GENERALIZED EXPLICIT INVERSIVE GENERATORS OF SMALL p -WEIGHT DEGREE

SARA D. CARDELL, DOMINGO GOMEZ, AND JAIME GUTIERREZ

Abstract. Using rational functions to generate pseudorandom number sequences is a popular research topic. In this paper, we study bounds on additive character sums of a new explicit generator based on rational functions with small $p-$weight degree. This extends the class of functions where a nontrivial character sum bound is known.

1. Introduction

Let p be a prime, n an integer with $n \geq 2$, $q = p^n$ and denote by $\mathbb{F}_q$ the finite field of $q = p^n$ elements. Let $\{\gamma_1, \ldots, \gamma_n\}$ be an ordered basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. For any $0 \leq i \leq q-1$ we define the sequence (ξ_i) by

$$\xi_i = i_1\gamma_1 + \cdots + i_n\gamma_n \tag{1}$$

where

$$i = i_1 + i_2 p + \cdots + i_n p^{n-1}, \qquad i_1, \ldots, i_n \in \{0, \ \ldots, p-1\}.$$

This sequence is extended using the relation $\xi_i = \xi_{i \bmod q}$ for any integer i, and it is called the *additive order*. For any function $A(X)$ from $\mathbb{F}_q$ to $\mathbb{F}_q$, we define the p -ary sequence (s_i) by

$$s_i = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(A(\xi_i)), \qquad i = 0, \ 1, \ 2 \ \ldots \tag{2}$$

where $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(A(\xi_i))$ is the trace of $A(\xi_i) \in \mathbb{F}_q$ over $\mathbb{F}_p$. (s_i) is called a sequence generated by $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(A(X))$ via the additive order and the pseudorandom number generator. $(A(\xi_i))$.

The additive order is related with the Counter (CTR) mode encryption of block ciphers, see [8]. The additive order is different from the conventional order in sequence design, and the randomness properties of the sequences from this order are hard to determine. On the other hand, not any $A(X)$ generates a sequence (s_i) with good pseudorandom properties, see [5].

For $A(X)$ defined for $x \in \mathbb{F}_q$,

$$A(x) = \begin{cases} (\alpha x + \beta)^{-1} & \text{if } \alpha x + \beta \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

$(A(\xi_i))$ is the digital explicit inversive pseudorandom number generator of period q for some $\alpha, \ \beta \in \mathbb{F}_q$, and $\alpha \neq 0$. In [11], Niederreiter and Winterhof introduced

The work of Sara D. Cardell was supported by a grant for research students from the Generalitat Valenciana with reference BFPI/2008/138 and by Spanish grant MTM2008-06674-C02-01.

The work of J. Gutierrez is partially supported in part by the Spanish Ministry of Science, project MTM2011-24678 .

this generator and studied exponential sums

$$\sum_{i=0}^{q-1} \psi\big(\sum_{j=0}^{s-1} \mu_j A(\xi_i + \xi_j)\big), \tag{3}$$

where s is a positive integer, $(\mu_0, \ldots, \mu_{s-1}) \in \mathbb{F}_q^s - (0, \ldots, 0)$ and ψ is a non trivial additive character of $\mathbb{F}_q$. Chen in [1] provided a bound on character sums with two arbitrary lags $0 \leq d_0 < d_1 < q$, i. e.

$$\sum_{i=0}^{q-1} \psi\big(\mu_0 A(\xi_{i+d_0}) + \mu_1 A(\xi_{i+d_1})\big), \quad \text{where } \mu_0, \mu_1 \in \mathbb{F}_q, \text{ and not both zero}$$

and later this result was generalized in [2] for any number of lags. In the same article, the authors proved bounds on linear complexity profile and correlation measure of order k of binary sequences derived from this generator. For more results about this class of generators see [12, 13, 14].

In this paper, we obtain a bound on some additive character sums of sequences generated by a class of functions $A(X)$, which will be introduced in Section 2.

The layout of the paper is the following. The first section is devoted to the preliminaries needed. The main theorem is presented in Section 3 where we prove a bound for the discrepancy and the last part is left for conclusions.

2. Preliminaries

It is clear that the properties of (s_i) are the translation of the properties of $(A(\xi_i))$. One example is *the Erdös-Turan-Koksma inequality*, which relates the discrepancy of a pseudorandom number sequence with character sums defined by the pseudorandom number generator, see [4].

For a non-negative integer m, we define its p -weight as the sum of the coefficients in its p-adic expansion:

$$\sigma_p(m) = m_1 + \ldots + m_l, \text{where } m = m_1 + m_2 p + \ldots + m_l p^{l-1},$$

and $0 \leq m_1, \ldots, m_l \leq p-1$.

Now, given a univariate polynomial $f(X) \in \mathbb{F}_q[X]$, the p -weight degree of the polynomial $f(X)$, $\omega_p(f(X))$, is equal to

$$\omega_p(f(X)) = \max\{\sigma_p(e_1), \ldots, \sigma_p(e_r)\},$$

where $f(X) = \delta_1 X^{e_1} + \ldots + \delta_r X^{e_r}$ and all the coefficients are non-zero.

Through the rest of the paper, the trace function $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ will be of maximum importance. The trace is defined by the following polynomial,

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(X) = X + X^p + \ldots + X^{p^{n-1}}.$$

Additive characters of $\mathbb{F}_q$ are defined through $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ and the additive characters of $\mathbb{F}_p$ are described in the following way,

$$\psi_\alpha(x) = e^{2\pi i \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha x)/p},$$

for many applications and properties of additive characters and the trace function, we recommend the reader to consult [7].

For $\alpha = 0$, this character is called the trivial one and for $\alpha = 1$ the canonical character. For simplicity, we will denote this character by $\psi_1 = \psi$.

In [6], the authors studied the nonlinear recursive pseudorandom number generators and proved a bound on character sums of the following form:

$$\sum_{\xi\in\mathbb{F}_q} \psi_\alpha(f(\xi)), \quad \alpha \neq 0$$

where $f(X)$ is a polynomial with low p -weight degree and satisfies

$$f(X) = \gamma X^d + \overline{f(X)}, \text{ with } \gamma \neq 0,\ \omega_p(\overline{f(X)}) < \sigma_p(d). \tag{4}$$

We start generalizing this result for rational functions, for which a similar condition as (4) is required for the numerator. We follow the strategy in [3, 6] and define *the traced* and *the normalized* polynomial.

Definition 1. *Let $f(X) \in \mathbb{F}_q[X]$, $\{\gamma_1, \ldots, \gamma_n\}$ be an ordered basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ and let $F(X_1, \ldots, X_n)$ be the multivariate polynomial*

$$F(X_1, \ldots, X_n) = f(X_1\gamma_1 + \ldots + X_n\gamma_n) \bmod (X_1^p - X_1, \ldots, X_n^p - X_n).$$

We define the traced polynomial $F_R(X_1, \ldots, X_n)$ as the only polynomial such that:

$$F_R(X_1, \ldots, X_n) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(F(X_1, \ldots, X_n)) \bmod (X_1^p - X_1, \ldots, X_n^p - X_n).$$

And, we define the normalized polynomial of $f(X)$,

$$F_N(X_1, \ldots, X_n) = \prod_{i=0}^{n-1} (F(X_1, \ldots, X_n))^{p^i} \bmod (X_1^p - X_1, \ldots, X_n^p - X_n).$$

Notice that the degree on each variable is less than p in both multivariate polynomials $F_R(X_1, \ldots, X_n)$ and $F_N(X_1, \ldots, X_n)$. Also, it is easy to prove that $F_N(X_1, \ldots, X_n)$ has coefficients over the prime field $\mathbb{F}_p$. The following result shows that its degree is n times the p -weight degree of $f(X)$ if this number is strictly less than p.

Lemma 1. *Let $f(X) \in \mathbb{F}_q[X]$, then the following holds,*

- *$F_R(X_1, \ldots, X_n) \in \mathbb{F}_p[X_1, \ldots, X_n]$ and the degree of the transformed polynomial is at most $\omega_p(f(X))$,*
- *$F_N(X_1, \ldots, X_n) \in \mathbb{F}_p[X_1, \ldots, X_n]$ and if $n\omega_p(f(X)) < p$ then the degree of is $n\omega_p(f(X))$.*

Proof. The first bullet of this lemma was proved in [6]. For the second part, we start noticing that

$$\prod_{i=0}^{n-1} (F(X_1, \ldots, X_n))^{p^i} = \prod_{i=1}^{n} (F(X_1, \ldots, X_n))^{p^i} \bmod (X_1^p - X_1, \ldots, X_n^p - X_n) = F_N(X_1, \ldots, X_n)^p \bmod (X_1^p - X_1, \ldots, X_n^p - X_n),$$

which clearly implies that $F_N(X_1, \ldots, X_n) \in \mathbb{F}_p[X_1, \ldots, X_n]$. The only thing that remains is to calculate the degree of $F_N(X_1, \ldots, X_n)$. Clearly, if $p > n\omega_p(f(X))$, then the degree of

$$f(X_1\gamma_1^{p^i} + \cdots + X_n\gamma_n^{p^i}) = F(X_1, \ldots, X_n)^{p^i} \bmod (X_1^p - X_1, \ldots, X_n^p - X_n)$$

is $\omega_p(f(X))$ and the degree of $F_N(X_1, \ldots, X_n)$ is $n\omega_p(f(X))$. □

The interest of the traced polynomial relies on the fact that, under certain assumptions, the total degree of the traced polynomial of a given one coincides with the p -weight degree of the original polynomial $f(X)$.

We consider the following property of a positive integer $D < q$:

$$\text{For all } t \mid n \text{ with } t < n, \implies \frac{q-1}{p^t-1} \not| D. \tag{5}$$

This is equivalent to $\mathbb{F}_q = \mathbb{F}_p(\xi^D)$ for some $\xi \in \mathbb{F}_q$.

We have introduced the necessary tools to prove bounds on the following character sum,

$$\sum_{\xi \in \mathbb{F}_q} \psi_\alpha \left(\frac{f(\xi)}{g(\xi)} \right), \quad \alpha \neq 0$$

with some restrictions on $f(X)$, $g(X)$ and for that we cite [6, Lemma 3], which appeared in [3] and an additive character sum bound from [9].

Lemma 2. *Let $f(X) \in \mathbb{F}_q[X]$ be of the form (4) with $D = d < q$ satisfying (5). Then, the degree of the transformed polynomial $F_R(X_1, \ldots, X_n)$ is $\sigma_p(d)$.*

Theorem 1. *Let Ψ_p be a nontrivial additive character of $\mathbb{F}_p$, and let $f(X)/g(X)$ be a rational function over $\mathbb{F}_p$ that is not constant. Let v be the number of distinct roots of the polynomial $g(X)$ in the algebraic closure of $\mathbb{F}_p$, then*

$$\left| \sum_{\xi \in \mathbb{F}_p,\ g(\xi) \neq 0} \Psi_p \left(\frac{f(\xi)}{g(\xi)} \right) \right| \leq (\max(\deg(f), \deg(g)) + v^* - 2)\ p^{1/2} + \delta,$$

where $v^* = v$ and $\delta = 1$ if $\deg(f) \leq \deg(g)$, otherwise $v^* = v + 1$ and $\delta = 0$.

The following lemma is a technical result about the existence of a special transformation.

Lemma 3. *Let $F(X_1, \ldots, X_n),\ G(X_1, \ldots, X_n) \in \mathbb{F}_p\ [X_1, \ldots, X_n]$ with $\deg(F(X_1, \ldots, X_n)) = d < p/2$ and $\deg(G(X_1, \ldots, X_n)) = d' < p/2$, there exist $a_1, \ldots, a_{n-1} \in \mathbb{F}_p$ such that*

$$\begin{aligned} F(X_1, X_2 + a_1X_1, \ldots, X_n + a_{n-1}X_1) &= \xi X_1^d + \overline{F(X_1, \ldots, X_n)}, \\ G(X_1, X_2 + a_1X_1, \ldots, X_n + a_{n-1}X_1) &= \xi' X_1^{d'} + \overline{G(X_1, \ldots, X_n)} \end{aligned}$$

where $\xi,\ \xi' \neq 0$ and the degree of $\overline{F(X_1, \ldots, X_n)}$ and $\overline{G(X_1, \ldots, X_n)}$ in X_1 are strictly smaller than d, d' respectively.

Proof. We introduce the new variables $Z_1, \ldots, Z_{n-1}$ and consider the following polynomials,

$$F(X_1, Z_1X_1 + X_2, \ldots, Z_{n-1}X_1 + X_n),\ G(X_1, Z_1X_1 + X_2, \ldots, Z_{n-1}X_1 + X_n).$$

Represented as a polynomial in the variable X_1,

$$\begin{aligned} F(X_1, Z_1X_1 + X_2, \ldots, Z_{n-1}X_1 + X_n) = \\ F_1(Z_1, \ldots, Z_{n-1})X_1^d + F_2(Z_1, \ldots, Z_{n-1}, X_1, \ldots, X_n) \end{aligned}$$

where the degree of $F_1(Z_1,\ldots,Z_{n-1})$ is at most d and the degree in the variable X_1 of F_2 is strictly less than d. The same applies for

$$G(X_1, Z_1X_1+X_2,\ldots,Z_{n-1}X_1+X_n) = \\ G_1(Z_1,\ldots,Z_{n-1})X_1^{d'} + G_2(Z_1,\ldots,Z_{n-1},X_1,\ldots,X_n).$$

Notice that the degree of the product $G_1(Z_1,\ldots,Z_{n-1})F_1(Z_1,\ldots,Z_{n-1})$ is at most $d+d'$, strictly less than p. Therefore, there exists $a_1,\ldots,a_{n-1}\in\mathbb{F}_p$ such that,

$$G_1(a_1,\ldots,a_{n-1})F_1(a_1,\ldots,a_{n-1})\neq 0.$$

In other words, $F(X_1, X_2+a_1X_1,\ldots,X_n+a_{n-1}X_1)$ has degree d in the variable X_1. Notice also that the polynomial has total degree d, it means that

$$F(X_1, X_2+a_1X_1,\ldots,X_n+a_{n-1}X_1) = \xi X_1^d + \overline{F(X_1,\ldots,X_n)},$$

where the degree on X_1 of $\overline{F(X_1,\ldots,X_n)}$ is strictly less than d. A similar argument applies to $G(X_1, X_2+a_1X_1,\ldots,X_n+a_{n-1}X_1)$ and this finishes the proof. □

We are ready to prove the following result.

Lemma 4. *Let ψ_α be a nontrivial additive character of $\mathbb{F}_q$, and $f(X), g(X)\in\mathbb{F}_q[X]$ $\gcd(f(X),g(X))=1$ with $\deg(f(X))$, $\deg(g(X))<q/2$ and satisfying*

$$f(X) = g(X)X^d + \overline{f(X)},\ \text{with } \omega_p(\overline{f(X)}) < \sigma_p(d)+\omega_p(g(X)), \tag{6}$$

and $d=D$ satisfying (5). Then,

$$\left|\sum_{\xi\in\mathbb{F}_q}\psi_\alpha\left(\frac{f(\xi)}{g(\xi)}\right)\right| \leq (\max(\sigma_p(d),\omega_p(g(X))) + n\ \omega_p(g(X)) - 1)\ p^{n-1/2}+1.$$

Proof. Without loss of generality, we can suppose that

$$\max(\sigma_p(d),\omega_p(g(X))) + n\ \omega_p(g(X)) - 1 \leq p^{1/2}. \tag{7}$$

The strategy to follow is to transform our initial sum in order to apply the result in Theorem 1.

We start from the definition of our sum and transform it to a sum in several variables,

$$\left|\sum_{\xi\in\mathbb{F}_q}\psi_\alpha\left(\frac{f(\xi)}{g(\xi)}\right)\right| = \left|\sum_{x_1,\ldots,x_n\in\mathbb{F}_p}\Psi_p\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(\alpha\frac{F(x_1,\ldots,x_n)}{G(x_1,\ldots,x_n)}\right)\right)\right| = \\ \left|\sum_{x_1,\ldots,x_n\in\mathbb{F}_p}\Psi_p\left(\frac{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha F(x_1,\ldots,x_n)G(x_1,\ldots,x_n)^{p+p^2+\ldots+p^{n-1}})}{G_N(x_1,\ldots,x_n)}\right)\right|,$$

where Ψ_p is the canonical additive character of $\mathbb{F}_p$.

We transform this sum to the same type as the one that appears in Theorem 1 for variable x_1. Now, $f(X)=g(X)X^d+\overline{f(X)}$, so

$$\frac{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha F(X_1,\ldots,X_n)G(X_1,\ldots,X_n)^{p+p^2+\ldots+p^{n-1}})}{G_N(X_1,\ldots,X_n)} = \\ E_R(X_1,\ldots,X_n) + \frac{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha\overline{F(X_1,\ldots,X_n)}G(X_1,\ldots,X_n)^{p+p^2+\ldots+p^{n-1}})}{G_N(X_1,\ldots,X_n)},$$

where $E_R(X_1,\ldots,X_n)$ is the traced polynomial of αX^d. The traced polynomial is not the zero polynomial, otherwise

$$E_R(X_1,\ldots,X_n)G_N(X_1,\ldots,X_n) = \\ -\operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha\overline{F(X_1,\ldots,X_n)}G(X_1,\ldots,X_n)^{p+p^2+\ldots+p^{n-1}}).$$

By Lemma 2, the degree of $E_R(X_1,\ldots,X_n)$ is $\sigma_p(d)$ and by Lemma 1 and Equation (7), $n\omega_p(g(X)) + \sigma_p(d)$ is is strictly greater than the degree of the traced polynomial of $\alpha\overline{F(X_1,\ldots,X_n)}G(X_1,\ldots,X_n)^{p+p^2+\ldots+p^{n-1}}$. Let's call

$$F_R(X_1,\ldots,X_n) = \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha F(X_1,\ldots,X_n)G(X_1,\ldots,X_n)^{p+p^2+\ldots+p^{n-1}}).$$

Selecting $a_1,\ldots,a_{n-1}$ as in Lemma 3 and for $x_1,\ldots,x_n \in \mathbb{F}_p$ we have that

$$F_R(x_1, x_2 + a_1x_1\ldots, x_n + a_{n-1}x_1) = \\ \xi'' x_1^{\sigma_p(d)+n\omega_p(g(X))} + \overline{F_R(x_1, x_2 + a_1x_1\ldots, x_n + a_{n-1}x_1)},$$

where $\xi'' \neq 0$, $\overline{F_R}$ has degree in variable X_1 strictly less than $\sigma_p(d) + n\omega_p(g(X))$ and

$$G_N(x_1, x_2 + a_1x_1\ldots, x_n + a_{n-1}x_1) = \\ \xi''' x_1^{n\ \omega_p(g(X))} + \overline{G_N(x_1, x_2 + a_1x_1\ldots, x_n + a_{n-1}x_1)},$$

where $\xi'' \neq 0$, $\overline{G_N}$ has degree in variable X_1 strictly less than $n\ \omega_p(g(X))$. Now,

$$\left|\sum_{x_1,\ldots,x_n\in\mathbb{F}_p} \Psi_p\left(\frac{\operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha F(x_1,\ldots,x_n)G(x_1,\ldots,x_n)^{p+p^2+\ldots+p^{n-1}})}{G_N(x_1,\ldots,x_n)}\right)\right| = \\ \left|\sum_{x_1,\ldots,x_n\in\mathbb{F}_p} \Psi_p\left(\frac{F_R(x_1,\ldots,x_n)}{G_N(x_1,\ldots,x_n)}\right)\right| = \\ \left|\sum_{x_1,\ldots,x_n\in\mathbb{F}_p} \Psi_p\left(\frac{F_R(x_1, x_2 + a_1x_1\ldots, x_n + a_{n-1}x_1)}{G_N(x_1, x_2 + a_1x_1\ldots, x_n + a_{n-1}x_1)}\right)\right| \leq \\ \sum_{x_2,\ldots,x_n\in\mathbb{F}_p}\left|\sum_{x_1\in\mathbb{F}_p} \Psi_p\left(\frac{F_R(x_1, x_2 + a_1x_1\ldots, x_n + a_{n-1}x_1)}{G_N(x_1, x_2 + a_1x_1\ldots, x_n + a_{n-1}x_1)}\right)\right|$$

Applying Theorem 1 for all fixed selections of $x_2,\ldots,x_n$, we have finished. □

3. Main Result

In this Section, we give a bound on the following additive character sum,

$$\sum_{i=0}^{N} \psi_\alpha(A(\xi_i))$$

where $A(X) = f(X)/g(X)$, satisfying the conditions in Equation (6). Before proving the main result, we recall the following result.

Lemma 5. *Suppose $\{\gamma_1, \ldots, \gamma_n\}$ is a fixed basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ and (ξ_i) is the sequence defined in Equation (1), then*

$$\sum_{\beta \in \mathbb{F}_q} \left| \sum_{i=0}^{N} \psi_\alpha(-\beta \xi_i) \right| \leq n^2 q \log p.$$

The proof of this Lemma can be found in [1].

Theorem 2. *Suppose that $A(X) = f(X)/g(X)$, satisfies the conditions in Equation (6) with d satisfying (5) and $\sigma_p(d) \geq 2$. The following bound*

$$\left| \sum_{i=0}^{N} \psi_\alpha(A(\xi_i)) \right| \leq (n^2 \log p)(\max(\sigma_p(d), \omega_p(g(X))) + n\ \omega_p(g(X)) - 1) p^{n-1/2},$$

holds for any $1 \leq N \leq q$.

Proof. We start with the definition of the sum,

$$\begin{aligned}
\left| \sum_{i=0}^{N} \psi_\alpha(A(\xi_i)) \right| &= \left| \sum_{x \in \mathbb{F}_q} \psi_\alpha(A(x)) \left(\frac{1}{q} \sum_{i=0}^{N} \sum_{\beta \in \mathbb{F}_q} \psi_\alpha(\beta(x - \xi_i)) \right) \right| \\
&= \frac{1}{q} \left| \sum_{i=0}^{N} \sum_{\beta \in \mathbb{F}_q} \psi_\alpha(-\beta \xi_i) \sum_{x \in \mathbb{F}_q} \psi_\alpha(A(x) + \beta x) \right| \\
&\leq \frac{1}{q} \sum_{\beta \in \mathbb{F}_q} \left| \sum_{i=0}^{N} \psi_\alpha(-\beta \xi_i) \right| \times \max_{\beta \in \mathbb{F}_q} \left| \sum_{x \in \mathbb{F}_q} \psi_\alpha(A(x) + \beta x) \right|.
\end{aligned}$$

Notice that $A(X) + \beta X = f(X)'/g(X)$, where

$$f(X)' = f(X) + \beta X g(X) = g(X) X^d + \overline{f(X)} + \beta X g(X).$$

still satisfies Equation (6). This is because

$$\max\{\omega_p(\overline{f(X)}), \omega_p(\beta X g(X))\} \ < \ \max\{\sigma_p(d) \ + \ \omega_p(g(X)), \ \ 2 \ + \ \omega_p(g(X))\}$$

So, for the right term of the product, we can apply Lemma 4 and for the left term of the product, we can apply Lemma 5.

Writing everything together, we have

$$\begin{aligned}
&\frac{1}{q} \sum_{\beta \in \mathbb{F}_q} \left| \sum_{i=0}^{N} \psi_\alpha(-\beta \xi_i) \right| \times \max_{\beta \in \mathbb{F}_q} \left| \sum_{x \in \mathbb{F}_q} \psi_\alpha(A(x) + \beta x) \right| \leq \\
&\qquad (n^2 \log p)(\max(\sigma_p(d), \omega_p(g(X))) + n\ \omega_p(g(X)) - 1) p^{n-1/2}.
\end{aligned}$$

This finishes the proof. □

Now, we estimate the discrepancy of the elements of the sequence

$$S_i = \frac{s_i}{p} \in [0, 1), \ i = 0, \ldots, N.$$

We recall that the *discrepancy* of the points $S_0, \ldots, S_N$ denoted by D_N is defined by

$$D_N = \sup_{[\alpha, \beta) \subset [0,1)} \left| \frac{A([\alpha, \beta), N)}{N} - \beta + \alpha \right|$$

where $A([\alpha,\beta),N)$ is the number of points $S_0,\ldots,S_N$ which are contained in the interval $[\alpha,\beta)$ and the supremum is taken over all such intervals, see [10].

Doing straightforward calculations (see the proof of Theorem 1 of [2]) and using Theorem2, it is easy to prove the following theorem.

Theorem 3. *Let $s_0,\ldots,s_N$ the sequence defined by (2). The discrepancy D_N can is of order*

$$\frac{n^4(\log p)^2(\max(\sigma_p(d),\omega_p(g(X))))p^{n-1/2}}{N}$$

where the implied constant is absolute.

4. Conclusions

In this paper we have started the study of a new pseudorandom generator via additive order. We have given a non trivial bound on sequences of the type (2). Apart from that, Lemma 4 generalizes [6, Lemma 4], when $g(X)=1$.

It would be certainly interesting to study the following more general character sum

$$\sum_{i=0}^{N}\psi_\alpha(\alpha_1 A(\xi_{i+1})+\ldots+\alpha_\tau A(\xi_{i+\tau})),$$

where $\alpha_1,\ldots,\alpha_\tau\in\mathbb{F}_q$, not all equal to zero. However, in this case, it is necessary to show that the transformed polynomial is not constant so one can apply Lemma 4. Also, the necessity of (5) for polynomials of the form (4) has been shown in [6].

5. Acknowledgments

Finally, the authors would like to thank Arne Winterhof for proposing the problem and useful discussions.

References

[1] Zhixiong Chen. Finite binary sequences constructed by explicit inversive methods. *Finite Fields Appl.*, 14(3):579–592, 2008.

[2] Zhixiong Chen, Domingo Gomez, and Arne Winterhof. Distribution of explicit digital inversive pseudorandom numbers and applications to some binary sequences. *Accepted in proceedings of The Eighth International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing*, 2008.

[3] Valérie Gillot. Bounds for exponential sums over finite fields. *Finite Fields Appl.*, 1(4):421–436, 1995.

[4] Peter Hellekalek. General discrepancy estimates: the walsh function system. *Acta Aritmetica*, 67:209–218, 1994.

[5] Honggang Hu and Guang Gong. A study on the pseudorandom properties of sequences generated via the additive order. *SETA 2008, Lecture Notes on Computer Science*, 5203:51–59, 2008.

[6] Alvar Ibeas and Arne Winterhof. Exponential sums and linear complexity of nonlinear pseduorandom number generators with polynomials of small p-degree. *Unif. Distrib. Theory*, 5(1):79–93, 2010.

[7] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[8] Helger Lipmaa, Phillip Rogaway, and David Wagner. Comments to nist concerning aes modes of operation: Ctr-mode encryption. In *Symmetric Key Block Cipher Modes of Operation Workshop*, 2000.

[9] Carlos Moreno and Oscar Moreno. Exponential sums and goppa codes. *Proceedings of the American Mathematical Monthly*, 111:523–531, 1991.

[10] 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.
[11] Harald Niederreiter and Arne Winterhof. Incomprete exponential sums over finite fields and their applications to new inversive pseudorandom number generatos. *Acta Aritmetica*, 93:387–399, 2000.
[12] Harald Niederreiter and Arne Winterhof. On a new class of inversive pseudorandom numbers for parallelized simulation methods. *Periodica Mathematica Hungarica*, 42(1–2):77–87, 2001.
[13] Harald Niederreiter and Arne Winterhof. On the lattice structure of pseudorandom numbers generated over arbitrary finite fields. *Appl. Algebra Eng. Commun. Comput.*, 12(3):265–272, 2001.
[14] Gottlieb Pirsic and Arne Winterhof. On the structure of digital explicit nonlinear and inversive pseudorandom number generators. *J. Complexity*, 26(1):43–50, 2010.

Departamento de Estadística e Investigación Operativa. Universidad de Alicante.
E-mail address: s.diaz@ua.es

Departamento de Estadística, Matemáticas y Computación. Universidad de Cantabria.
E-mail address: domingo.gomez@unican.es

Departamento de Matemática Aplicada y Ciencias de la Computación. Estadística. Universidad de Cantabria.
E-mail address: jaime.gutierrez@unican.es