Period Math Hung (2017) 74:79–87
DOI 10.1007/s10998-016-0143-2

On the pseudorandomness of quaternary sequences derived from sequences over $\mathbb{F}_4$

Ming Su[1] · **Arne Winterhof**[2]

Published online: 21 July 2016

Abstract In analogy to the corresponding measures of pseudorandomness for quaternary sequences introduced by Mauduit and Sárközy (for m-ary sequences) we introduce the well-distribution measure and correlation measure of order k for sequences over $\mathbb{F}_4$. Using any fixed bijection from $\mathbb{F}_4$ to the set of complex fourth roots of unity, we analyze the relation of these pseudorandomness measures for sequences over $\mathbb{F}_4$ and for the corresponding quaternary sequences. More precisely, we show that they differ only by a multiplicative constant (depending only on k). We also apply the results for deriving new quaternary pseudorandom sequences from pseudorandom sequences over $\mathbb{F}_4$ and vice versa.

Keywords Quaternary sequences · Pseudorandomness · Well-distribution measure · Correlation measure

Mathematics Subject Classification 11B50 · 94A55 · 11K36

1 Introduction

Sequences with ideal pseudorandomness properties have been widely used in wireless communication and cryptography, such as radar and stream cipher cryptosystems. For the sake of simplicity of implementation, binary and quadriphase sequences are preferred for most applications. Pseudorandom binary sequences have been extensively studied, see for example [2]. However, results on the pseudorandomness of quaternary sequences are comparatively

✉ Arne Winterhof
arne.winterhof@oeaww.ac.at

Ming Su
nksuker@gmail.com

[1] Department of Computer Science, Nankai University, Tianjin 300071, People's Republic of China

[2] Johann Radon Institute for Computational and Applied Mathematics, Altenberger Straße 69, 4040 Linz, Austria

rare, which motivates us to investigate the pseudorandomness of sequences defined over four symbols.

Let $\mathbb{F}_4 = \{0, 1, \rho, \rho^2\}$ be the finite field of four elements, where $\rho^2 = \rho + 1$, and $A_N = (\alpha_1, \alpha_2, \ldots, \alpha_N) \in \mathbb{F}_4^N$ be a sequence of length N. Let $\mathcal{E} = \{1, -1, i, -i\}$ be the set of complex fourth roots of unity. There is a close relationship between sequences over $\mathbb{F}_4$ and quaternary sequences over $\mathcal{E}$. We address that our results hold true for any bijection from $\mathbb{F}_4$ to $\mathcal{E}$. However, we have to fix one. We use the bijection defined as follows.

Let ψ denote the additive canonical character of $\mathbb{F}_4$, that is

$$\psi(0) = \psi(1) = 1 \quad \text{and} \quad \psi(\rho) = \psi(\rho^2) = -1.$$

Since $\{\rho, \rho^2\}$ is a basis of $\mathbb{F}_4$ over $\mathbb{F}_2$, we can split A_N into two sequences $(a_1, a_2, \ldots, a_N)$ and $(b_1, b_2, \ldots, b_N)$ over $\mathbb{F}_2$ defined by

$$\alpha_n = a_n\rho + b_n\rho^2, \quad n = 1, 2, \ldots, N. \tag{1.1}$$

Then we derive two sequences $E_N = (e_1, e_2, \ldots, e_N)$ and $F_N = (f_1, f_2, \ldots, f_N)$ over $\{-1, 1\}$ by

$$e_n = (-1)^{a_n} \quad \text{and} \quad f_n = (-1)^{b_n}, \quad n = 1, 2, \ldots, N. \tag{1.2}$$

Note that

$$e_n = \psi(\rho\alpha_n) \quad \text{and} \quad f_n = \psi(\rho^2\alpha_n), \quad n = 1, 2, \ldots, N. \tag{1.3}$$

We get a quaternary sequence $G_N = (g_1, g_2, \ldots, g_N)$ over $\mathcal{E}$ by

$$g_n = \frac{1+i}{2}e_n + \frac{1-i}{2}f_n, \quad n = 1, 2, \ldots, N. \tag{1.4}$$

Conversely, from $G_N = (g_1, g_2, \ldots, g_N) \in \mathcal{E}^N$ we derive two binary sequences $E_N = (e_1, e_2, \ldots, e_N)$ and $F_N = (f_1, f_2, \ldots, f_N) \in \{-1, 1\}^N$ by

$$e_n = \frac{(1-i)g_n + (1+i)\overline{g_n}}{2}, \quad n = 1, 2, \ldots, N, \tag{1.5}$$

and

$$f_n = \frac{(1+i)g_n + (1-i)\overline{g_n}}{2} \quad n = 1, 2, \ldots, N, \tag{1.6}$$

where $\overline{x}$ denotes the complex conjugate of a complex number x. Then we derive two binary sequences by (1.2) and reconstruct $A_N = (\alpha_1, \alpha_2, \ldots, \alpha_N)$ over $\mathbb{F}_4$ by (1.1).

Note that a similar approach for sequences over $\mathbb{F}_4$ was also considered in [3] for finding a set of sequences with low correlation value in wireless communication applications. However, we focus on cryptographic applications and deal also with correlation of higher order.

Mauduit and Sárközy introduced several measures of pseudorandomness of m-ary sequences [5,6]. We focus on binary and quaternary sequences.

Let $E_N = (e_1, e_2, \ldots, e_N) \in \{-1, 1\}^N$ be a finite binary sequence. Then the *well-distribution measure* of E_N is defined as

$$W(E_N) = \max_{M,u,v} \left| \sum_{j=0}^{M-1} e_{u+jv} \right|,$$

where the maximum is taken over all M, u, v with $1 \le u \le u + (M-1)v \le N$, and the *correlation measure of order k* of E_N is defined as

$$C_k(E_N) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_k} \right|,$$

where the maximum is taken over all $D = (d_1, d_2, \ldots, d_k)$ and M such that $0 \le d_1 < d_2 < \ldots < d_k \le N - M$.

In the case of quaternary sequences we have the following analogues.

Let $\mathcal{D}$ be the set of the 24 permutations of $\mathcal{E}$. For a quaternary sequence $G_N = (g_1, g_2, \ldots, g_N) \in \mathcal{E}^N$ the *well-distribution measure* of G_N is defined as

$$\Delta(G_N) = \max_{\tilde{\varphi}, M, u, v} \left| \sum_{j=0}^{M-1} \tilde{\varphi}(g_{u+jv}) \right|,$$

where the maximum is taken over all $\tilde{\varphi} \in \mathcal{D}$ and M, u, v with $1 \le u \le u + (M-1)v \le N$, and the *correlation measure of order k* of G_N is defined as

$$\Gamma_k(G_N) = \max_{\Phi, M, D} \left| \sum_{n=1}^{M} \tilde{\varphi}_1(g_{n+d_1}) \tilde{\varphi}_2(g_{n+d_2}) \cdots \tilde{\varphi}_k(g_{n+d_k}) \right|,$$

where the maximum is taken over all $\Phi = (\tilde{\varphi}_1, \tilde{\varphi}_2, \ldots, \tilde{\varphi}_k) \in \mathcal{D}^k$, $D = (d_1, d_2, \ldots, d_k)$ and M such that $0 \le d_1 < d_2 < \ldots < d_k \le N - M$.

We also define the *crosscorrelation measure* $C_k(H_1, \ldots, H_k)$ of k binary sequences $H_1 = (h_{1,1}, h_{2,1}, \ldots, h_{N,1})$, $H_2 = (h_{1,2}, h_{2,2}, \ldots, h_{N,2}), \ldots,$
$H_k = (h_{1,k}, h_{2,k}, \ldots, h_{N,k}) \in \{-1, 1\}^N$ by

$$C_k(H_1, \ldots, H_k) = \max_{M, D} \left| \sum_{n=1}^{M} h_{n+d_1,1} h_{n+d_2,2} \cdots h_{n+d_k,k} \right|,$$

where the maximum is taken over all $D = (d_1, d_2, \ldots, d_k)$ and M such that $0 \le d_1 \le d_2 \le \ldots \le d_k \le N - M$ and $d_i < d_{i+1}$ if $H_i = H_{i+1}$. (Note that if $H_1 = H_2 = \ldots = H_k = H$ we have $C_k(H_1, H_2, \ldots, H_k) = C_k(H)$.)

In case of sequences defined over $\mathbb{F}_4$ (or any alphabet of size 4), Mauduit and Sárközy introduced closely related figures of merit [6]. Write

$$x(A_N, \alpha, M, u, v) = |\{j : 0 \le j \le M - 1, \alpha_{u+jv} = \alpha\}|$$

and for $w = (\theta_1, \ldots, \theta_k) \in \mathbb{F}_4^k$ and $D = (d_1, \ldots, d_k)$ with non-negative integers $d_1 < \ldots < d_k$,

$$g(A_N, w, M, D) = |\{n : 1 \le n \le M, (\alpha_{n+d_1}, \ldots, \alpha_{n+d_k}) = w\}|.$$

Then the *f-well-distribution measure* (f for frequency) of A_N is defined as

$$\delta(A_N) = \max_{\alpha, M, u, v} \left| x(A_N, \alpha, M, u, v) - \frac{M}{4} \right|, \tag{1.7}$$

where the maximum value is taken over all $\alpha \in \mathbb{F}_4$ and u, v, M with $1 \le u \le u + (M-1)v \le N$, while the *f-correlation-measure of order k* of A_N is defined as

$$\gamma_k(A_N) = \max_{w, M, u, v} \left| g(A_N, w, M, u, v) - \frac{M}{4^k} \right|, \tag{1.8}$$

where the maximum is taken over all $w \in \mathbb{F}_4^k$, $D = (d_1, \ldots, d_k)$, and M such that $M + d_k \le N$.

We also introduce different measures for sequences over $\mathbb{F}_4$ which consider the additive structure of $\mathbb{F}_4$. Denote by $\mathcal{F}$ the set of the 24 permutations of $\mathbb{F}_4$. For a sequence $A_N = (\alpha_1, \alpha_2, \ldots, \alpha_N) \in \mathbb{F}_4^N$, we define the *well-distribution measure* of A_N as

$$W(A_N) = \max_{\lambda, M, u, v} \left| \sum_{j=0}^{M-1} \psi(\lambda(\alpha_{u+jv})) \right|, \tag{1.9}$$

where the maximum is taken over all $\lambda \in \mathcal{F}$ and M, u, v with $1 \le u \le u + (M-1)v \le N$, and we define the *correlation measure of order* k of A_N as

$$C_k(A_N) = \max_{\Lambda, M, D} \left| \sum_{n=1}^{M} \psi(\lambda_1(\alpha_{n+d_1}))\psi(\lambda_2(\alpha_{n+d_2})) \cdots \psi(\lambda_k(\alpha_{n+d_k})) \right|, \tag{1.10}$$

where the maximum is taken over all $\Lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathcal{F}^k$, $D = (d_1, \ldots, d_k)$ and M such that $0 \le d_1 < d_2 < \ldots < d_k \le N - M$.

In this paper we study the relation of the pseudorandomness measures for a sequence A_N over $\mathbb{F}_4$ and for its corresponding quaternary sequence G_N. In Sect. 2, we prove that the proposed definitions of well-distribution measure (1.9) and correlation measure of order k (1.10) are up to a multiplicative constant (depending only on k) the same as the corresponding f-measures (1.7) and (1.8). In Sect. 3, we study the relation of the well-distribution measures for sequences over $\mathbb{F}_4$ and for their corresponding quaternary sequences, as well as the relation of the correlation measure of order k. The results on well-distribution and correlation measure show that sequences over $\mathbb{F}_4$ and corresponding quaternary sequences linked by any fixed bijection have essentially the same pseudorandomness properties. Finally we apply our results to some explicit sequence constructions in Sect. 4.

Note that the results of this paper do not depend on the particular choice (1.3) and (1.4) of the bijection between $\mathbb{F}_4$ and $\mathcal{E}$ since $\Delta(G_N)$, $W(A_N)$, $\Gamma_K(G_N)$, and $C_k(A_N)$ consider the maxima over all permutations of $\mathbb{F}_4$ and $\mathcal{E}$, respectively. The results hold also true for any other bijection between $\mathbb{F}_4$ and $\mathcal{E}$.

2 Measures for sequences over $\mathbb{F}_4$ and f-measures

In this section we will prove two theorems on the strong connection between the f-measures and our measures for sequences over $\mathbb{F}_4$.

Theorem 2.1 *For $A_N \in \mathbb{F}_4^N$ we have*

$$\frac{4}{3}\delta(A_N) \le W(A_N) \le 4\delta(A_N). \tag{2.1}$$

Proof Clearly for all $\varphi = \psi \circ \lambda$, $\lambda \in \mathcal{F}$, M, u, v we have

$$\begin{aligned}
\Big| \sum_{j=0}^{M-1} \varphi(\alpha_{u+jv}) \Big| &= \Big| \sum_{\alpha \in \mathbb{F}_4} x(A_N, \alpha, M, u, v)\varphi(\alpha) \Big| \\
&= \Big| \sum_{\alpha \in \mathbb{F}_4} \big(x(A_N, \alpha, M, u, v) - \frac{M}{4}\big)\varphi(\alpha) + \frac{M}{4} \sum_{\alpha \in \mathbb{F}_4} \varphi(\alpha) \Big| \\
&= \Big| \sum_{\alpha \in \mathbb{F}_4} \big(x(A_N, \alpha, M, u, v) - \frac{M}{4}\big)\varphi(\alpha) \Big| \\
&\le \sum_{\alpha \in \mathbb{F}_4} \big| x(A_N, \alpha, M, u, v) - \frac{M}{4} \big| \le \sum_{\alpha \in \mathbb{F}_4} \delta(A_N) = 4\delta(A_N),
\end{aligned}$$

which proves the upper bound in (2.1).

By the orthogonality relation

$$\sum_{\beta\in\mathbb{F}_4}\psi(\beta x)=\begin{cases}4, & x=0,\\ 0, & x\neq 0,\end{cases}$$

we have

$$x(A_N,\alpha,M,u,v)=\frac{1}{4}\sum_{\beta\in\mathbb{F}_4}\sum_{j=0}^{M-1}\psi(\beta(\alpha_{u+jv}-\alpha)),$$

thus

$$|x(A_N,\alpha,M,u,v)-\frac{M}{4}|\le\frac{3}{4}\max_{\beta\neq 0}|\sum_{j=0}^{M-1}\psi(\beta\alpha_{u+jv})|\le\frac{3}{4}W(A_N),$$

and the lower bound follows. □

Theorem 2.2 *For $A_N\in\mathbb{F}_4^N$, $k\ge 2$, we have*

$$\frac{C_k(A_N)}{4^k}\le\gamma_k(A_N)<\max_{1\le t\le k}C_t(A_N). \tag{2.2}$$

Proof For $\lambda_i\in\mathcal{F}$ put $\varphi_i=\psi\circ\lambda_i$, $i=1,\dots,k$. For all $\phi=(\varphi_1,\dots,\varphi_k)$, M and $D=(d_1,\dots,d_k)$ we get

$$\begin{aligned}
&\Big|\sum_{n=1}^{M}\varphi_1(\alpha_{n+d_1})\dots\varphi_k(\alpha_{n+d_k})\Big|\\
&=\Big|\sum_{(\theta_1,\dots,\theta_k)\in\mathbb{F}_4^k}g\big(A_N,(\theta_1,\dots,\theta_k),M,D\big)\varphi_1(\theta_1)\cdots\varphi_k(\theta_k)\Big|\\
&\le\sum_{(\theta_1,\dots,\theta_k)\in\mathbb{F}_4^k}\Big|g\big(A_N,(\theta_1,\dots,\theta_k),M,D\big)-\frac{M}{4^k}\Big|\\
&\quad+\frac{M}{4^k}\Big|\sum_{(\theta_1,\dots,\theta_k)\in\mathbb{F}_4^k}\varphi_1(\theta_1)\cdots\varphi_k(\theta_k)\Big|\\
&\le\sum_{w\in\mathbb{F}_4^k}\gamma_k(A_N)+\frac{M}{4^k}\Big|(\sum_{a\in\mathbb{F}_4}\varphi_1(a))\cdots(\sum_{a\in\mathbb{F}_4}\varphi_k(a))\Big|=4^k\gamma_k(A_N),
\end{aligned}$$

which proves the lower bound in (2.2).

For all $(\theta_1,\dots,\theta_k)\in\mathbb{F}_4^k$, M, D we have

$$\begin{aligned}
g(A_N,(\theta_1,\dots,\theta_k),M,D)&=\Big|\big\{n:1\le n\le M,\alpha_{n+d_j}=\theta_j\text{ for }j=1,\dots,k\big\}\Big|\\
&=\sum_{n=1}^{M}\frac{1}{4^k}\prod_{j=1}^{k}\left(\sum_{\beta\in\mathbb{F}_4}\psi(\beta(\alpha_{n+d_j}-\theta_j))\right)
\end{aligned}$$

and thus

$$4^k\left|g(A_N,(\theta_1,\ldots,\theta_k),M,D)-\frac{M}{4^k}\right|$$
$$=\left|\sum_{t=1}^{k}\sum_{1\le i_1<\ldots<i_t\le k}\sum_{\beta_1,\ldots,\beta_t\in\mathbb{F}_4^*}\sum_{n=1}^{M}\psi(\beta_1(\alpha_{n+d_{i_1}}-\theta_{i_1}))\cdots\psi(\beta_t(\alpha_{n+d_{i_t}}-\theta_{i_t}))\right|$$
$$\le\sum_{t=1}^{k}3^t\binom{k}{t}C_t(A_N),$$

which proves the upper bound in (2.2). □

Remark 2.3 The results of this section (and the corresponding definitions) can be easily extended to sequences over any finite field $\mathbb{F}_q$, see the final remarks in Sect. 5 below.

3 Measures for sequences over $\mathbb{F}_4$ and for their corresponding quaternary sequences

In this section, first we will discuss the relationship of the well-distribution measures for sequences over $\mathbb{F}_4$ and for their corresponding quaternary sequences.

Theorem 3.1 *Let $A_N\in\mathbb{F}_4^N$ be a sequence over $\mathbb{F}_4$ and G_N be the quaternary sequence defined by (1.3) and (1.4). Then we have the following relations*

$$\frac{1}{\sqrt{2}}\Delta(G_N)\le W(A_N)\le 3\Delta(G_N).$$

Proof Let $E_N, F_N\in\{-1,1\}^N$ be the two sequences defined by (1.1) and (1.2). Since $\lambda\in\mathcal{F}$ is a permutation over $\mathbb{F}_4$, we have $\lambda(x)=ax^i+b$, where $i\in\{1,2\}$ and $a\in\mathbb{F}_4^*$, $b\in\mathbb{F}_4$. Since $\psi(ax^i+b)=\psi(ax^i)\psi(b)=\pm\psi(ax^i)$ and $\psi(ax^2)=\psi(a^2x)$, we have to consider only three mappings λ with $a\in\{1,\rho,\rho^2\}$ and $i=1$.

Then $\lambda(\alpha_n)\in\{\alpha_n,\rho\alpha_n,\rho^2\alpha_n\}$ and we get $\psi(\alpha_n)=e_nf_n$, $\psi(\rho\alpha_n)=e_n$, $\psi(\rho^2\alpha_n)=f_n$.

Therefore, from (1.9) we derive

$$W(A_N)=\max\{W(E_NF_N),W(E_N),W(F_N)\},$$

and by [4, Theorem 1], we have $W(A_N)\le 3\Delta(G_N)$ and

$\Delta(G_N)\le\sqrt{2}\max\{W(E_NF_N),W(E_N),W(F_N)\}=\sqrt{2}W(A_N)$. □

Remark 3.2 The upper bound can also be obtained by [6, Theorem 1]

$$\frac{4}{3}\delta(G_N)\le\Delta(G_N)\le 4\delta(G_N),$$

Theorem 2.1, and $\delta(G_N)=\delta(A_N)$. However, this approach gives only a slightly weaker lower bound with constant $\frac{1}{3}$ (vs. $\frac{1}{\sqrt{2}}$ in Theorem 3.1).

Next we will discuss the relationship of the correlation measures of order k.

Theorem 3.3 *Let $A_N\in\mathbb{F}_4^N$ and G_N be the quaternary sequence defined by (1.3) and (1.4). Then we have the following relations on the correlation measures of order k*

$$2^{-k/2}\Gamma_k(G_N)\le C_k(A_N)\le 3^k\Gamma_k(G_N).$$

Proof Let $E_N, F_N \in \{-1,1\}^N$ be derived from A_N by (1.3). Since $\psi(\lambda_i(\alpha_n)) \in \{\pm e_n, \pm f_n, \pm e_n f_n\}$ for $\lambda_i \in \mathcal{F}$, we get

$$C_k(A_N) = \max C_k(H_1, \ldots, H_k),$$

where $(H_1, \ldots, H_k) \in \{E_N, F_N, E_N F_N\}^k$.
By [4, Theorem 2], $\max C_k(H_1, \ldots, H_k) \le 3^k \Gamma_k(G_N)$ and
$\Gamma_k(G_N) \le 2^{k/2} \max C_k(H_1, \ldots, H_k)$, which completes the proof. □

4 Examples

Here we apply our results to some standard sequence constructions using trace functions and characters of a finite field.

4.1 From sequences over $\mathbb{F}_4$ to quaternary sequences

Denote by tr the trace function from $\mathbb{F}_{2^{2t}}$ to $\mathbb{F}_4$:

$$\mathrm{tr}(x) = \sum_{j=0}^{t-1} x^{4^j}.$$

Theorem 4.1 *Let $\mathbb{F}_{2^{2t}}$ be the finite field of $q = 2^{2t}$ elements with a positive integer t, $\eta \in \mathbb{F}_q^*$ be a primitive element of $\mathbb{F}_{2^{2t}}$, and $\xi, \sigma \in \mathbb{F}_{2^{2t}}^*$. We define the sequence A_{q-1} by*

$$\alpha_n = \mathrm{tr}\big((\xi \eta^n + \sigma)^{-1}\big), \quad n = 1, \ldots, q-1$$

with the convention $0^{-1} = 0$. Then we have

$$W(A_{q-1}) = O(q^{1/2} \log q) \quad \text{and} \quad C_k(A_{q-1}) = O(k q^{1/2} \log q), \quad k = 2, 3, \ldots$$

Proof Since $\chi = \psi \circ \mathrm{tr}$ is an additive character of $\mathbb{F}_{2^{2t}}$ into $\{-1, +1\}$, for the well distribution measure we have

$$W(A_{q-1}) = \max_{\lambda, M, u, v} \left| \sum_{j=0}^{M-1} \psi\Big(\lambda(\mathrm{tr}((\xi \eta^{u+jv} + \sigma)^{-1}))\Big) \right|,$$

where the maximum is taken over all $\lambda \in \mathcal{F}$ and M, u, v with $1 \le u \le u + (M-1)v \le q-1$. Note that we only need to consider the three permutations $\lambda(x) = \rho^i x$, $i = 0, 1, 2$ and that $\chi(\rho^i x)$ is a nontrivial additive character of $\mathbb{F}_{2^{2t}}$. Hence,

$$W(A_{q-1}) = \max_{\substack{\mu \in \{1, \rho, \rho^2\} \\ M, u, v}} \left| \sum_{j=0}^{M-1} \chi(\mu(\xi \eta^{u+jv} + \sigma)^{-1}) \right|$$

and the correlation measure of order k can be expressed as

$$C_k(A_{q-1}) = \max_{\substack{(\mu_1, \ldots, \mu_k) \in \{1, \rho, \rho^2\}^k \\ M, D}} \left| \sum_{n=1}^{M} \chi\Big(\sum_{j=1}^{k} \mu_j (\xi \eta^{n+d_j} + \sigma)^{-1}\Big) \right|,$$

where the maximum is taken over all $D = (d_1, d_2, \ldots, d_k)$ and M such that $0 \le d_1 < d_2 < \ldots < d_k \le q - 1 - M$. Now the result follows by [7, Theorem 2]. □

We immediately get a corresponding quaternary sequence by (1.4) as follows.

Corollary 4.2 *Let the notations be as above. Then we get a corresponding quaternary sequence G_{q-1} for $n = 1, \ldots, q-1$ by*

$$g_n = \frac{1+i}{2}\psi\left(\rho \mathrm{tr}\left((\xi\eta^n + \sigma)^{-1}\right)\right) + \frac{1-i}{2}\psi\left(\rho^2 \mathrm{tr}\left((\xi\eta^n + \sigma)^{-1}\right)\right).$$

Then we have $\Delta(G_{q-1}) = O(q^{1/2}\log q)$ and $\Gamma_k(G_{q-1}) = O(k2^{k/2}q^{1/2}\log q)$.

Proof By Theorems 3.1, 3.3, and 4.1, we get the upper bounds. □

Remark 4.3 The sequence G_{q-1} behaves essentially like a "truly random" quaternary sequence, see [1].

4.2 From quaternary sequences to sequences over $\mathbb{F}_4$

Let p be a prime with $p \equiv 1 \bmod 4$ and τ a multiplicative character of order 4 of the finite field $\mathbb{F}_p$. Then we define the quaternary sequence $G_{p-1} = (\tau(1), \tau(2), \ldots, \tau(p-1)) \in \mathcal{E}^{p-1}$. By [6, Theorems 1, 2, 3] we have

$$\Delta(G_{p-1}) = O(p^{1/2}\log p) \quad \text{and} \quad \Gamma_k(G_{p-1}) = O(kp^{1/2}\log p).$$

By (1.1), (1.2), (1.5) and (1.6), we derive the sequence $A_{p-1} \in \mathbb{F}_4$ from G_{p-1}. According to Theorems 3.1 and 3.3 we have the following results

$$W(A_{p-1}) = O(p^{1/2}\log p) \quad \text{and} \quad C_k(A_{p-1}) = O(3^k kp^{1/2}\log p).$$

5 Final remarks

Using the canonical additive character of the finite field $\mathbb{F}_q$ we can define well-distribution measure $W(A_N)$ and correlation measure $C_k(A_N)$ of order k for any sequence A_N of length N over $\mathbb{F}_q$. Analogously to Sect. 2 we can prove the following relations to frequency measures $\delta(A_N)$ and $\gamma_k(A_N)$:

$$\frac{q}{q-1}\delta(A_N) \le W(A_N) \le q\delta(A_N), \tag{5.1}$$

$$\frac{C_k(A_N)}{q^k} \le \gamma_k(A_N) < \max_{1\le t\le k} C_t(A_N). \tag{5.2}$$

However, Theorem 3.3 cannot be directly generalized, in particular if q is large. Anyway, combining the results of [6, Theorems 1, 2] with (5.1) and (5.2) we get the following relation to the measures $\Delta(G_N)$ and $\Gamma_k(G_N)$ for corresponding sequences G_N over the qth complex roots of unity $\mathcal{E}_q$ (identified via any fixed bijection between $\mathbb{F}_q$ and $\mathcal{E}_q$):

$$\frac{\Delta(G_N)}{q-1} \le W(A_N) \le (q-1)\Delta(G_N),$$

$$C_k(A_N) < q^k \max_{1\le t\le k} \Gamma_t(G_N), \tag{5.3}$$

$$\Gamma_k(G_N) < q^k \max_{1\le t\le k} C_t(A_N). \tag{5.4}$$

Note that relations as (5.3) and (5.4) are weaker than a possible generalization of Theorem 3.3 in the following sense. If $\Gamma_k(G_N)$ (resp. $C_k(A_N)$) is small but $\Gamma_t(G_N)$ (resp. $C_t(A_N)$) is

large for some $1 \leq t < k$, (5.3) (resp. (5.4)) does not give any bound on $C_k(A_N)$ in terms of $\Gamma_k(G_N)$ (resp. vice versa). However, an analogue of Theorem 3.3 would provide this.

Acknowledgements The first author thanks for the hospitality during his visit to RICAM, Austrian Academy of Science, and for the support by ÖAD Ernst-Mach follow-up scholarship. The second author is partially supported by the Austrian Science Fund FWF Project F5511-N26 which is part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

References

1. G. Bérczi, On finite pseudorandom sequences of k symbols. Period. Math. Hungar. **47**(1–2), 29–44 (2003)
2. K. Gyarmati, Measures of pseudorandomness. Finite fields and their applications. Radon. Ser. Comput. Appl. Math. **11**, 43–64 (2013)
3. S.M. Krone, D.V. Sarwate, Quadriphase sequences for spread-spectrum multiple-access communication. IEEE Trans. Inform. Theory **30**(3), 520–529 (1984)
4. R. Marzouk, A. Winterhof, On the pseudorandomness of binary and quaternary sequences linked by the gray mapping. Period. Math. Hungar. **60**(1), 1–11 (2010)
5. C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the legendre symbol. Acta Arith. **82**(4), 365–377 (1997)
6. C. Mauduit, A. Sárközy, On finite pseudorandom sequences of k symbols. Indag. Math. **13**(1), 89–101 (2002)
7. A. Winterhof, *On the distribution of some new explicit inversive pseudorandom numbers and vectors. Monte Carlo and Quasi-Monte Carlo methods* (Springer, Berlin, 2004), pp. 487–499