
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 24 October 2006; accepted 25 October 2006

Unfortunately Theorems 1 and 3 of our recent paper “Character sums and nonlinear recurrence sequences” [1] of this journal do not hold in full generality (though the results do hold over a finite field, which is the main case of interest). This brief note states corrected versions of these theorems.

We first remind the reader of the notation used in [1]. Let \( R \) be a finite ring of \( m \) elements. Let \( a_0, a_1, \ldots \) be a sequence over \( R \) that satisfies a nonlinear recurrence of order \( d \), so there is a function \( F : R^d \to R \) with the property
\[
a_n + d = F(a_{d+n-1}, \ldots, a_n)
\]
for \( n = 0, 1, \ldots \). There exist nonnegative integers \( r \) and \( t \), which we take as small as possible, such that \( a_{n+r} = a_n \) for all \( n \geq r \). We set \( T = r + t \). Let \( \chi : R \to \mathbb{C} \) be a nontrivial additive character of \( R \).

For a vector \( u = (u_0, u_1, \ldots, u_h) \in R^{h+1} \) and a positive integer \( N \), we define
\[
S(u; N) = \sum_{n=0}^{N-1} \chi(u_0a_n + u_1a_{n+1} + \cdots + u_ha_{n+h}).
\]

A correct version of Theorem 1 may be stated as follows.

**Theorem A.** Let \( d, T, u = (u_0, u_1, \ldots, u_h), \chi \) and \( S(u; N) \) be defined as above. Suppose that there exists \( i \in \{0, 1, \ldots, h\} \) such that \( u_i R \not\subseteq \ker \chi \). Then for any integer \( v \geq 1 \), whenever \( h < d \) and \( N \leq T \), we have that
\[
|S(u; N)| < v^{1+1/2v}N^{1-1/2v}m^{d/v}(d-h)^{-1/2} + d - h.
\]

If we compare Theorem 1 of our paper [1] to Theorem A above, we see that the condition that \( (u_0, u_1, \ldots, u_h) \in R^{h+1} \) is a nonzero vector has been replaced by the condition that there exists \( i \in \{0, 1, \ldots, h\} \) such that \( u_i R \not\subseteq \ker \chi \). Note that when \( R \) is a finite field, this new condition is equivalent to the condition that the vector is nonzero. The conditions are also equivalent when \( \chi \) has a trivial kernel. However, for a general finite ring \( R \) the new condition is strictly stronger.

The proof of Theorem A is the same as that of Theorem 1 in [1], except the line below Eq. (5) should refer to \( \chi \phi \) being nontrivial and the paragraph which follows should be replaced by the paragraph below.

Define the (additive) group \( G \) by \( G = R/ \ker \chi \). We write \( \overline{x} \) or \( \overline{x} \), respectively, for the image of a set \( X \subseteq R \) or \( x \in R \) in \( G \), under the natural homomorphism. By our condition on \( u \), at least one of the sets \( u_j R \) is nontrivial, and so we may choose a prime \( \kappa \) that divides the order of some element in \( \bigcup_{j \in \{0, 1, \ldots, h\}} u_j R \). Let \( \kappa^e \) be the largest

DOI of original article: 10.1016/j.disc.2006.02.012.
E-mail addresses: s.blackburn@rhul.ac.uk (S.R. Blackburn), igor@ics.mq.edu.au (I.E. Shparlinski).
power of \( \kappa \) that divides an element in \( \bigcup_{j \in [0,1,\ldots,h]} u_j \mathcal{R} \), and define \( j_0 \) to be the minimum integer \( j \) such that \( u_j \mathcal{R} \) contains an element of order divisible by \( \kappa^e \). (Thus in particular, \( u_{j_0} \) has order divisible by \( \kappa^e \).) Define \( \overline{P} \) to be the subgroup of \( \overline{G} \) generated by all elements of \( \overline{G} \) whose order is not divisible by \( \kappa^e \). For \( i \in \{0, 1, \ldots, f - 1\} \), define ‘multiplicities’ \( \mu_i \) and \( \eta_i \) by

\[
\mu_i = \# \{ j \in \{1, \ldots, v\} : k_j = i \}
\]

and

\[
\eta_i = \# \{ j \in \{1, \ldots, v\} : \ell_j = i \}.
\]

We claim that if there exists \( i \in \{0, 1, \ldots, f - 1\} \) with \( \mu_i - \eta_i \not\equiv 0 \mod \kappa \) then \( \chi \phi \) is nontrivial. To see this, let \( i_0 \) be the minimum integer \( i \in \{0, 1, \ldots, f - 1\} \) with this property. Then

\[
\phi(c_0, c_1, \ldots, c_{d-1}) = \sum_{i=0}^{f} (\mu_i - \eta_i) \sum_{j=0}^{h} u_j c_{i+j} \in (\mu_{i_0} - \eta_{i_0}) u_{j_0} c_{i_0 + j_0} + X + \overline{P},
\]

where \( X \) is an expression that does not involve \( c_{i_0 + j_0} \). When \( c_{i_0 + j_0} = 1 \), we see that \( u_{j_0} c_{i_0 + j_0} \) does not lie in \( \overline{P} \) and therefore \( \phi(c_0, c_1, \ldots, c_{d-1}) \) does not always lie in \( \ker \chi \). Thus \( \chi \phi \) is nontrivial, as required.

Our paper [1] gives two applications of Theorem 1. The first application (Corollary 2) to autocorrelation properties needs no change as the vector \( u = (-1, 0, 0, \ldots, 1) \) satisfies the new condition we stated above. However, the statement of Theorem 3, the application to window distributions, requires some modifications. We state a correct version of the theorem by defining the notion of a principled ring as follows. We say that an additive character \( \chi \) of a ring \( \mathcal{R} \) is (right) unprincipled if \( \mathcal{R} c \subseteq \ker \chi \) for some nonzero element \( c \in \mathcal{R} \), otherwise we say that \( \chi \) is principled. We say that the ring \( \mathcal{R} \) is principled if it has a principled character. Recall from [1] the definition of \( R(e_0, e_1, \ldots, e_{h-1}; N) \) to be the number of integers \( n \in \{0, 1, \ldots, N - 1\} \) for which \( (a_n, a_{n+1}, \ldots, a_{n+h-1}) = (e_0, e_1, \ldots, e_{h-1}) \).

**Theorem B.** Let \( \mathcal{R} \) be a principled ring. 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

\[
|R(e_0, \ldots, e_{h-1}; N)| = \frac{N}{m^h} < v^{1+1/2\nu} N^{1-1/2\nu} m^{d/2\nu} (d - h)^{-1/2} + d - h.
\]

So the statement of Theorem B is exactly the same as that of Theorem 3 of [1], except that we have added the restriction that the finite ring \( \mathcal{R} \) is principled. This restriction is needed because in the proof of Theorem 3 we need to choose a character \( \chi \) of \( \mathcal{R} \) such that

\[
\frac{1}{\# \mathcal{R}} \sum_{u \in \mathcal{R}} \chi(u c) = \begin{cases} 1 & \text{if } c = 0, \\ 0 & \text{otherwise} \end{cases}
\]

and only principled characters have this property.

Note that finite fields \( \mathbb{F}_q \) are principled (as any nontrivial additive character is principled), as are residue rings \( \mathbb{Z}/m\mathbb{Z} \) (as any character with trivial kernel is principled). Many other finite rings, such as the ring of \( m \times m \) matrices over a finite field, are principled. To see that not all finite rings are principled, consider the quotient ring \( \mathcal{R} = \mathbb{F}_q[x_1, x_2]/(x_1^2, x_1x_2, x_2^2) \). A character \( \chi \) of \( \mathcal{R} \) has a kernel \( K \) of index at most \( p \), and so \( K \) contains a nonzero element \( c \in \langle x_1, x_2 \rangle \). But then \( \mathcal{R} c = \langle c \rangle \subseteq K \), and so all characters \( \chi \) are unprincipled. An interesting open problem is to characterise those finite rings that are principled.

**References**