sciendo

uniform distribution theory

DOI: 10.2478/udt-2019–0004
Unif. Distrib. Theory **14** (2019), no.1, 43–52

A COMPLETE CLASSIFICATION OF DIGITAL $(0, m, 3)$-NETS AND DIGITAL $(0, 2)$-SEQUENCES IN BASE 2

Roswitha Hofer[1] — Kosuke Suzuki[2]

[1]Johannes Kepler University Linz, Linz, AUSTRIA

[2]Hiroshima University, Higashi-Hiroshima, JAPAN

ABSTRACT. We give a complete classification of all matrices $C_1, C_2, C_3 \in \mathbb{F}_2^{m\times m}$ which generate a digital $(0, m, 3)$-net in base 2 and a complete classification of all matrices $C_1, C_2 \in \mathbb{F}_2^{\mathbb{N}\times\mathbb{N}}$ which generate a digital $(0, 2)$-sequence in base 2.

Communicated by Friedrich Pillichshammer

1. Introduction and main results

The algorithms for constructing digital (t, m, s)-nets and (t, s)-sequences, which were introduced by Niederreiter [7], are well-established methods to obtain low-discrepancy point sets and low-discrepancy sequences. Low-discrepancy point sets and sequences are the main ingredients of quasi-Monte Carlo quadrature rules for numerical integration (see for example [1, 8] for details). The purpose of this paper is to characterize digital nets and sequences in base 2 with best possible quality parameter t. We start the paper with introducing the algorithm for digital (t, m, s)-nets and digital (t, s)-sequences in base b and defining the quality parameter t.

2010 Mathematics Subject Classification: 11K16, 11K38.
Keywords: digital nets, digital sequences, classification of generating matrices.
The first author is supported by the Austrian Science Fund (FWF): Project F5505-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications". The second author is supported by Grant-in-Aid for JSPS Fellows (No. 17J00466).

Let $\mathbb{N}$ be the set of all positive integers, $\mathbb{F}_b$ be the field of b elements with a prime power b, and $\mathbf{Z}_b := \{0, 1, \dots, b-1\}$. For $m \in \mathbb{N}$, $\mathbb{F}_b^{m \times m}$ denotes the set of all $m \times m$ matrices over $\mathbb{F}_b$. For $n \in \mathbb{N} \cup \{0\}$, we write the b-adic expansion of n as $n = \sum_{i=1}^{\infty} z_i(n) b^{i-1}$ with $z_i(n) \in \mathbf{Z}_b$, where all but finitely many $z_i(n)$ equal zero. Let s, $m \in \mathbb{N}$.

The definition of the digital net over $\mathbb{F}_b$ needs the following data:

(A) bijections $\psi_r \colon \mathbf{Z}_b \to \mathbb{F}_b$ for integers $1 \le r \le m$ with $\psi_r(0) = 0$,

(B) matrices $C_1, \dots, C_s \in \mathbb{F}_b^{m \times m}$,

(C) bijections $\lambda_{i,j} \colon \mathbb{F}_b \to \mathbf{Z}_b$ for integers $1 \le i \le m$ and $1 \le j \le s$.

For $1 \le j \le s$ and $k \in \mathbb{N} \cup \{\infty\}$, we define the function $\phi_{k,j} \colon \mathbb{F}_b^k \to [0,1]$ as

$$\phi_{k,j}\big((y_1, \dots, y_k)^\top\big) := \sum_{i=1}^{k} \frac{\lambda_{i,j}(y_i)}{b^i}.$$

The digital net generated by $(C_1, \dots, C_s)$ is a set of b^m points in $[0,1)^s$ that is constructed as follows. We define

$$\boldsymbol{y}_{n,j} \in \mathbb{F}_b^m \quad \text{for} \quad 0 \le n < b^m \quad \text{and} \quad 1 \le j \le s$$

as

$$\boldsymbol{y}_{n,j} := C_j \cdot \Big(\psi_1\big(z_1(n)\big), \dots, \psi_m\big(z_m(n)\big)\Big)^\top \in \mathbb{F}_b^m.$$

Then we obtain the n-th point $\boldsymbol{x}_n$ by applying $\phi_{m,j}$ componentwise to the $\boldsymbol{y}_{n,j}$, i.e.,

$$\boldsymbol{x}_n := \big(\phi_{m,1}(\boldsymbol{y}_{n,1}), \dots, \phi_{m,s}(\boldsymbol{y}_{n,s})\big).$$

Finally letting n range between 0 and $b^m - 1$ we obtain the point set

$$\{\boldsymbol{x}_0, \dots, \boldsymbol{x}_{b^m-1}\} \subset [0,1)^s$$

that is called the digital net generated by $(C_1, \dots, C_s)$.

In a similar way, to define digital sequences we choose data of

(A') bijections $\psi_r \colon \mathbf{Z}_b \to \mathbb{F}_b$ for all integers $r \ge 1$ with $\psi_r(0) = 0$,

(B') infinite matrices $C_1, \dots, C_s \in \mathbb{F}_b^{\mathbb{N} \times \mathbb{N}}$,

(C') bijections $\lambda_{i,j} \colon \mathbb{F}_b \to \mathbf{Z}_b$ for all integers $i \ge 1$ and $1 \le j \le s$.

Then the digital sequence generated by $(C_1, \dots, C_s)$ is the sequence of points in $[0,1]^s$ that is constructed as follows. We define

$$\boldsymbol{y}_{n,j} \in \mathbb{F}_b^{\mathbb{N}} \quad \text{for} \;\; n \in \mathbb{N} \cup \{0\}$$

and

$$1 \le j \le s \quad \text{as} \quad \boldsymbol{y}_{n,j} := C_j \cdot \Big(\psi_1\big(z_1(n)\big), \psi_2\big(z_2(n)\big), \dots\Big)^\top \in \mathbb{F}_b^{\mathbb{N}}.$$

This matrix-vector multiplication is well-defined since almost all $z_i(n)$ equal zero. Then we obtain the n-th point $\boldsymbol{x}_n$ by setting

$$\boldsymbol{x}_n := \big(\phi_{\infty,1}(\boldsymbol{y}_{n,1}), \dots, \phi_{\infty,s}(\boldsymbol{y}_{n,s})\big).$$

The digital sequence generated by $(C_1, \dots, C_s)$ is the sequence of points $\{\boldsymbol{x}_0, \boldsymbol{x}_1, \dots\} \subset [0,1]^s$.

The nonnegative integer t in the notions of (t,m,s)-nets and (t,s)-sequences quantifies in a certain sense the uniformity of digital nets and sequences. Let $b \in \mathbb{N} \setminus \{1\}$. A set $\mathcal{P}$ of b^m points in $[0,1)^s$ is said to be a (t,m,s)-net in base b if every subinterval of the form

$$\prod_{i=1}^{s} \big[a_i/b^{c_i}, (a_i+1)/b^{c_i}\big) \quad \text{with integers} \quad c_i \geq 0 \quad \text{and} \quad 0 \leq a_i < b^{c_i}$$

and of volume b^{t-m} contains exactly b^t points from $\mathcal{P}$. For the definition of (t,s)-sequences in base b, we need to introduce the truncation operator. For $x \in [0,1]$ with the prescribed b-adic expansion $x = \sum_{i=1}^{\infty} x_i/b^i$ (where the case $x_i = b-1$ for almost all i is allowed), we define the m-digit truncation

$$[x]_m := \sum_{i=1}^{m} x_i/b^i.$$

For $\boldsymbol{x} = (x_1, \dots, x_s) \in [0,1]^s$, the coordinate-wise m-digit truncation of $\boldsymbol{x}$ is defined as

$$[\boldsymbol{x}]_m := ([x_1]_m, \dots, [x_s]_m).$$

A sequence $\mathcal{S} = \{\boldsymbol{x}_0, \boldsymbol{x}_1, \dots\}$ of points in $[0,1]^s$ with prescribed b-adic expansions is said to be a (t,s)-sequence in base b if, for all nonnegative integers k and m, the set

$$\{[\boldsymbol{x}_{kb^m}]_m, \dots, [\boldsymbol{x}_{(k+1)b^m-1}]_m\}$$

is a (t,m,s)-net in base b.

By the definitions of (t,m,s)-nets and (t,s)-sequences, a smaller t implies more conditions on the uniformity of the points and of the sequences. Indeed a smaller t corresponds with a smaller discrepancy bound (cf. [7]). Hence smaller t would be appreciated and $t = 0$ is the best possible. Having lowest possible value 0 for t has another merit: the randomized quasi-Monte Carlo estimator of a scrambled $(0,m,s)$-net in base b is asymptotically normal [6]. However, $t = 0$ cannot be attained when s is large. It is well known that $(0,m,s)$-nets in any base b exist only if $s \leq b+1$ and $(0,s)$-sequences in base b exist only if $s \leq b$ [8, Corollary 4.24]. On the other hand, there are many known digital $(0,b)$-sequences in prime base b, including the two-dimensional Sobol′ sequence for $b = 2$ [9], Faure sequences [2], generalized Faure sequences [10], and its reorderings [3]. From these sequences we can construct digital $(0, m, b+1)$-nets in base b, see [8, Lemma 4.22] or Lemma 2.3.

A characterization of $(0, m, 3)$-net in base 2 generated by (I, C, C^2) with some $C \in \mathbb{F}_2^{m \times m}$ was given in [5] and a characterization of $(0, 2)$-sequences in base 2 generated by non-singular upper-triangular matrices (C_1, C_2) was given in [4]. Our contribution in this note is to classify all generating matrices of digital $(0, m, 3)$-nets and digital $(0, 2)$-sequences in base 2.

For the statements of our results, we introduce some notation. We fix a prime power b and consider digital nets over $\mathbb{F}_b$. Let I_m be the $m \times m$ identity matrix in $\mathbb{F}_b^{m \times m}$. Let J_m be the $m \times m$ anti-diagonal matrix in $\mathbb{F}_b^{m \times m}$ whose anti-diagonal entries are all 1, and P_m be the $m \times m$ upper-triangular Pascal matrix in $\mathbb{F}_2^{m \times m}$ (note that for P_m we only consider the case $b = 2$), i.e.,

$$J_m = \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix}, \qquad P_m = \left(\binom{j-1}{i-1} \right)_{i,j=1}^{m} = \begin{pmatrix} \binom{0}{0} & \binom{1}{0} & \cdots & \binom{m-1}{0} \\ & \binom{1}{1} & & \vdots \\ & & \ddots & \vdots \\ & & & \binom{m-1}{m-1} \end{pmatrix},$$

where the latter is considered modulo 2. If there is no confusion, we omit the subscripts and simply write I, J, and P. Let $\mathcal{L}_m$ (resp. $\mathcal{U}_m$) be the set of non-singular lower- (resp. upper-) triangular $m \times m$ matrices over $\mathbb{F}_b$. Let $\mathcal{L}_\infty$ (resp. $\mathcal{U}_\infty$) be the set of non-singular lower- (resp. upper-) triangular infinite matrices over $\mathbb{F}_b$. Let

$$P_\infty \in \mathbb{F}_2^{\mathbb{N} \times \mathbb{N}}$$

be the infinite matrix whose $m \times m$ upper left submatrix is P_m for all $m \geq 1$. Note that for $C \in \mathbb{F}_b^{\mathbb{N} \times \mathbb{N}}$ and $L \in \mathcal{L}_\infty$, $U \in \mathcal{U}_\infty$ the products LC and CU are well defined and $(LC)U = L(CU)$. For $C \in \mathbb{F}_b^{m \times m}$ with $m \in \mathbb{N} \cup \{\infty\}$ and for $k \in \mathbb{N}$ with $k \leq m$ we write $C^{(k)} \in \mathbb{F}_b^{k \times k}$ for the upper left $k \times k$ submatrix of C.

We are now ready to state our main results.

Theorem 1.1. *Let $b = 2$, $m \geq 1$ be an integer, and $C_1, C_2, C_3 \in \mathbb{F}_2^{m \times m}$. Then the following statements are equivalent:*

(i) *(C_1, C_2, C_3) generates a digital $(0, m, 3)$-net in base 2;*

(ii) *There exist $L_1, L_2 \in \mathcal{L}_m$, $U \in \mathcal{U}_m$, and non-singular $M \in \mathbb{F}_2^{m \times m}$ such that*

$$(C_1, C_2, C_3) = (JM, L_1UM, L_2PUM).$$

Theorem 1.2. *Let $b = 2$ and $C_1, C_2 \in \mathbb{F}_2^{\mathbb{N}\times\mathbb{N}}$. Then the following statements are equivalent:*

(i) *(C_1, C_2) generates a digital $(0, 2)$-sequence in base 2;*

(ii) *There exist $L_1, L_2 \in \mathcal{L}_\infty$ and $U \in \mathcal{U}_\infty$ such that*

$$(C_1, C_2) = (L_1 U, L_2 P_\infty U).$$

Well-known generating matrices of the digital $(0, 2)$-sequences over $\mathbb{F}_2$ are the following: (I, P) for two-dimensional Sobol′ sequence and the Faure sequence over $\mathbb{F}_2$, (L_1, L_2P) with any $L_1, L_2 \in \mathcal{L}_\infty$ for generalized Faure sequences over $\mathbb{F}_2$. We also know good reorderings of digital $(0, 2)$-sequences in the sense that we have that (G_1U, G_2U) with any $U \in \mathcal{U}_\infty$ generates a $(0, 2)$-sequence if (G_1, G_2) generates $(0, 2)$-sequence. Thus Theorem 1.2 states that every digital $(0, 2)$-sequence over $\mathbb{F}_2$ is a reordering of a generalized Faure sequence.

In the rest of the paper, we give auxiliary results in Section 2 and prove the above theorems in Section 3.

2. Auxiliary results

In this section, we fix a prime power b and consider digital nets and digital sequences over $\mathbb{F}_b$. We start with t-value-preserving operations.

Lemma 2.1 ([5, Lemma 2.2])**.** *Let*

$$C_1, \dots, C_s \in \mathbb{F}_b^{m\times m} \quad \text{and} \quad L_1, \dots, L_s \in \mathcal{L}_m.$$

Let $G \in \mathbb{F}_b^{m\times m}$ be non-singular. Then the following are equivalent.

(i) *$(C_1, \dots, C_s)$ generates a digital (t, m, s)-net in base b.*

(ii) *$(L_1C_1G, \dots, L_sC_sG)$ generates a digital (t, m, s)-net in base b.*

Lemma 2.2. *Let*

$$C_1, \dots, C_s \in \mathbb{F}_b^{\mathbb{N}\times\mathbb{N}}, \qquad L_1, \dots, L_s \in \mathcal{L}_\infty \quad \text{and} \quad U \in \mathcal{U}_\infty.$$

Then the following are equivalent.

(i) *$(C_1, \dots, C_s)$ generates a digital (t, s)-sequence in base b.*

(ii) *$(L_1C_1U, \dots, L_sC_sU)$ generates a digital (t, s)-sequence in base b.*

Proof. A slight adaption of the proof of [3, Proposition 1] (resp. [10, Theorem 1]) shows that multiplying L_i from left (resp. multiplying U from right) does not change the t-value. Note that here we used that L_i^{-1} exists in $\mathcal{L}_\infty$ and U^{-1} exists in $\mathcal{U}_\infty$. □

The following results point out relations between digital nets and sequences.

Lemma 2.3 ([8, Lemma 4.22]). *Let $\{\boldsymbol{x}_i\}_{i\geq 0}$ be a (t,s)-sequence in base b. Then $\{(\boldsymbol{x}_i, ib^{-m})\}_{i=0}^{b^m-1}$ is a $(t,m,s+1)$-net in base b.*

Lemma 2.4. *Let*

$$C_1,\dots,C_s \in \mathbb{F}_b^{\mathbb{N}\times\mathbb{N}}.$$

Then the following are equivalent.

(i) *$(C_1,\dots,C_s)$ generates a digital (t,s)-sequence in base b.*

(ii) *$(C_1^{(m)},\dots,C_s^{(m)})$ generates a digital (t,m,s)-net in base b for every $m\in\mathbb{N}$.*

(iii) *$(J_m, C_1^{(m)},\dots,C_s^{(m)})$ generates a digital $(t,m,s+1)$-net in base b for every $m\in\mathbb{N}$.*

Proof. (ii) implies (i) by [8, Theorem 4.36]. Clearly (iii) shows (ii). (i) implies (iii) by Lemma 2.3. ☐

Having $t=0$ is related to LU decomposability. In particular, we have a characterization of digital $(0,1)$-sequences and digital $(0,m,2)$-nets in base b.

Lemma 2.5. *Let b be a prime power. Let $B\in\mathbb{F}_b^{m\times m}$. Then (J_m,B) generates a digital $(0,m,2)$-net in base b if and only if there exist $L\in\mathcal{L}_m$ and $U\in\mathcal{U}_m$ such that $B=LU$.*

Proof. This is essentially proved in [5, Lemma 3.1] for $b=2$, and the proof therein can be applied to the general case. However, for its importance, we give a brief proof. It can be shown that (J_m,B) generates a digital $(0,m,2)$-net in base b if and only if all leading principal minors of B are different from zero, which is equivalent to the LU decomposability of B. ☐

Lemma 2.6. *Let $m\geq 1$ be an integer and $C_1,C_2\in\mathbb{F}_b^{m\times m}$. Then (C_1,C_2) generates a $(0,m,2)$-net in base b if and only if there exist $L\in\mathcal{L}_m$, $U\in\mathcal{U}_m$ and non-singular $M\in\mathbb{F}_b^{m\times m}$ such that $(C_1,C_2)=(JM,LUM)$.*

Proof. Let $M=JC_1$. By putting $C_2'=C_2M^{-1}$, $t(C_1,C_2)=0$ is equivalent to $t(JM,C_2'M)=0$, which is equivalent to $t(J,C_2')=0$ by Lemma 2.1. Hence Lemma 2.6 reduces to the case $C_1=J$, i.e., Lemma 2.5. ☐

Lemma 2.7. *Let $B\in\mathbb{F}_b^{\mathbb{N}\times\mathbb{N}}$. Then B generates a digital $(0,1)$-sequence in base b if and only if there exist $L\in\mathcal{L}_\infty$ and $U\in\mathcal{U}_\infty$ such that $B=LU$.*

Proof. First we assume that B generates a digital $(0,1)$-sequence in base b. Then it follows from Lemma 2.4 that $(J_m, B^{(m)})$ generates $(0,m,2)$-net for every $m \in \mathbb{N}$. Thus by Lemma 2.5 there exist unique $L_m \in \mathcal{L}_m$ whose diagonal entries are one and $U_m \in \mathcal{U}_m$ such that $B^{(m)} = L_m U_m$. By comparing the upper left $n \times n$ submatrix of this equation for $n \leq m$, we have $L_m^{(n)} = L_n$ and $U_m^{(n)} = U_n$ for all $n \leq m$. This implies that there exists unique $L \in \mathcal{L}_\infty$ and $U \in \mathcal{U}_\infty$ such that $L^{(m)} = L_m$ and $U^{(m)} = U_m$ holds for all m, and hence we have $B = LU$. This shows the "only if" part. The converse holds from Lemma 2.2 and the fact that I generates a digital $(0,1)$-sequence in base b. □

In the rest of the section, we focus on digital nets over $\mathbb{F}_2$. The first author and Larcher essentially determined all digital $(0,2)$-sequences in base 2 generated by non-singular infinite upper-triangular matrices [4, Proposition 4]. The following two auxiliary results are mainly based on this result, whose proof essentially needs the restriction to a finite field with just two elements. Thus a generalization of our theorems in this paper to a more arbitrary finite field would need a generalization of [4, Proposition 4]. We would like to keep this task for future research.

Lemma 2.8. *Let $U_1, U_2 \in \mathcal{U}_m$. Then (J_m, U_1, U_2) generates $(0,m,3)$-net in base 2 if and only if $U_2 = P_m U_1$ holds.*

Proof. The "only if" part is essentially derived in the proof of [4, Proposition 4]. Now we assume $U_2 = P_m U_1$. From the construction in [2] and Lemma 2.3, (J, I, P) generates a $(0,m,3)$-net. Then it follows from Lemma 2.1 with

$$(L_1, L_2, L_3) = (JU_1^{-1}J, I, I) \quad \text{and} \quad G = U_1$$

that

$$\big((JU_1^{-1}J)JU_1, IU_1, PU_1\big) = (J, U_1, PU_1)$$

also generates a $(0,m,3)$-net. Thus we have proved the converse. □

Proposition 2.9. *Let $U_1, U_2 \in \mathcal{U}_\infty$. Then the following are equivalent:*

(i) *(U_1, U_2) generates a digital $(0,2)$-sequence in base 2.*
(ii) *$U_2 = P_\infty U_1$ holds.*

Proof. (i) implies (ii) by [4, Proposition 4].
The converse follows from Lemma 2.2 and the construction in [2]. □

3. Proofs of Theorem 1.1 and 1.2

Having all the auxiliary results of the previous section at hand, the proofs of our theorems are rather short. In the proofs, for matrices

$$Q, R, S \in \mathbb{F}_2^{m\times m}$$

let $t(Q, R, S)$ be the t-value of the digital net generated by (Q, R, S).

P r o o f o f T h e o r e m 1.1. Let $M = JC_1$. By putting

$$C_2' = C_2 M^{-1} \quad \text{and} \quad C_3' = C_3 M^{-1},$$

$$t(C_1, C_2, C_3) = 0 \quad \text{is equivalent to} \quad t(JM, C_2'M, C_3'M) = 0,$$

which is equivalent to

$$t(J, C_2', C_3') = 0$$

by Lemma 2.1. Hence Theorem 1.1 reduces to the case $C_1 = J$, i.e., it suffices to show the following claim.

Proposition 3.1. *Let $m \geq 1$ be an integer and*

$$C_1, C_2 \in \mathbb{F}_2^{m\times m}.$$

Then the following are equivalent.

(i) (J, C_1, C_2) *generates a* $(0, m, 3)$*-net in base* 2.

(ii) *There exist*

$$L_1, L_2 \in \mathcal{L}_m \quad \textit{and} \quad U \in \mathcal{U}_m$$

such that

$$C_1 = L_1 U \quad \textit{and} \quad C_2 = L_2 P U.$$

We now prove Proposition 3.1. First we assume (ii). By Lemma 2.1 with

$$(L_1, L_2, L_3) = (I, L_1^{-1}, L_2^{-1}) \quad \text{and} \quad G = I$$

we have

$$\begin{aligned} t(J, C_1, C_2) &= t(J, L_1 U, L_2 P U) \\ &= t(J, U, PU) = 0, \end{aligned}$$

where the last equality follows from Lemma 2.8. Thus we have (i).

We now assume (i). By Lemma 2.5, there exist

$$L_1, L_2 \in \mathcal{L}_m \quad \text{and} \quad U_1, U_2 \in \mathcal{U}_m$$

such that

$$C_1 = L_1 U_1 \quad \text{and} \quad C_2 = L_2 U_2.$$

Hence, by Lemma 2.1 with

$$(L_1, L_2, L_3) = (I, L_1, L_2) \quad \text{and} \quad G = I$$

we have

$$\begin{aligned} t(J, U_1, U_2) &= t(J, L_1U_1, L_2U_2) \\ &= t(J, C_1, C_2) = 0. \end{aligned}$$

Finally, Lemma 2.8 implies $U_2 = PU_1$, which shows (ii). □

P r o o f o f T h e o r e m 1.2. (ii) implies (i) by Lemma 2.2 and Proposition 2.9. Let us now assume (i). Then by Lemma 2.7 there exist

$$L_1,\, L_2 \in \mathcal{L}_\infty \quad \text{and} \quad U_1,\, U_2 \in \mathcal{U}_\infty$$

such that

$$C_1 = L_1U_1 \quad \text{and} \quad C_2 = L_2U_2.$$

We apply Lemma 2.2 and obtain that (U_1, U_2) generates a $(0, 2)$-sequence in base 2. Finally Proposition 2.9 brings

$$U_2 = P_\infty U_1$$

and the result follows. □

REFERENCES

[1] DICK, J.—PILLICHSHAMMER, F.: *Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration*. Cambridge University Press, Cambridge, 2010.

[2] FAURE, H.: *Discrépance de suites associées à un système de numération (en dimension s)*, Acta Arith. **41** (1982), 337–351.

[3] FAURE, H.—TEZUKA, S.: *Another random scrambling of digital (t, s)-sequences*. In: *Monte Carlo and Quasi-Monte Carlo Methods 2000*, (K. T. Fang et. al, eds.), Springer--Verlag, Berlin, 2002, pp. 242–256.

[4] HOFER, R.—LARCHER, G.: *On existence and discrepancy of certain digital Niederreiter-Halton sequences,* Acta Arith. **141** (2010), 369–394.

[5] KAJIURA, H.—MATSUMOTO, M.—SUZUKI, K.: *Characterization of matrices B such that (I, B, B^2) generates a digital net with t-value zero,* Finite Fields Appl. **52** (2018), 289–300.

[6] LOH, W. L.: *On the asymptotic distribution of scrambled net quadrature,* Ann. Statist. **31** (2003), 1282–1324.

[7] NIEDERREITER, H.: *Point sets and sequences with small discrepancy,* Monatsh. Math. **104** (1987), 273–337.

[8] ——— *Random Number Generation and Quasi-Monte Carlo Methods*. In: *CBMS-NSF Regional Conference Series, Applied Mathematics* Vol. 63, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.

[9] SOBOĽ, I. M.: *Distribution of points in a cube and approximate evaluation of integrals*, Ž. Vyčisl. Mat. i Mat. Fiz. **7** (1967), 784–802. (In Russian)

[10] TEZUKA, S.: *A Generalization of Faure Sequences and its Efficient Implementation*, Research Report IBM RT0105 (1994), 1–10.
Retrieved as a preprint 2nd of August 2018 from
`https://www.researchgate.net/publication/311808492_A_generalization_of_Faure_sequences_and_its_efficient_implementation`

Received June 11, 2018
Accepted August 22, 2018

Roswitha Hofer
Institute of Financial Mathematics and Applied Number Theory
Johannes Kepler University Linz
Altenbergerstr. 69, 4040 Linz
AUSTRIA
E-mail: roswitha.hofer@jku.at

Kosuke Suzuki
Graduate School of Science
Hiroshima University
1-3-1 Kagamiyama
Higashi-Hiroshima, 739-8526
JAPAN

JSPS Research Fellow
E-mail: kosuke-suzuki@hiroshima-u.ac.jp