Character sums and nonlinear recurrence sequences

Simon R. Blackburna, Igor E. Shparlinskib

aDepartment of Mathematics, Royal Holloway University of London, Egham, Surrey, TW20 0EX, UK
bDepartment of Computing, Macquarie University, Sydney, NSW 2109, Australia

Received 8 March 2005; received in revised form 6 February 2006; accepted 14 February 2006
Available online 17 April 2006

Abstract

We obtain upper bounds on character sums and autocorrelation of nonlinear recurrence sequences over arbitrary finite rings.

© 2006 Elsevier B.V. All rights reserved.

Keywords: Character sums; Autocorrelation; Nonlinear recurrence sequences; Stream ciphers

1. Introduction

There is an extensive literature devoted to bounds of character sums and linear recurrence sequences, see [1, Chapter 5] and [2, Chapter 8]. Character sums have also been studied in the context of nonlinear recurrence sequences, see [3–5] and references therein. However, they apply only to special classes of such sequences. Typically, such results apply only to sequences of fixed order \( d \) (for example, \( d = 1 \)) defined over a finite but sufficiently large ring. They also require the period of the sequence to be close to its largest possible value.

Here we explore the complementary situation, when the order of the sequence grows (but the ring size may remain bounded). Our method is purely combinatorial and applies to essentially any sequence. However, as in the previously studied situation, the results are non-trivial only for sequences of very large period.

Let \( F(X_1, \ldots, X_d) \) be an arbitrary function in \( d \) variables over a finite ring \( \mathcal{R} \) of \( m \) elements. We assume that \( \mathcal{R} \) has a multiplicative identity. We consider an infinite sequence \( (a_n)_{n=0}^{\infty} \) of elements of \( \mathcal{R} \) satisfying the nonlinear recurrence relation

\[
a_{n+d} = F(a_{d+n-1}, \ldots, a_n), \quad n = 0, 1, \ldots
\]

(1)

Such a sequence can be viewed as the output of the stream cipher associated with \( F \) with the key \( K = (a_0, \ldots, a_{d-1}) \). Thus studying statistical properties of such sequences, in particular their autocorrelation, is of prime interest for cryptography.

It is clear that any sequence satisfying (1) is ultimately periodic with period \( t \). That is, there exists a non-negative integer \( r \) (which we take as small as possible) such that \( a_{n+t} = a_n \) for \( n \geq r \). We write \( T = r + t \) and recall the obvious fact that \( T \leq m^d \).

Let \( \chi(a) \) denote an arbitrary non-trivial additive character of \( \mathcal{R} \). The main aim of this paper is to obtain a non-trivial upper bound on character sums associated with \( (a_n)_{n=0}^{\infty} \) and give various applications for these sums. We may state

\[E-mail addresses: s.blackburn@rhul.ac.uk (S.R. Blackburn), igor@ics.mq.edu.au (I.E. Shparlinski).\]
our main result as follows. Let $h$ be a positive integer and let $u \in \mathbb{R}^{h+1}$, so $u = (u_0, u_1, \ldots, u_h)$. For a positive integer $N$, define the character sums $S(u; N)$ by

$$S(u; N) = \sum_{n=0}^{N-1} \chi(u_0a_n + u_1a_{n+1} + \cdots + u_{h}a_{n+h}).$$

**Theorem 1.** Let $d, T, h$ and $S(u; N)$ be defined as above. Then, for any integer $v \geq 1$, whenever $h < d$ and $N \leq T$, and provided that $u$ is not the all zero vector, we have that

$$|S(u; N)| < v^{1+1/2v}N^{1-1/2v}m^{d/2v}(d - h)^{-1/2} + d - h.$$  

For positive integers $h$ and $N$ we define correlation coefficients by

$$C(h; N) = \sum_{n=0}^{N-1} \chi(a_{n+h} - a_n).$$

When $u = (-1, 0, 0, \ldots, 0, 1)$, it is easy to see that $C(h; N) = S(u; N)$, so Theorem 1 immediately yields:

**Corollary 2.** Let $m, d, T$ and $C(h; N)$ be defined as above. Then, for any integer $v \geq 1$, whenever $h < d$ and $N \leq T$ we have that

$$|C(h; N)| < v^{1+1/2v}N^{1-1/2v}m^{d/2v}(d - h)^{-1/2} + d - h.$$  

Theorem 1 can also be used to study the frequency of the appearance of a prescribed string $(e_0, \ldots, e_{h-1}) \in \mathbb{R}^h$ among the first $N$ windows of $h$ consecutive elements of the sequence $(a_n)_{n=0}^{\infty}$. Namely, let $R(e_0, \ldots, e_{h-1}; N)$ denote the number of $n = 0, \ldots, N - 1$ for which $(a_n, \ldots, a_{n+h-1}) = (e_0, \ldots, e_{h-1})$.

**Theorem 3.** Let $d, T, h$ and $R(e_0, \ldots, e_{h-1}; N)$ be defined as above. Then whenever $h < d$ and $N \leq T$, we have that

$$\left| R(e_0, \ldots, e_{h-1}; N) - \frac{N}{m^h} \right| < v^{1+1/2v}N^{1-1/2v}m^{d/2v}(d - h)^{-1/2} + d - h.$$  

2. Proof of Theorem 1

We begin by defining some more notation. We write $a_n$ for the vector $(a_n, a_{n+1}, \ldots, a_{n+h}) \in \mathbb{R}^{h+1}$. We write $a \cdot b$ for the standard inner product of two vectors $a$ and $b$ in $\mathbb{R}^{h+1}$. With this notation, we may write

$$S(u; N) = \sum_{n=0}^{N} \chi(u \cdot a_n).$$

We also put $f = d - h$.

Let $k$ be a positive integer. Then clearly

$$|S(u; N) - \sum_{n=0}^{N-1} \chi(u \cdot a_{n+k})| = \left| \sum_{n=0}^{k-1} \chi(u \cdot a_n) - \sum_{n=N}^{N+k-1} \chi(u \cdot a_n) \right| \leq 2k.$$  

Using this inequality for $k = 0, \ldots, f - 1$ we find that

$$|S(u; N) - \frac{1}{f} \sum_{k=0}^{f-1} \sum_{n=0}^{N-1} \chi(u \cdot a_{n+k})| \leq \frac{2}{f} \sum_{k=0}^{f-1} k < f.$$
Hence

\[ |S(u; N)| \leq \left| \frac{1}{f} \sum_{k=0}^{f-1} \sum_{n=0}^{N-1} \chi(u \cdot a_{n+k}) \right| + f. \] (2)

Now,

\[ \left| \sum_{k=0}^{f-1} \sum_{n=0}^{N-1} \chi(u \cdot a_{n+k}) \right|^{2v} \leq \left( \sum_{n=0}^{N-1} \left| \sum_{k=0}^{f-1} \chi(u \cdot a_{n+k}) \right| \right)^{2v} \]

\[ \leq N^{2v-1} \sum_{n=0}^{N-1} \left| \sum_{k=0}^{f-1} \chi(u \cdot a_{n+k}) \right|^{2v}, \] (3)

the last bound following by the Hölder inequality. Since \( N \leq T \), the \( d \)-tuples \((a_n, \ldots, a_{n+d-1})\) are pairwise distinct for \( n = 0, \ldots, N - 1 \). Therefore,

\[ \sum_{n=0}^{N-1} \left| \sum_{k=0}^{f-1} \chi(u \cdot a_{n+k}) \right|^{2v} \leq \sum_{c_0, \ldots, c_{d-1} \in \mathcal{R}} \left| \sum_{k=0}^{f-1} \chi(u \cdot c_k) \right|^{2v}, \]

where \( c_k = (c_k, c_{k+1}, \ldots, c_{k+d}) \). But

\[ \sum_{c_0, \ldots, c_{d-1} \in \mathcal{R}} \left| \sum_{k=0}^{f-1} \chi(u \cdot c_k) \right|^{2v} \]

\[ = \sum_{c_0, \ldots, c_{d-1} \in \mathcal{R}} \prod_{j=1}^{v} \left( \sum_{k_j=0}^{f-1} \chi(u \cdot c_{k_j}) \right) \prod_{\ell_j=0}^{f-1} \chi(u \cdot c_{\ell_j}) \]

\[ = \sum_{c_0, \ldots, c_{d-1} \in \mathcal{R}} \prod_{j=1}^{v} \left( \sum_{k_j=0}^{f-1} \chi(u \cdot c_{k_j}) \right) \prod_{\ell_j=0}^{f-1} \chi(-u \cdot c_{\ell_j}) \]

\[ = \sum_{c_0, \ldots, c_{d-1} \in \mathcal{R}} \sum_{k_1, \ldots, k_v=0}^{f-1} \sum_{\ell_1, \ldots, \ell_v=0}^{f-1} \chi \left( \sum_{j=1}^{v} u \cdot (c_{k_j} - c_{\ell_j}) \right). \]

Hence,

\[ \sum_{n=0}^{N-1} \left| \sum_{k=0}^{f-1} \chi(u \cdot a_{n+k}) \right|^{2v} \leq \sum_{k_1, \ldots, k_v=0}^{f-1} \sum_{c_{0}, \ldots, c_{d-1} \in \mathcal{R}} \chi \left( \sum_{j=1}^{v} u \cdot (c_{k_j} - c_{\ell_j}) \right). \] (4)

We now aim to show that the inner character sum on the right-hand side of (4) is zero for most choices of \( k_1, \ldots, k_v \) and \( \ell_1, \ldots, \ell_v \).

Let the (additive) group homomorphism \( \phi : \mathbb{R}^d \to \mathcal{R} \) be defined by

\[ \phi(c_0, c_1, \ldots, c_{d-1}) = \sum_{j=1}^{v} u \cdot (c_{k_j} - c_{\ell_j}). \]
Note that
\[
\sum_{c_0,\ldots,c_{d-1}\in \mathbb{R}} \chi \left( \sum_{j=1}^{v} u \cdot (c_k - c_{\ell_j}) \right) = \sum_{c_0,\ldots,c_{d-1}\in \mathbb{R}} \chi(\phi(c_0, \ldots, c_{d-1}))
\]
where \( \chi \) is the image set of \( \phi \). Thus the sum is equal to 0 if \( \phi \) is non-trivial and is equal to \( m^d \) otherwise.

Define the integer \( j_0 \) by \( j_0 = \min\{j \in \{0, 1, \ldots, h\} : u_j \neq 0\} \), and let \( \kappa \) be the additive order of \( u_{j_0} \). For \( i \in \{0, 1, \ldots, f - 1\} \), define ‘multiplicities’ \( \mu_i \) and \( \eta_i \) by
\[
\mu_i = \#\{ j \in \{1, \ldots, v\} : k_j = i \} \quad \text{and} \quad \eta_i = \#\{ j \in \{1, \ldots, v\} : \ell_j = i \}.
\]
Then it is easy to see that
\[
\phi(c_0, c_1, \ldots, c_{d-1}) = \sum_{i=0}^{f-1} (\mu_i - \eta_i) u_i \cdot c_i
\]
\[
= \sum_{i=0}^{f-1} (\mu_i - \eta_i) \sum_{j=0}^{h} u_j c_{i+j} = \sum_{i=0}^{f-1} (\mu_i - \eta_i) \sum_{j=j_0}^{h} u_j c_{i+j}.
\]
Suppose that there exists \( i \in \{0, 1, \ldots, f - 1\} \) such that \( \mu_i - \eta_i \neq 0 \mod \kappa \). Then \( \phi \) is non-trivial, since if we define
\[
i_0 = \min\{ i \in \{0, 1, \ldots, f - 1\} : \mu_i - \eta_i \neq 0 \mod \kappa \},
\]
we find that
\[
\phi(c_0, c_1, \ldots, c_{d-1}) = (\mu_{i_0} - \eta_{i_0}) u_{j_0} c_{i_0+j_0} + X,
\]
where \( X \) is an expression that does not involve \( c_{i_0+j_0} \). Hence we find that the sum (5) is equal to 0 in this case.

Let \( Q_v \) be the number of choices for the integers \( k_1, \ldots, k_v \) and \( \ell_1, \ldots, \ell_v \) with the property that \( \mu_i - \eta_i \equiv 0 \mod \kappa \) for all \( i \in \{0, 1, \ldots, f - 1\} \). Then, by (4) we have
\[
\sum_{n=0}^{N-1} \sum_{k=0}^{f-1} \left| \chi(u \cdot a_{n+k}) \right|^{2v} \leq Q_v m^d.
\]

We now concentrate on estimating \( Q_v \).

We first bound the number of possibilities for the integers \( \mu_i \) and \( \eta_i \). Define non-negative integers \( s_i, t_i, r_i \) and \( q_i \) by
\[
\mu_i = s_i \kappa + r_i \quad \text{and} \quad \eta_i = t_i \kappa + q_i,
\]
where \( 0 \leq r_i < \kappa \) and \( 0 \leq q_i < \kappa \) for \( i \in \{0, 1, \ldots, f - 1\} \). Since \( \mu_i - \eta_i \equiv 0 \mod \kappa \), we have that \( q_i = r_i \) for \( i \in \{0, 1, \ldots, f - 1\} \). Define
\[
s = \sum_{i=0}^{f-1} s_i.
\]
Since 
\[ \sum_{i=0}^{f-1} \mu_i = v, \]
we have that
\[ s = \sum_{i=0}^{f-1} \lceil \mu_i / \kappa \rceil \leq v / \kappa. \]

Now \( s_0, s_1, \ldots, s_{f-1} \) is a sequence of \( f \) non-negative integers that sum to \( s \), and so there are at most \( f^s \) possibilities for the sequence \( s_0, s_1, \ldots, s_{f-1} \) once \( s \) is fixed. The sequence \( r_0, r_1, \ldots, r_{f-1} \) consists of non-negative integers that sum to \( v - \kappa s \), since
\[ \sum_{i=0}^{f-1} r_i = \sum_{i=0}^{f-1} \mu_i - \kappa \sum_{i=0}^{f-1} s_i = v - \kappa s. \]

Hence there are at most \( f^{v-\kappa s} \) possibilities for \( r_0, r_1, \ldots, r_{f-1} \). Now,
\[ \sum_{i=0}^{f-1} t_i = \frac{1}{\kappa} \left( \sum_{i=0}^{f-1} \eta_i - \sum_{i=0}^{f-1} r_i \right) = \frac{1}{\kappa} \left( v - \sum_{i=0}^{f-1} r_i \right) \]
\[ = \frac{1}{\kappa} \left( \sum_{i=0}^{f-1} \mu_i - \sum_{i=0}^{f-1} r_i \right) = s \]
and so there are at most \( f^s \) possibilities for the sequence \( t_0, t_1, \ldots, t_{f-1} \). The multiplicities \( \mu_i \) and \( \eta_i \) are determined by the integers \( s_i, t_i \) and \( r_i \) and so there are at most
\[ \sum_{s=0}^{\lfloor v/\kappa \rfloor} f^{v-(\kappa-2)s} \]
possibilities for the multiplicities \( \mu_i \) and \( \eta_i \).

The multiplicities \( \mu_i \) determine the elements in the sequence \( k_1, k_2, \ldots, k_v \) up to reordering, and so there are at most \( v! \) possibilities for the sequence \( k_1, k_2, \ldots, k_v \) once the integers \( \mu_i \) are determined. Similarly, there are at most \( v! \) possibilities for the sequence \( \ell_1, \ell_2, \ldots, \ell_v \) once the multiplicities \( \eta_i \) have been fixed. So, to summarise, we have shown that
\[ Q_v \leq (v!)^2 \sum_{s=0}^{\lfloor v/\kappa \rfloor} f^{v-(\kappa-2)s} \leq v(v!)^2 f^v, \]
which, together with (2), (3) and (6), implies the theorem.

3. Proof of Theorem 3

Let \( \chi \) be a fixed non-trivial additive character of \( \mathcal{A} \). From the well known identity
\[ \frac{1}{m} \sum_{u \in \mathcal{A}} \chi(uc) = \begin{cases} 1 & \text{if } c = 0, \\ 0 & \text{otherwise}, \end{cases} \]
we see that
\[ R(e_0, \ldots, e_{h-1}; N) = \frac{1}{m^h} \sum_{n=0}^{N-1} \prod_{j=0}^{h-1} \chi(u_j(a_{n+j} - e_j)) \]

\[ = \frac{1}{m^h} \sum_{n=0}^{N-1} \prod_{j=0}^{h-1} \chi(u_j(a_{n+j} - e_j)) \]

\[ = \frac{1}{m^h} \sum_{u_0, \ldots, u_{h-1} \in \mathcal{R}} \sum_{n=0}^{N-1} \left( -\sum_{j=0}^{h-1} u_j e_j \right) \left( \sum_{j=0}^{h-1} u_j a_{n+j} \right) \]

\[ = \frac{1}{m^h} \sum_{u_0, \ldots, u_{h-1} \in \mathcal{R}} \left( -\sum_{j=0}^{h-1} u_j e_j \right) \sum_{n=0}^{N-1} \left( \sum_{j=0}^{h-1} u_j a_{n+j} \right). \]

The term corresponding to \( u_0 = \cdots = u_{h-1} = 0 \) is equal to \( N \), and so Theorem 3 follows by applying the bound of Theorem 1 to each of the remaining terms in this sum.

4. Remarks

Clearly, for \( h \leq d/2 \), we have
\[ v^{1+(1/2)\nu}N^{1-(1/2)\nu}m^{d/2\nu}(d-h)^{-1/2} + d - h \leq 2^{1/2}v^{1+(1/2)\nu}N^{1-(1/2)\nu}m^{d/2\nu}d^{-1/2} + d. \]

Thus for \( h \leq d/2 \) our bounds can be written in a form which does not depend on \( h \).

The above bounds on \( S(u; N) \) and \( C(h; N) \) are non-trivial only when \( N \), and thus \( T \) and \( t \), is close to its largest possible value \( m^d \). An important special case of this situation is \( T = t = m^d \). In this case, every possible window of length \( d \) occurs exactly once within a period of the sequence; such sequences are known as de Bruijn sequences. Such sequences, or sequences close to them, have a long and varied history both in pure combinatorics and in the design of sequences with good correlation properties for applications in communication systems. Sequences having large values of \( T \) also routinely occur in stream cipher applications (where recurrence relations are often chosen so that the period of the resulting output sequence is as large as possible).

In more detail, if we take \( v = \lfloor 2 \ln(m^d/N + 1) \rfloor \) then we get a bound of the form \( O(Nd^{-1/2}\ln(m^d/N + 1)) \) (for \( h \leq d/2 \)). In particular, the bound is non-trivial if \( T \geq N \geq m^d \exp(o(d^{1/2})) \). When \( N = T = t = m^d \), that is for the full cycle of a de Bruijn sequence, if \( m \) is fixed (for example, for a binary de Bruijn sequence) our bound becomes \( O(t \log t)^{-1/2} \) (In fact in this case the choice \( v = 1 \) is optimal).

For \( R(e_0, \ldots, e_{h-1}; N) \), we have similar results under the additional constraint \( h = o(\log d) \) (which can be slightly relaxed).

References