in St. Petersburg Math. J. 13(2002), no. 2, 301–337.
[3] Josef Dick. Walsh spaces containing smooth functions and quasi-Monte Carlo rules of arbitrary high order. SIAM J. Numer. Anal., 46(3):1519–1553, 2008.
[4] Josef Dick. The decay of the Walsh coefficients of smooth functions. Bull. Aust. Math. Soc., 80(3):430–453, 2009.
[5] Josef Dick and Makoto Matsumoto. On the Fast Computation of the Weight Enumerator Polynomial and the t Value of Digital Nets over Finite Abelian Groups. SIAM J. Discrete Math., 27(3):1335–1359, 2013.
[6] Josef Dick and Friedrich Pillichshammer. Digital nets and sequences: Discrepancy theory and quasi-Monte Carlo integration. Cambridge University Press, Cambridge, 2010.
[7] Gerhard Larcher, Harald Niederreiter, and Wolfgang Ch. Schmid. Digital nets and sequences constructed over finite rings and their application to quasi-Monte Carlo integration. Monatsh. Math., 121(3):231–253, 1996.
[8] F. J. MacWilliams and N. J. A. Sloane. The theory of error-correcting codes. I. North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.
[9] Jiří Matoušek and Jaroslav Nešetřil. Invitation to discrete mathematics. The Clarendon Press Oxford University Press, New York, 1998.
[10] Makoto Matsumoto, Mutsuo Saito, and Kyle Matoba. A computable figure of merit for quasi-Monte Carlo point sets. Mathematics of Computation, 83(287):1233–1250, 2014.
[11] Makoto Matsumoto and Takehito Yoshiki. Existence of higher order convergent quasi-Monte Carlo rules via Walsh figure of merit. In Monte Carlo and quasi-Monte Carlo methods 2012, pages 569–579. Springer, Berlin, 2013.
[12] Harald Niederreiter. Low-discrepancy point sets. Monatsh. Math., 102(2):155–167, 1986.
[13] Harald Niederreiter. Random number generation and quasi-Monte Carlo methods, volume 63 of CBMS-NSF Regional Conference Series in Applied Mathematics. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.
[14] Harald Niederreiter and Chaoping Xing. Rational points on curves over finite fields: theory and applications, volume 285 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 2001.
[15] M. Yu. Rozenblyum and M. A. Tsfasman. Codes for the m-metric. Problemy Peredachi Informatsii, 33(1):55–63, 1997.
[16] Jean-Pierre Serre. Linear representations of finite groups. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.
[17] M. M. Skriganov. Coding theory and uniform distributions. Algebra i Analiz, 13(2):191–239, 2001.
[18] Kosuke Suzuki. An explicit construction of point sets with large minimum Dick weight. J. Complexity, 30(3):347–354, 2014.
[19] Takehito Yoshiki. A lower bound on WAFOM. Hiroshima Math. J., 44(3):261–266, 2014.

Kosuke Suzuki
Graduate School of Mathematical Sciences
The University of Tokyo
3-8-1 *Komaba, Meguro-ku, Tokyo* 153-8914, *Japan*
E-mail: ksuzuki@ms.u-tokyo.ac.jp