J. Aust. Math. Soc. **77** (2004), 425–436

ON THE PSEUDORANDOMNESS OF THE SIGNS OF KLOOSTERMAN SUMS

ÉTIENNE FOUVRY, PHILIPPE MICHEL, JOËL RIVAT and ANDRÁS SÁRKÖZY

(Received 17 February 2003; revised 29 September 2003)

Communicated by W. W. L. Chen

Abstract

In this paper we study the pseudorandom properties of the signs of Kloosterman sums.

2000 *Mathematics subject classification*: primary 11K36, 11L05; secondary 11K45, 11K38.
Keywords and phrases: Pseudo-random, binary sequence, correlation, Kloosterman sums, monodromy.

1. Introduction

Throughout this paper we use the following notation: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ denote the set of the positive integers, respectively integers, real numbers, complex numbers.

In a series of papers Mauduit, Rivat and Sárközy (partly with other coauthors) studied finite pseudorandom binary sequences

$$E_N = \{e_1, \dots, e_N\} \in \{-1, +1\}^N.$$

In particular, in [8] Mauduit and Sárközy first introduced the following measures of pseudo-randomness: the *well-distribution measure* of E_N is defined by

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|$$

Research of the fourth author partially supported by Hungarian National Foundation for Scientific Research, Grant No T 029 759 and 'Balaton' French-Hungarian exchange program F-18/00.

where the maximum is taken over all $a, b, t \in \mathbb{N}$ such that $1 \leqslant a \leqslant a+(t-1)b \leqslant N$, and the *correlation measure of order l* of E_N is defined as

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

where the maximum is taken over all $D = (d_1, \ldots, d_l)$ and M such that $0 \leqslant d_1 < \cdots < d_l \leqslant N - M$. Then the sequence is considered as a 'good' pseudo-random sequence if both these measures $W(E_N)$ and $C_l(E_N)$ (at least for 'small' l) are 'small' in terms of N (in particular, both are $o(N)$ as $N \to \infty$). Indeed, later Cassaigne, Mauduit and Sárközy [1] showed that this terminology is justified since for almost all $E_N \in \{-1, +1\}^N$, both $W(E_N)$ and $C_l(E_N)$ are less than $N^{1/2}(\log N)^c$.

The aim of this paper is to give new examples of pseudorandom sequences. These examples come from the theory of exponential sums.

For $x \in \mathbb{R}$, we write $e(x) = \exp(2i\pi x)$ and we denote by $S(l, m; n)$ the Kloosterman sum

$$S(l, m; n) = \sum_{\substack{k \bmod n \\ (k,n)=1}} e\left(\frac{lk + m\bar{k}}{n}\right)$$

where $\bar{k}$ is the multiplicative inverse of k modulo n.

By Weil's theorem, if p is a prime number, $n \in \mathbb{Z}$ and $(n, p) = 1$, then we have

$$|S(1, n; p)| \leqslant 2p^{1/2}.$$

The Kloosterman sum $S(1, n; p)$ is a real non zero number, thus there is a unique real number $\theta_{p,n}$ with

$$\frac{S(1, n; p)}{2p^{1/2}} = \cos \theta_{p,n}, \quad 0 \leqslant \theta_{p,n} \leqslant \pi, \ \theta_{p,n} \neq \pi/2.$$

It follows from results of Deligne and Katz that for $p \to +\infty$, $0 \leqslant \alpha < \beta \leqslant \pi$ the numbers $\theta_{p,n}$ with $1 \leqslant n \leqslant p-1$ satisfy the asymptotic formula

$$\frac{1}{p-1} \left| \{n : 1 \leqslant n \leqslant p-1, \ \alpha \leqslant \theta_{p,n} \leqslant \beta\} \right| \sim \frac{2}{\pi} \int_{\alpha}^{\beta} \sin^2 t \, dt.$$

The angle $\theta_{p,n}$ has been studied in several papers, in particular, by Fouvry and Michel in [4]. Their work suggests that the signs of Kloosterman sums

$$S(1, 1; p), \ S(1, 2; p), \ \ldots, \ S(1, p-1; p) \tag{1}$$

(that is, the fact whether $0 \leqslant \theta_{p,n} < \pi/2$ or $\pi/2 < \theta_{p,n} \leqslant \pi$ holds) may have certain 'random' behaviour. More specifically, do the signs of the numbers in (1) form a 'good' pseudorandom binary sequence in terms of the measures introduced above? In this paper our goal is to show that the answer to this question is affirmative.

THEOREM 1.1. *If p is a prime number, $l \in \mathbb{N}$, and the binary sequence $E_{p-1} = \{e_1, \dots, e_{p-1}\}$ is defined by*

$$e_n = \begin{cases} +1, & \text{if } S(1,n;p) > 0; \\ -1, & \text{if } S(1,n;p) < 0 \end{cases}$$

then we have

$$W(E_{p-1}) < c_1 p^{3/4} (\log p)^{1/2} \quad \text{and} \quad C_l(E_{p-1}) < c_2(l) p^{(2l+1)/(2l+2)} (\log p)^{1/(l+1)}$$

(where $c_2(l)$ is a constant which may depend on l).

2. Kloosterman sums

If $k \in \mathbb{Z}$, $k \geqslant 0$, we denote by $\operatorname{sym}_k \theta$ the function

$$\operatorname{sym}_k \theta = \frac{\sin(k+1)\theta}{\sin\theta},$$

and by $\operatorname{Sym}_k(\mathrm{SL}_2)$ the k-th symetric power representation of $\mathrm{SL}_2(\mathbb{C})$ (see [9] for further details).

LEMMA 2.1. *For every integer $r \geqslant 1$, there exists a constant $C(r)$ such that*

- *for every r-tuple of polynomials $(f_1, \dots, f_r)$ of the form $f_i(X) = a_i X + b_i$, with $a_i, b_i \in \mathbb{Z}$, $(1 \leqslant i \leqslant r)$, satisfying $\prod_{1 \leqslant i \leqslant r} a_i \neq 0$ and $(a_i, b_i) \neq (a_j, b_j)$ $(1 \leqslant i < j \leqslant r)$;*
- *for every prime p, for every $r+1$-tuple of integers $(k_1, \dots, k_r, h)$, such that $k_i \geqslant 0$ $(1 \leqslant i \leqslant r)$ and $(k_1, \dots, k_r, h \pmod p) \neq (0, \dots, 0)$,*

we have the inequality

$$\left| \sideset{}{^*}\sum_{0 \leqslant n < p} \operatorname{sym}_{k_1}(\theta_{p,f_1(n)}) \cdots \operatorname{sym}_{k_r}(\theta_{p,f_r(n)}) \mathrm{e}\left(\frac{hn}{p}\right) \right| \leqslant C(r)(k_1+1)\cdots(k_r+1)\, p^{1/2},$$

where, in $\sum^*$, the asterisk indicates that only the terms with

$$f_1(n) \cdots f_r(n) \not\equiv 0 \mod p \tag{2}$$

are considered.

PROOF. This lemma shows the independence of the distribution of the sets of angles $\{\theta_{p,f_j(n)};\ n \pmod p\}$ for $1 \leqslant j \leqslant r$. The additive character $n \mapsto \mathrm{e}(hn/p)$ will be

https://doi.org/10.1017/S1446788700014543 Published online by Cambridge University Press

used to detect n in an interval modulo p. A similar result of independence appears in [9, Proposition 2.8], where the following equality

$$\sum_{m=1}^{p-1} \mathrm{sym}_{k_1}(\theta_{p,\overline{m}^2}) \mathrm{sym}_{k_2}(\theta_{p,\overline{am}^2}) \mathrm{e}\left(-\frac{hm}{p}\right) = O(p^{1/2}),$$

is proved uniformly for $a \neq 0, \pm 1$ (modulo p) and $(k_1, k_2, h \pmod p) \neq (0,0,0)$. Our proof of the lemma follows the same lines so we give a sketch of the proof only. It is based on the important works of Katz on the computation of some geometric monodromy groups and its diophantine consequences [6, 7].

Let $\mathscr{L}_\psi$ be the rank 1 lisse sheaf on $\mathbf{A}^1_{\mathbb{F}_p}$ associated to the (possibly trivial) additive character of $\mathbb{F}_p$, $\psi(x) = \mathrm{e}(hx/p)$; let $\mathscr{K}l$ be the (rank 2 sheaf, lisse on $\mathbf{G}_{m,\mathbb{F}_p}$) Kloosterman sheaf (which satisfies $\mathrm{tr}(\mathrm{Frob}_x, \mathscr{K}l) = -S(1,m;p)/\sqrt{p}$), and f_j the morphisms $x \mapsto f_j(x) = a_j x + b_j$; by the Lefshetz trace formula, Deligne's theorem on the weight and a computation of an Euler characteristic, it is sufficient to prove that the sheaf

$$\mathrm{Sym}_{k_1}([f_1]^*\mathscr{K}l) \otimes \cdots \otimes \mathrm{Sym}_{k_r}([f_r]^*\mathscr{K}l) \otimes \mathscr{L}_\psi$$

is geometrically irreducible. This in turn follows from the fact that the geometric monodromy group of the sheaf

$$[f_1]^*(\mathscr{K}l) \oplus \cdots \oplus [f_r]^*(\mathscr{K}l)$$

is as large as possible (that is, is $\mathrm{SL}_2 x \cdots x \mathrm{SL}_2$). The latter fact is proved as in [3, 9] using the Goursat-Kolchin-Ribet criterion and the computation by Katz, of the local monodromy of $\mathscr{K}l$ at 0 and ∞.

This technique of independence of sheaves also appears (even in a more complicated context) in other works: [4, 10, 11], for instance, with applications to the study of exponential sums. □

To switch from the complete sums in Lemma 2.1 to incomplete sums, we need a principle coming at least from Vinogradov which is based on the following inequality.

LEMMA 2.2. *If $m \in \mathbb{N}$, the function $g(x) : \mathbb{Z} \to \mathbb{C}$ is periodic of period m, and X, Y are real numbers with $Y > 0$, then*

$$\left|\sum_{X < n \leqslant X+Y} g(n)\right| \leqslant \frac{Y+1}{m} \left|\sum_{n=1}^{m} g(n)\right| + \sum_{1 \leqslant |h| \leqslant m/2} |h|^{-1} \left|\sum_{n=1}^{m} g(n)\, \mathrm{e}\left(\frac{hn}{m}\right)\right|.$$

PROOF. This is implicit in [14] and explicitly stated in [2, formula (6.4)] and in [8]. □

https://doi.org/10.1017/S1446788700014543 Published online by Cambridge University Press

LEMMA 2.3. *For every $r \in \mathbb{N}$, there exists a constant $C'(r)$ such that under the conditions of Lemma* 2.1 *and also assuming $(k_1, \dots, k_r) \neq (0, \dots, 0)$, we have*

$$\max_{0 \leqslant M < p} \left| \sideset{}{^*}\sum_{0 \leqslant n < M} \operatorname{sym}_{k_1}\left(\theta_{p,f_1(n)}\right) \cdots \operatorname{sym}_{k_r}\left(\theta_{p,f_r(n)}\right) \right| \leqslant C'(r)(k_1+1)\cdots(k_r+1)\sqrt{p}\log p.$$

where, in $\sum^*$, the asterisk has the same meaning as in Lemma 2.1.

PROOF. We apply Lemma 2.2 with the function $g(x)$ defined by

$$g(n) = \operatorname{sym}_{k_1}\left(\theta_{p,f_1(n)}\right) \cdots \operatorname{sym}_{k_r}\left(\theta_{p,f_r(n)}\right)$$

if n satisfies (2) and $g(n) = 0$ otherwise.

We obtain

$$\left| \sideset{}{^*}\sum_{0 \leqslant n < M} \operatorname{sym}_{k_1}\left(\theta_{p,f_1(n)}\right) \cdots \operatorname{sym}_{k_r}\left(\theta_{p,f_r(n)}\right) \right| \leqslant \frac{M+1}{p} \left| \sideset{}{^*}\sum_{0 \leqslant n < p} \operatorname{sym}_{k_1}\left(\theta_{p,f_1(n)}\right) \cdots \operatorname{sym}_{k_r}\left(\theta_{p,f_r(n)}\right) \right| + \sum_{1 \leqslant |h| \leqslant p/2} |h|^{-1} \left| \sideset{}{^*}\sum_{0 \leqslant n < p} \operatorname{sym}_{k_1}\left(\theta_{p,f_1(n)}\right) \cdots \operatorname{sym}_{k_r}\left(\theta_{p,f_r(n)}\right) \mathrm{e}\left(\frac{hn}{p}\right) \right|.$$

Applying now Lemma 2.1 first with $h = 0$ and then for all h with $1 \leqslant |h| \leqslant p/2$, we obtain that this upper bound is

$$\leqslant C(r)(k_1+1)\cdots(k_r+1)\,p^{1/2}\left(\frac{M+1}{p} + \sum_{1 \leqslant |h| \leqslant p/2} |h|^{-1}\right)$$

$$\leqslant C'(r)(k_1+1)\cdots(k_r+1)\,p^{1/2}\log p. \qquad \square$$

3. Trigonometric approximation

In 1974, A. Selberg proved the optimal form of the large sieve, using some entire functions with extremal properties. These functions, already studied by Beurling in the 1930's (unpublished), have many applications in analysis and in number theory, see, for example, Vaaler [13], Montgomery [12] and Graham-Kolesnik [5].

https://doi.org/10.1017/S1446788700014543 Published online by Cambridge University Press

In this section we apply the method described in [13, Theorem 19] to approximate a function of bounded variation by trigonometric polynomials. For the sake of clarity, the notations in this section are adopted from Vaaler's paper and are therefore independent of the rest of this paper.

Let f be the even and 1-periodic function defined by

$$f(x) = \begin{cases} +1 & \text{if } |x| < 1/4; \\ 0 & \text{if } |x| = 1/4; \\ -1 & \text{if } 1/4 < |x| \leqslant 1/2. \end{cases}$$

According to inequality (7.24) of [13, Theorem 19], for all integer $N \geqslant 1$, we have

$$|f(x) - f * j_N(x)| \leqslant (2N+2)^{-1}(dV_f) * k_N(x) \quad (x \in \mathbb{R}), \tag{3}$$

where j_N and k_N are defined by (7.2) and (7.3) of Vaaler [13]:

$$j_N(x) = \sum_{n=-N}^{N} \widehat{J_{N+1}}(n)\, \mathrm{e}(nx), \quad k_N(x) = \sum_{n=-N}^{N} \widehat{K_{N+1}}(n)\, \mathrm{e}(nx),$$

and the convolutions $f * j_N$ and $(dV_f) * k_N$ are defined by

$$f * j_N(x) = \sum_{n=-N}^{N} \widehat{f}(n)\, \widehat{J_{N+1}}(n)\, \mathrm{e}(nx),$$

$$(dV_f) * k_N(x) = \sum_{n=-N}^{N} \widehat{dV_f}(n)\, \widehat{K_{N+1}}(n)\, \mathrm{e}(nx).$$

For $n \in \mathbb{Z}$, we compute the Fourier coefficients

$$\begin{aligned} \widehat{f}(n) &= \int_{-1/2}^{1/2} f(t)\, \mathrm{e}(-nt)\, dt = 2\int_{0}^{1/2} f(t) \cos(2\pi nt)\, dt \\ &= 2\int_{0}^{1/4} \cos(2\pi nt)\, dt - 2\int_{1/4}^{1/2} \cos(2\pi nt)\, dt, \end{aligned}$$

hence $\widehat{f}(0) = 0$ and for $n \neq 0$,

$$\widehat{f}(n) = \frac{\sin(\pi n/2)}{\pi n/2} - \frac{\sin(\pi n)}{\pi n} = \frac{\sin(\pi n/2)}{\pi n/2}.$$

The variation V_f of the function f is piecewise constant, with jumps of $+2$ in $-1/4$ and $+1/4$, so that with the help of Dirac measures we can write $dV_f = 2\delta_{-1/4} + 2\delta_{1/4}$, thus

$$\widehat{dV_f}(n) = \int_{-1/2}^{1/2} \mathrm{e}(-nt)\, dV_f(t) = 2\,\mathrm{e}(n/4) + 2\,\mathrm{e}(-n/4) = 4\cos(\pi n/2).$$

https://doi.org/10.1017/S1446788700014543 Published online by Cambridge University Press

According to the notations of Vaaler, by definition

$$\widehat{J_{N+1}}(n) = \widehat{J}\left(\frac{n}{N+1}\right), \quad \widehat{K_{N+1}}(n) = \widehat{K}\left(\frac{n}{N+1}\right),$$

where, from [13, Theorem 6], we know that $\widehat{J}$ is even, non negative, continuously differentiable, steadily decreasing over $[0, 1]$, and non zero only over $]-1, +1[$. Furthermore, we have

$$\widehat{K}(t) = \max(1 - |t|, 0).$$

Finally,

$$f * j_N(x) = 2\sum_{n=1}^{N} \frac{\sin(\pi n/2)}{\pi n/2}\, \widehat{J}\left(\frac{n}{N+1}\right)\cos(2\pi nx), \tag{4}$$

$$d V_f * k_N(x) = 4 + 8\sum_{n=1}^{N} \cos(\pi n/2)\, \widehat{K}\left(\frac{n}{N+1}\right)\cos(2\pi nx). \tag{5}$$

4. Exponential sums

Let ξ be the even and 2π periodic function defined by

$$\xi(x) = \begin{cases} +1 & \text{if } |x| < \pi/2; \\ 0 & \text{if } |x| = \pi/2; \\ -1 & \text{if } \pi/2 < |x| \leqslant \pi. \end{cases}$$

LEMMA 4.1. *For any $K \in \mathbb{N}$, there exist real coefficients $a_K(k)$ and $b_K(k)$ $k = 0, \ldots, K$ with*

$$a_K(0) = 0, \tag{6}$$

and for $k = 0, \ldots, K$,

$$a_K(k) = O((k+1)^{-1}), \quad b_K(k) = O(K^{-1}), \tag{7}$$

such that the trigonometric polynomials

$$\phi_K(x) := \sum_{k=0}^{K} a_K(k)\cos(kx), \tag{8}$$

$$\psi_K(x) := \sum_{k=0}^{K} b_K(k)\cos(kx) \tag{9}$$

https://doi.org/10.1017/S1446788700014543 Published online by Cambridge University Press

satisfy for all $x \in \mathbb{R}$,

$$|\xi(x) - \phi_K(x)| \leqslant \psi_K(x). \tag{10}$$

PROOF. It follows from (3), (4) and (5) with $\xi(x) = f(x/2\pi)$. □

LEMMA 4.2. *The functions* $\phi_K(x)$ *and* $\psi_K(x)$ *in Lemma* 4.1 *can be written in the form*

$$\phi_K(x) = \sum_{k=0}^{K} c_K(k)\,\mathrm{sym}_k(x); \quad \psi_K(x) = \sum_{k=0}^{K} C_K(k)\,\mathrm{sym}_k(x) \tag{11}$$

with

$$c_K(0) = 0 \quad \textit{and} \tag{12}$$

$$c_K(k) = O((k+1)^{-1}), \quad C_K(k) = O(K^{-1}) \quad \textit{for } k = 0, \dots, K. \tag{13}$$

PROOF. As in [4], the coefficients in (11) can be computed in the following way:

$$\begin{aligned} c_K(k) &= \frac{2}{\pi}\int_0^\pi \phi_K(t)\,\mathrm{sym}_k(t)\sin^2(t)\,dt \\ &= \frac{1}{\pi}\int_0^\pi \phi_K(t)\cos(kt)\,dt - \frac{1}{\pi}\int_0^\pi \phi_K(t)\cos((k+2)t)\,dt \\ &= (a_K(k) - a_K(k+2))/2 \end{aligned} \tag{14}$$

and similarly,

$$C_K(k) = (b_K(k) - b_K(k+2))/2. \tag{15}$$

Then (13) follows from (7), (14) and (15).

Concerning the value of $c_K(0)$, we use the value obtained for $a_K(k)$ from [13, Theorem 19], namely

$$a_K(k) = 2\,\frac{\sin(\pi k/2)}{\pi k/2}\,\widehat{J}\left(\frac{k}{K+1}\right),$$

where $\widehat{J}$ is a continuous function over [0, 1]. For $k = 2$, the first factor is 0. Therefore, $a_K(2) = 0$ and (12) follows from (6). □

LEMMA 4.3. *Let* $z_1, \dots, z_r, z_1', \dots, z_r'$ *be complex numbers of modulus at most* 1. *Then* $|z_1 \cdots z_r - z_1' \cdots z_r'| \leqslant |z_1 - z_1'| + \cdots + |z_r - z_r'|$.

PROOF. It suffices to observe that $z_1 \cdots z_r - z_1' \cdots z_r'$ is equal to

$$(z_1 - z_1')z_2 \cdots z_r + z_1'(z_2 - z_2')z_3 \cdots z_r + \cdots + z_1' \cdots z_{r-1}'(z_r - z_r'),$$

and the triangle inequality gives the result. □

https://doi.org/10.1017/S1446788700014543 Published online by Cambridge University Press

LEMMA 4.4. *If $N \in \mathbb{N}$, $\alpha_{i,j}$ are real numbers with $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant N$, and $B > 0$ is such that for any $(k_1, \dots, k_r) \in \mathbb{Z}^k$, $(k_1, \dots, k_r) \neq (0, \dots, 0)$, $(k_i \geqslant 0)$,*

$$\left|\sum_{j=1}^{N} \mathrm{sym}_{k_1}(\alpha_{1,j}) \cdots \mathrm{sym}_{k_r}(\alpha_{r,j})\right| \leqslant (k_1+1)\cdots(k_r+1)B, \tag{16}$$

then there exists $c(r) > 0$ (independent of B) such that

$$\left|\sum_{j=1}^{N} \xi(\alpha_{1,j}) \cdots \xi(\alpha_{r,j})\right| \leqslant c(r)\left(N^{r/(r+1)}B^{1/(r+1)} + B\right).$$

PROOF. By (7) and (9) we have $|\psi_K(x)| \ll 1$. Hence by (10) we get

$$|\phi_K(x)| \leqslant |\xi(x)| + |\psi_K(x)| \ll 1,$$

and using Lemma 4.3, for any integer $K > 0$ we obtain

$$\left|\sum_{j=1}^{N} \xi(\alpha_{1,j}) \cdots \xi(\alpha_{r,j}) - \sum_{j=1}^{N} \phi_K(\alpha_{1,j}) \cdots \phi_K(\alpha_{r,j})\right| \ll_r \sum_{i=1}^{r}\sum_{j=1}^{N} \psi_K(\alpha_{i,j}), \tag{17}$$

(where $\ll_r$ means that the implicit constant may depend on r), and by using Lemma 4.2 and (16) with $k_1 = k$, $k_2 = \cdots = k_r = 0$,

$$\begin{aligned}\left|\sum_{i=1}^{r}\sum_{j=1}^{N} \psi_K(\alpha_{i,j})\right| &\leqslant r\,|C_K(0)|\,N + \sum_{i=1}^{r}\sum_{k=1}^{K} |C_K(k)| \left|\sum_{j=1}^{N} \mathrm{sym}_k(\alpha_{i,j})\right| \\ &\ll \frac{rN}{K} + rKB.\end{aligned} \tag{18}$$

By Lemma 4.2 and (16) we have

$$\begin{aligned}&\sum_{j=1}^{N} \phi_K(\alpha_{1,j}) \cdots \phi_K(\alpha_{r,j}) \\ &\quad = \sum_{k_1=1}^{K} \cdots \sum_{k_r=1}^{K} c_K(k_1) \cdots c_K(k_r) \sum_{j=1}^{N} \mathrm{sym}_{k_1}(\alpha_{1,j}) \cdots \mathrm{sym}_{k_r}(\alpha_{r,j}) \\ &\quad \ll_r \left(\sum_{k=1}^{K} |c_K(k)|\,(k+1)\right)^r B \ll_r K^r B.\end{aligned} \tag{19}$$

By (17), (18) and (19),

$$\left|\sum_{j=1}^{N} \xi(\alpha_{1,j}) \cdots \xi(\alpha_{r,j})\right| \ll_r \frac{N}{K} + K^r B,$$

and the result follows if we choose $K \asymp \max(1, (N/B)^{1/(r+1)})$. □

https://doi.org/10.1017/S1446788700014543 Published online by Cambridge University Press

LEMMA 4.5. *For any integer $r \geqslant 1$, there exists a constant $c(r) > 0$ such that under the conditions of Lemma* 2.1

$$\max_{0\leqslant M<p}\left|\sideset{}{^*}\sum_{0\leqslant n<M}\xi(\theta_{p,f_1(n)})\cdots\xi(\theta_{p,f_r(n)})\right| \leqslant c(r)p^{(2r+1)/(2r+2)}(\log p)^{1/(r+1)}.$$

PROOF. By Lemma 2.3, (16) holds with $B \asymp p^{1/2}\log p$ if $(\alpha_{1,j},\dots,\alpha_{r,j})$ is an r-tuple $(\theta_{p,f_1(n)},\dots,\theta_{p,f_r(n)})$ with an n satisfying (2) and thus the result follows from Lemma 4.4. □

REMARK. Using the same techniques derived from [13, Theorem 19] we can prove that

$$\left|\frac{1}{p-1}\#\{m : 1\leqslant m\leqslant p-1, \alpha\leqslant\theta_{p,\overline{m}^2}\leqslant\beta\} - \frac{2}{\pi}\int_\alpha^\beta \sin^2 t\,dt\right| \ll p^{-1/4}$$

for fixed real α and β satisfying $0\leqslant\alpha<\beta\leqslant\pi$. This improves the upper bound $p^{-1/8}$ obtained by Fouvry and Michel in [4, Lemma 2.3].

5. Completion of the proof of the theorem

It follows from the definitions of $E_{p-1} = \{e_1,\dots,e_{p-1}\}$ and $\theta_{p,n}$ that for all $1\leqslant n\leqslant p-1$ we have $e_n = \xi(\theta_{p,n})$. Thus it follows from Lemma 4.5 that

$$W(E_{p-1}) = \max_{a,b,t}\left|\sum_{j=0}^{t-1} e_{a+jb}\right| = \max_{a,b,t}\left|\sum_{j=0}^{t-1}\xi(\theta_{p,a+jb})\right| \ll p^{3/4}(\log p)^{1/2}$$

and

$$C_l(E_{p-1}) = \max_{M,D}\left|\sum_{n=1}^{M} e_{n+d_1}\cdots e_{n+d_l}\right| = \max_{M,D}\left|\sum_{n=1}^{M}\xi(\theta_{p,n+d_1})\cdots\xi(\theta_{p,n+d_l})\right|$$
$$\ll_l p^{(2l+1)/(2l+2)}(\log p)^{1/(l+1)}.$$

(Note that in both cases, by the definition of the max only $\theta_{p,n}$ values with $1\leqslant n<p$ occur so that adding the asterisk to the sum does not change its value.)

FINAL REMARK. Of course, the above results could be generalized in several directions. We could choose a fixed non zero integer a and define e_n to be the sign of the Kloosterman sum $S(a,n;p)$. The bounds for $W(E_{p-1})$ and $C_l(E_{p-1})$ would be the

https://doi.org/10.1017/S1446788700014543 Published online by Cambridge University Press

same. We could also deal with e_n to be the sign of the Kloosterman sum $S(n, n; p)$. More interesting would be to consider, for instance the cubic trigonometric sum

$$S^{(3)}(l, m; n) = \sum_{k \bmod n} \mathrm{e}\left(\frac{lk^3 + mk}{n}\right).$$

This sum is real, satisfies Weil's bound $\left|S^{(3)}(l, m; p)\right| \leqslant 2\sqrt{p}$. We define e_n to be the sign of the trigonometric sum $S^{(3)}(n, n; p)$. All the above results would be the same, since all the techniques of Katz are applicable there. This could be generalized to other situations where Katz's results are proved, that means to other sums of the form

$$S(f; p) = \sum_{\substack{k \bmod p \\ f(k) \neq \infty}} \mathrm{e}\left(\frac{f(k)}{p}\right),$$

where f is a rational function with integer coefficients satisfying generic properties. We would define $e_n = \pm 1$ according to the value of the modulus of $S(nf; p)$. The exponents appearing in the upper bounds of Theorem 1.1 would be different. They would be obtained after a delicate harmonic analysis on the compact groups $\mathrm{SU}_j(\mathbb{C})$ or $\mathrm{USp}_j(\mathbb{C})$ (for instance, see [4] for an introduction to these techniques).

Acknowledgement

The first and last two authors would like to thank for their invitation in July 2002 to the Erwin Schrödinger Institut and the Graz University, where this work started.

References

[1] J. Cassaigne, C. Mauduit and A. Sárközy, 'On finite pseudorandom binary sequences VII: The measures of pseudorandomness', *Acta Arith.* **103** (2002), 97–118.
[2] W. Duke, J. Friedlander and H. Iwaniec, 'Bilinear forms with Kloosterman fractions', *Invent. Math.* **128** (1997), 23–43.
[3] E. Fouvry, H. Iwaniec and N. Katz, 'The divisor function over arithmetic progressions', *Acta Arith.* **61** (1992), 271–287.
[4] E. Fouvry and P. Michel, 'Sommes de modules de sommes d'exponentielles', *Pacific J. Math.* **209** (2003), 261–288.
[5] S. W. Graham and G. Kolesnik, *Van der Corput's method of exponential sums*, London Math. Soc. Lecture Note Ser. 126 (Cambridge University Press, 1991).
[6] N. M. Katz, *Sommes exponentielles*, Astérisque 79 (Société Mathématique de France, Paris, 1980).
[7] ———, *Gauss sums, Kloosterman sums and monodromy groups*, Ann. of Math. Stud. 116 (Princeton University Press, Princeton, 1988).

[8] C. Mauduit and A. Sárközy, 'On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol', *Acta Arith.* **82** (1997), 365–377.
[9] P. Michel, 'Autour de la conjecture de Sato-Tate pour les sommes de Kloosterman', *Invent. Math.* **121** (1995), 61–78.
[10] ———, 'Autour de la conjecture de Sato-Tate pour les sommes de Kloosterman, II', *Duke Math. J.* **92** (1998), 221–254.
[11] ———, 'Minorations de sommes d'exponentielles', *Duke Math. J.* **95** (1998), 227–240.
[12] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Math. 84 (American Mathematical Society, Providence, 1994).
[13] J. Vaaler, 'Some extremal functions in Fourier analysis', *Bull. Amer. Math. Soc.* **12** (1985), 183–216.
[14] I. M. Vinogradov, *Elements of number theory* (Dover, 1954).

Mathématique
Bâtiment 425
Campus d'Orsay
Université Paris-Sud
91405 Orsay Cedex
France
e-mail: etienne.fouvry@math.u-psud.fr

Mathématiques
Université Montpellier II
CC 052
34095 Montpellier Cedex
France
e-mail: philippe.michel@math.univ-montp2.fr

Institut de Mathématiques de Luminy
CNRS-UMR 6206
Université de la Méditerranée
163 avenue de Luminy
Case 907
13288 Marseille Cedex 9
France
e-mail: rivat@iml.univ-mrs.fr

Eötvös Loránd University
Department of Algebra and
Number Theory
H-1117 Budapest
Pázmány Péter sétány 1/c
Hungary
e-mail: sarkozy@cs.elte.hu