ACTA ARITHMETICA
185.1 (2018)

Exponential sums with automatic sequences

by

Sary Drappeau (Marseille) and Clemens Müllner (Wien)

1. Introduction. A complex-valued sequence (a_n) is called *automatic* if there is a finite deterministic automaton such that for each n, the value a_n is given by a function of the final state of the automaton when the automaton is given as input the digital representation of n. There has been strong interest recently in understanding correlation of automatic sequences with other types of arithmetical functions. Much of this interest has stemmed from the Sarnak conjecture: it was recently shown by the second author [Mül17] that all automatic sequences are asymptotically orthogonal to the Möbius function $\mu(n)$, in the sense that $\sum_{n\le x} a_n\mu(n) = o(x)$ as $x\to\infty$.

In the present paper, we are interested in asymptotic orthogonality of automatic sequences with oscillating functions given by periodic exponentials of rational fractions. The prototype of correlations we wish to study are the incomplete Kloosterman sums

$$\sum_{\substack{n\in\mathcal{I}\\(n,q)=1}} a_n \mathrm{e}\Big(\frac{\overline{n}}{q}\Big), \qquad (\mathrm{e}(z)=e^{2\pi i z},\ n\overline{n}=1\ (\mathrm{mod}\ q)) \tag{1.1}$$

for an interval $\mathcal{I}$ of integers. Our goal is to find conditions on q and on the size $|\mathcal{I}|$ of the interval which ensure that we have *asymptotic orthogonality* of (a_n) and $(\mathrm{e}(\overline{n}/q))$, in the sense that the sum in (1.1) is $o(|\mathcal{I}|)$ as $|\mathcal{I}|\to\infty$.

When (a_n) is constant, a classical result of Weil [Wei48] shows that the condition $|\mathcal{I}|\ge q^{1/2+\varepsilon}$ suffices; we will refer to this condition as the *Pólya–Vinogradov range* (in reference to the Pólya–Vinogradov bound for sums of Dirichlet characters). This may be improved in specific circumstances [Kor00, Irv15], but the range obtained by the Weil bound remains unsurpassed in general.

2010 *Mathematics Subject Classification*: Primary 11L07, 11B85; Secondary 11L05, 11L26.
Key words and phrases: exponential sums, Weil bound, automatic sequences.
Received 2 October 2017; revised 5 March 2018.
Published online 15 June 2018.

DOI: 10.4064/aa171002-20-3

Our main result, which we will describe shortly, shows that asymptotic orthogonality for (1.1) holds in the Pólya–Vinogradov range for *all* automatic sequences.

Statement of results. Let us now describe the precise setting of our study. Given a base $k \geq 2$, $\Sigma = \{0, \dots, k-1\}$, and a deterministic finite automaton $\mathcal{A} = (Q, \Sigma, \delta, q_0, \tau)$ with output function $\tau : Q \to \mathbb{C}$, we define the associated automatic sequence $(a_n)_{n\geq 0} = (\tau(\delta(q_0, (n)_k)))_{n\geq 0}$, where $(n)_k$ denotes the representation of n in base k without leading zeros. When we refer to an *automatic sequence* in what follows, it will always be one given by such a construction. In particular, we assume without loss of generality that $\delta(q_0, 0) = q_0$. For a more detailed treatment of automatic sequences see for example [AS03].

For a rational fraction $f = P(X)/Q(X) \in \mathbb{Q}(X)$, $n \in \mathbb{Z}$ and $q \in \mathbb{N}_{>0}$, we define $\mathrm{e}_q(f(n))$ following [CFH$^+$14, Section 4A]; we describe this in detail below (Section 2) and simply note for now that whenever $(Q(n), q) = 1$, we have

$$\mathrm{e}_q(f(n)) = \mathrm{e}\biggl(\frac{P(n)\overline{Q(n)}}{q}\biggr).$$

Definition 1. Let $f \in \mathbb{Q}(X)$, which we write in reduced form $f = P/Q$ with $P, Q \in \mathbb{Z}[X]$ and coprime. Let also an integer $q \geq 1$ be given.

(i) We let (q, Q) denote the greatest common divisor of q and Q in $\mathbb{Z}[X]$.
(ii) We will say that f *is well-defined modulo* q if $(q, Q) = 1$.
(iii) We define a subset of the primes by

$$\mathcal{Q}_f = \{p : f \text{ reduces to a quadratic polynomial modulo } p\}.$$

(iv) We will say that f *has degree* d if $\max(\deg P, \deg Q) = d$.

Our main result is the following bound.

Theorem 2. *Let (a_n) be an automatic sequence, $f \in \mathbb{Q}[X]$ be a rational function of total degree $d \geq 1$, and $q \geq 1$ be such that f is well-defined modulo q. Let q_1 be the largest squarefree divisor of q, coprime to k and having no prime factor in $\mathcal{Q}_f$:*

$$q_1 := \prod_{\substack{p \| q \\ p \notin \mathcal{Q}_f,\, p \nmid k}} p.$$

Then there exists $c > 0$, depending at most on d and the underlying automaton $\mathcal{A}$, such that

$$\sum_{n \in \mathcal{I}} a_n \mathrm{e}_q(f(n)) \ll_{\varepsilon, \mathcal{A}, d} |\mathcal{I}|^{1+\varepsilon} \biggl(\frac{1}{q_1} + \frac{q^2}{q_1 |\mathcal{I}|^2}\biggr)^c \tag{1.2}$$

for any interval $\mathcal{I} \neq \emptyset$ of integers.

If $f(X)$ is a polynomial of degree exactly 2 and leading coefficient u/v with $(v,q)=1$, then

$$\sum_{n\in\mathcal{I}} a_n \mathrm{e}_q(f(n)) \ll_{\varepsilon,\mathcal{A},u,v} |\mathcal{I}|^{1+\varepsilon}\left(\frac{1}{q}+\frac{q}{|\mathcal{I}|^2}\right)^c, \tag{1.3}$$

where the implied constant may now also depend on u and v.

REMARKS. 1. When $q=p$ is prime, and f does not reduce to a linear function modulo p, the estimates (1.2) and (1.3) are non-trivial in the range $|\mathcal{I}|\ge q^{1/2+\varepsilon}$. Actually, É. Fouvry has remarked to the authors that in the case when q is prime, we can apply a recent result of Fouvry, Kowalski, Michel, Raju, Rivat and Soundararajan [FKM+17], and obtain the improvement

$$\sum_{y<n\le y+x} a_n \mathrm{e}_p(f(n)) = o_{\mathcal{A},f}(x) \tag{1.4}$$

whenever $x,q\to\infty$, $x\le q^{O(1)}$ and $x/q^{1/2}\to\infty$ (see the remark after Lemma 4 below).

As an example, if $s_2(n)$ denotes the sum of digits of n in base 2, and given a function $\psi(q)\to\infty$ as $q\to\infty$, we have

$$\sum_{\substack{y<n\le y+x\\ s_2(n)\text{ is even}}} \mathrm{e}\left(\frac{\overline{n}}{q}\right) = o(x) \qquad (y\ge 0,\ x\ge 1)$$

for q prime, $q\to\infty$ and $q^{1/2}\psi(q)\le x\le q^{O(1)}$.

2. Note that the bound (1.2) is trivial when f is a linear or constant polynomial, as $q_1=1$ in this case. It is clear that for f constant, or $f(X)=X$, there is essentially no cancellation on the left-hand side of (1.2) in the range $\mathcal{I}=[0,q/2]\cap\mathbb{Z}$ when $a_n=1$ for all n.

3. As mentioned, we will prove a general statement (Proposition 13 below) showing that for a bounded sequence of coefficients $(K(n))_{n\ge1}$, we obtain a non-trivial bound for $\sum_{n\in\mathcal{I}} a_n K(n)$ as soon as we have non-trivial bounds on two-point correlation sums of the kind

$$\sum_{\substack{n\in\mathcal{I}\\ n\equiv a\,(\mathrm{mod}\,q)}} K(n+r)\overline{K(n)}$$

with some mild uniformity in q and r. For instance, this offers the possibility to take $K(n)$ to be a more general algebraic trace function [FKM14, FKM15], or Fourier coefficients of a GL_2 holomorphic cusp form [Blo04].

4. The case when the automatic sequence is sparse, in the sense that $\sum_{n\in\mathcal{I}}|a_n| = o(|\mathcal{I}|)$ as $|\mathcal{I}|\to\infty$, is more delicate, as then the "trivial bound" obtained from the triangle inequality is possibly smaller than the right-hand sides of our bounds (1.2) and (1.3). Our bounds yield a non-trivial saving as

long as $\sum_{n\in\mathcal{I}} |a_n| \gg |\mathcal{I}|^{1-\eta}$ and $\eta > 0$ is small enough, in the range $|\mathcal{I}|^{O(\eta)} \le q \le |\mathcal{I}|^{2-O(\eta)}$. For instance, our results apply for numbers with one missing digit in a large enough base $k \ge k_0$. Obtaining a good estimate for the smallest such k_0 is a challenging question, which we do not address here; see [May16] for recent progress on the corresponding question for primes.

Bounds of the type of Theorem 2 can be used to answer additive problems (see [FM98], and the argument in [OS12a, p. 30]). We illustrate this by the following statement, concerning solutions to congruence equations.

THEOREM 3. *Let $\mathcal{S} \subset \mathbb{N}$ be a set of integers with the property that $(a_n) = (\mathbf{1}_{n\in\mathcal{S}})$ is an automatic sequence; such a set is called an automatic set. There exists $\delta > 0$, depending only on the automaton $\mathcal{A}$ underlying (a_n), such that the following holds. For all rational fractions f_1, f_2, f_3 none of which is a linear or constant polynomial, all $m \in \mathbb{Z}$ and all prime q, the number $N_{\mathcal{S}}((f_j), q)$ of solutions to the congruence equation*

$$f_1(n_1) + f_2(n_2) + f_3(n_3) \equiv m \pmod q$$

with $n_j \in \mathcal{S} \cap [1, q]$ for each j is asymptotically

$$N_{\mathcal{S}}((f_j), q) = \frac{|\mathcal{S} \cap [1, q]|^3}{q}\{1 + O(q^{-\delta})\}. \tag{1.5}$$

The implied constant may depend on f_1, f_2, f_3 and $\mathcal{S}$.

REMARK. As we have already remarked, constant sequences are automatic, so the above does not hold in general when considering a single congruence $f(n_1) \equiv m \pmod d$.

Context and overview. There has been much work on correlations of automatic sequences with other arithmetic objects. Some of this interest has stemmed from questions of diophantine approximations and normality of numbers constructed from automatic sequences. For instance, Mauduit [Mau86] obtains non-trivial bounds on sums of the kind

$$\sum_{n\le x} a_n \mathrm{e}(\alpha n) \tag{1.6}$$

for irrational α. See the references in [Mau86] for more on the history of this question (1) We also mention the papers [OS12b, BCS02], whose authors study exponential and character sums over specific sequences, related to digit expansions. In particular, the sum $T_{\ell,q}(r, f)$ of [BCS02] is closely related to (1.1).

(1) We emphasize that in these works, the case when $\sum_{n\le x} |a_n| = o(x)$ is particularly important. As we have already remarked, we do not focus on sparse sequences in the present paper.

The method presented here, however, is related to partial progress on Sarnak's conjecture [Sar12]. For automatic sequences of the kind of $(-1)^{s_2(n)}$ (where we recall that $s_2(n)$ is the sum of base-2 digits of n), Mauduit and Rivat [MR10] point out a certain property (which was later called "carry property"), and show how it can be exploited, in conjunction with the differencing method of Weyl and van der Corput together with strong estimates for the L^1 norm of the discrete Fourier transform of this sequence, to obtain Sarnak's conjecture for this case; they also apply this method to show orthogonality to $\Lambda(n)$, which gives a prime number theorem. Their approach was further formalized and generalized in [MR15] (see also [Han17]), but the estimates on the L^1 norm were replaced by a so-called "Fourier property" (L^∞-bounds on the discrete Fourier transform). Finally, the second author recently showed Sarnak's conjecture for automatic sequences [Mül17], generalizing in particular results for synchronizing automatic sequences [DDM15] and invertible automatic sequences [Drm14, FKP$^+$16].

The present work shows that both Mauduit–Rivat's "carry property" and the second author's structure theorems for automatic sequences can be successfully combined with van der Corput differencing when handling algebraic exponential sums. At the heart of the bounds (1.2) and (1.3) lie Weil's bounds on exponential sums [Wei48].

In Section 2, we state the precise version of Weil's bounds which we will use, and in Section 3 we quote auxiliary results on automata, mainly from [DDM15, DM12, Mül17]. In Section 4, we prove a general statement (Proposition 13) linking generic sums over automatic sequences to differentiated sums over intervals. In Section 5, we prove Theorem 2 in a particular case, and in Section 6 we deduce the general case.

2. Weil bounds. We begin by recalling from [CFH$^+$14] a convention regarding $\mathrm{e}_q(f(n))$. Write in reduced form $f(X) = P(X)/Q(X)$ with $P, Q \in \mathbb{Z}[X]$. Given a prime power p^ν with $Q \not\equiv 0 \pmod{p^\nu}$, reduce $P/Q \equiv P_1/Q_1 \pmod{p^\nu}$. For $n \in \mathbb{Z}$, we define a function of the pair (f, n) by

$$\mathrm{e}_{p^\nu}(f; n) = \begin{cases} \mathrm{e}(P_1(n)\overline{Q_1(n)}/p^\nu), & (Q_1(n), p) = 1, \\ 0, & \text{otherwise}. \end{cases}$$

We will denote this $\mathrm{e}_{p^\nu}(f(n))$ by the slight abuse of notation. We extend this definition to arbitrary moduli $q \geq 1$ with $(q, Q) = 1$ by the Chinese remainder theorem,

$$\mathrm{e}_q(f(n)) := \prod_{p^\nu \| q} \mathrm{e}_{p^\nu}\left(\frac{f(n)}{q/p^\nu}\right). \tag{2.1}$$

The purpose of this section is to justify the following bound on particular exponential sums.

Lemma 4. *Let $x, s \geq 1$, $y \geq 0$, $q \geq 2$, $(a,r) \in \mathbb{Z}^2$, and let $f \in \mathbb{Q}[X]$ of degree at most d be well-defined modulo q. Then*

$$\sum_{\substack{y<n\leq y+x \\ n\equiv a \,(\mathrm{mod}\, s)}} \mathrm{e}_q(f(n+r)-f(n)) \ll_{\varepsilon,d} q^{\varepsilon}\Big(\prod_{\substack{p\| q,\, p\nmid rs \\ p\notin \mathcal{Q}_f}} p\Big)^{-1/2}\Big(\frac{x}{s}+q\Big). \tag{2.2}$$

If $f(X) = \frac{u}{v}X^2$ with $(uq,v)=1$, then

$$\sum_{\substack{y<n\leq y+x \\ n\equiv a \,(\mathrm{mod}\, s)}} \mathrm{e}_q(f(n+r)-f(n)) \ll \min\Big(\frac{x}{s}+1, \Big\|\frac{2u\bar{v}rs}{q}\Big\|_{\mathbb{R}/\mathbb{Z}}^{-1}\Big). \tag{2.3}$$

The bound claimed in (2.2) corresponds to square-root cancellation in the part of the modulus which is squarefree, has no factor in $\mathcal{Q}_f$ and is coprime to rs. We have assumed squarefreeness because it usually suffices in applications, and greatly simplifies the argument; the contribution of higher powers of primes could be studied in specific cases by elementary arguments (see [IK04, Lemmas 12.2 and 12.3]).

Remark. When q is prime, [FKM$^+$17, Theorem 1.1] may be used to obtain an $o(x)$ bound whenever $x/q^{1/2} \to \infty$.

The proof of Lemma 4 is based on the following Weil bound, which is a slightly weaker form of [CFH$^+$14, Proposition 4.6].

Lemma 5 (Weil [Wei48], [CFH$^+$14, Proposition 4.6]). *Let $q \geq 1$ be squarefree, and let $f \in \mathbb{Q}(X)$ of degree $\leq d$ be well-defined modulo q. Then*

$$\sum_{n\,(\mathrm{mod}\, q)} \mathrm{e}_q(f(n)) \ll_{\varepsilon,d} q^{1/2+\varepsilon}(q,f')^{1/2}.$$

To deal with the factor (q, f'), we will use the following lemma.

Lemma 6. *Let $f \in \mathbb{Q}(X)$, which is not a polynomial of degree ≤ 2. Let $q \geq 2$ be squarefree and such that for all $p \mid q$, $p \notin \mathcal{Q}_f$, we have $Q \not\equiv 0 \pmod p$. Then*

$$(q, f'(X+r)-f'(X)+\ell) \ll_{\mathcal{A}} (q,r) \prod_{\substack{p\mid q,\, p\nmid r \\ p\in\mathcal{Q}_f}} p \qquad (r,\ell\in\mathbb{Z}).$$

Proof. Write $f = P/Q$ in reduced form with $P, Q \in \mathbb{Z}[X]$. It will suffice to prove that $(p, f'(X+r)-f'(X)+\ell) = 1$ when p is large enough in terms of the degrees of P and Q, $p \notin \mathcal{Q}_f$, $p \nmid 2r$. Suppose this is not the case. Then by [CFH$^+$14, Lemma 4.5(i)], we have $(p, f(X+r)-f(X)+\ell X - c) = p$ for some class $c \pmod p$. Adding to f an appropriate quadratic polynomial, we may suppose $(p, f(X+r)-f(X)) = p$. Write $P/Q = P_1/Q_1 \pmod p$

with P_1, Q_1 coprime. Then we deduce

$$P_1(a)Q_1(a+r) \equiv Q_1(a)P_1(a+r) \pmod{p}.$$

By coprimality, for all $a \pmod{p}$, $Q_1(a) \equiv 0$ implies $Q_1(a+r) \equiv 0$. Iterating yields $Q_1(a) \equiv 0$ for all $a \pmod{p}$. If p is large enough in terms of $\deg Q$, we would obtain $Q_1 \equiv 0$, which is a contradiction. We deduce $Q_1(a) \not\equiv 0 \pmod{p}$ for all a, so that $P_1(X)/Q_1(X)$ takes a constant value and has no poles. If p is large enough in terms of $\deg P$ and $\deg Q$, we conclude that P_1/Q_1 is a constant polynomial, which again contradicts the hypothesis $p \notin \mathcal{Q}_f$. ∎

Proof of Lemma 4. We may assume $x \geq s$. As (2.3) is a simple bound for a geometric sum, we focus on proving (2.2). After changing indices, the LHS is

$$\sum_{(y-a)/s<m\leq(y+x-a)/s} \mathrm{e}_q(f(a+ms+r)-f(a+ms)).$$

We cover the summation interval by at most $1 + x/sq$ intervals of length q, and detect the size conditions on m by additive characters. We obtain

$$\sum_{(y-a)/s<m\leq(y+x-a)/s} \mathrm{e}_q(f(a+ms+r)-f(a+ms)) \ll \frac{x}{sq}|S_0(q)| + \sum_{1\leq|\ell|\leq q/2} \frac{|S_\ell(q)|}{\ell},$$

where

$$S_\ell(q) = \sum_{m \,(\mathrm{mod}\, q)} \mathrm{e}_q\big(f(a+ms+r)-f(a+ms)+\ell m\big).$$

Let q_1 be the largest divisor of q which is squarefree, coprime to rs and q/q_1, and has no prime factor in $\mathcal{Q}_f$:

$$q_1 = \prod_{\substack{p\| q,\, p\nmid rs\\ p\notin\mathcal{Q}_f}} p.$$

By the Chinese remainder theorem, we may write $S_\ell(q) = T_1T_2$, where

$$T_1 = \sum_{m \,(\mathrm{mod}\, q_1)} \mathrm{e}_{q_1}\big((q/q_1)^{-1}(f(a+ms+r)-f(a+ms)+\ell m)\big),$$

$$T_2 = \sum_{m \,(\mathrm{mod}\, q/q_1)} \mathrm{e}_{q/q_1}\big(q_1^{-1}(f(a+ms+r)-f(a+ms)+\ell m)\big).$$

On T_2 we use the trivial bound $|T_2| \leq q/q_1$. Concerning T_1, by Lemma 5 applied with $f(X)$ replaced by $f(a+sX+r)-f(a+sX)+\ell X$, we get

$$T_1 \ll_\varepsilon q_1^{1/2+\varepsilon}(q_1, \ell + sf'(a+sX+r) - sf'(a+sX))^{1/2}.$$

Let $v \in \mathbb{Z}$ be such that $sv \equiv 1 \pmod{q}$. We apply Lemma 6 with $r \leftarrow rv$ and $f(X) \leftarrow f(a+sX)$. We obtain $(q_1, \ell + sf'(a+sX+r) - sf'(a+sX)) = O(1)$, therefore $|T_1| = O(q_1^{1/2+\varepsilon})$, and so

$$|S_\ell(q)| \ll q^{1+\varepsilon}q_1^{-1/2}.$$

This leads to the desired conclusion. ∎

3. Auxiliary results on automata. In this section we quote a few results from the literature which we will use in our proof of Theorem 2.

From now on, we let (a_n) denote a fixed automatic sequence corresponding to a strongly connected automaton $\mathcal{A} = (Q', \Sigma, \delta', q_0', Q_0)$, where $\delta'(q_0', 0) = q_0'$. We follow the arguments and notations of [Mül17] and consider a naturally induced *transducer* $\mathcal{T}_{\mathcal{A}} = (Q, \Sigma, \delta, q_0, \Delta, \lambda)$, where $Q \subset (Q')^{n_0}, \pi_1(q_0) = q_0'$, δ is a transition function which is synchronizing (2) and $\lambda : Q \times \Sigma \to \Delta \subset S_{n_0}$ is an output function which "attaches" a permutation to each transition in the naturally induced transducer.

A transducer can be viewed as a mean to define functions: on the input word $\mathbf{w} = w_1 w_2 \dots w_r$ the transducer enters successively the states $q_0 = \delta(q_0, \varepsilon), \delta(q_0, w_1), \dots, \delta(q_0, w_1 w_2 \dots w_r)$ and produces the outputs

$$\lambda(q_0, w_1), \lambda(\delta(q_0, w_1), w_2), \dots, \lambda(\delta(q_0, w_1 w_2 \dots w_{r-1}), w_r).$$

The function $T(\mathbf{w})$ is then defined as

$$T(\mathbf{w}) := \prod_{j=0}^{r-1} \lambda(\delta(q_0, w_1 w_2 \dots w_j), w_{j+1}).$$

We also define the slightly more general form

$$T(q, \mathbf{w}) := \prod_{j=0}^{r-1} \lambda(\delta(q, w_1 w_2 \dots w_j), w_{j+1}).$$

Proposition 2.5 of [Mül17] shows how the original automaton and the naturally induced transducer are related:

$$a_n = \tau(\delta'(q_0', (n)_k)) = \tau\big(\pi_1(T(q_0, (n)_k) \cdot \delta(q_0, (n)_k))\big). \tag{3.1}$$

The following theorem highlights an important closure property of naturally induced transducers.

THEOREM 7 ([Mül17, Theorem 2.7]). *Let $\mathcal{A}$ be a strongly connected automaton. There exists a minimal $d \in \mathbb{N}$, $m_0 \in \mathbb{N}$, a naturally induced transducer $\mathcal{T}_{\mathcal{A}}$ and a subgroup G of Δ such that:*

- *For all $q \in Q$, $\mathbf{w} \in (\Sigma^d)^*$ we have $T(q, \mathbf{w}) \in G$.*
- *For all $g \in G$, $q, \overline{q} \in Q$ and $n \geq m_0$ we have*

$$\{T(q, \mathbf{w}) : \mathbf{w} \in \Sigma^{nd},\ \delta(q, \mathbf{w}) = \overline{q}\} = G.$$

The integers $d = d(\mathcal{A})$ and $m_0 = m_0(\mathcal{A})$ only depend on $\mathcal{A}$, but not on its initial state q_0'.

---

(2) This means that there exists a *synchronizing word* $\mathbf{w}_0$, i.e., $\delta(q_0, \mathbf{w}_0) = \delta(q, \mathbf{w}_0)$ for all $q \in Q$.

Finally, [Mül17, Corollary 2.26] shows that there is $\mathcal{A} = (Q', \Sigma, q_0', \delta', \tau)$ generating (a_n) such that $d(\mathcal{A}) = 1$ and we consider a naturally induced transducer which fulfills Theorem 7.

One crucial idea in [Mül17] was that the functions T and δ corresponding to a naturally induced transducer behave "independently" of each other. Thus, we start by giving an important property of synchronizing automata.

LEMMA 8 (see [DDM15, Lemma 2.2]). *Let $\mathcal{A}$ be a synchronizing DFAO with synchronizing word $\mathbf{w} \in \Sigma^{m_0}$. There exists $\eta > 0$ depending only on m_0 and k such that the number of integers $n \in (y, y + x]$ such that*

$$\delta(q, (n)_k) \neq \delta(q, (n)_k^\lambda)$$

is bounded by $O(xk^{-\eta\lambda})$ uniformly for $\lambda < \lfloor \log_k(x) \rfloor$ and $y \geq 0$. Here, $(n)_k^\lambda$ denotes the digital representation of n truncated at the λth digit, in other words $(n)_k^\lambda = (m)_k$ where $m \in [0, k^\lambda) \cap \mathbb{N}$ and $m \equiv n \pmod{k^\lambda}$.

The next result is the carry property for automatic sequences, or more precisely T.

DEFINITION 9. A function $f : \mathbb{N} \to U_d$ has the *carry property* if there exists $\eta > 0$ such that uniformly for $\lambda, \alpha, \rho \in \mathbb{N}$ with $\rho < \lambda$, the number of integers $0 \leq \ell < k^\lambda$ such that there exists $(n_1, n_2) \in \{0, \ldots, k^\alpha - 1\}^2$ with

$$f(\ell k^\alpha + n_1 + n_2)^H f(\ell k^\alpha + n_1) \neq f_{\alpha+\rho}(\ell k^\alpha + n_1 + n_2)^H f_{\alpha+\rho}(\ell k^\alpha + n_1) \tag{3.2}$$

is at most $O(k^{\lambda - \eta\rho})$ where the implied constant may depend only on k and f.

LEMMA 10 ([Mül17, Lemma 4.9]). *The carry property holds, uniformly in r, for $f(n) = D(T(n + r))$ where D is a unitary and irreducible representation of G, η is given by* [DDM15, Lemma 2.2], *and the implied constant does not depend on r.*

To use the carry property efficiently, we need the following lemma which is a generalization of van der Corput's inequality.

LEMMA 11 (see [DM12, Lemma 5]). *Let $y \geq 0$ and $x \geq 1$, and let $Z(n) \in \mathbb{C}^{m \times m}$ be given for all $n \in (y, y + x]$. Then for any real $R \geq 1$ and any integer $k \geq 1$,*

$$\begin{aligned} &\Big\| \sum_{y < n \leq y + x} Z(n) \Big\|_F^2 \\ &\leq \frac{x + k(R-1) + 1}{R} \sum_{|r| < R} \left(1 - \frac{|r|}{R}\right) \sum_{y < n, n + kr \leq y + x} \operatorname{tr}(Z(n + kr)^H Z(n)), \end{aligned} \tag{3.3}$$

where $\operatorname{tr}(Z)$ denotes the trace of Z, and $\|Z\|_F$ the Frobenius norm of Z.

We now quote some results from representation theory. Let G be a finite group. A *representation* D is a continuous homomorphism $D : G \to U_m$, where U_m denotes the group of unitary $m \times m$ matrices over $\mathbb{C}$. The representation D is called *irreducible* if there exists no non-trivial subspace $V \subset U_m$ such that $D(g)V \subseteq V$ for all $g \in G$. It is well-known that there are only finitely many equivalence classes of irreducible unitary representations of G (see for example [Ser77, Part I, Section 2.5]). The Peter–Weyl theorem (see for example [KN74, Chapter 4, Theorem 1.2]) states that the entry functions of irreducible representations (suitably renormalized) form an orthonormal basis of $L^2(G)$. Thus we can express any function $f : G \to \mathbb{C}$ by the entry functions:

Lemma 12. *Let G be a finite group. There exists $M_0 \in \mathbb{N}$ and M_0 irreducible unitary representations $(D^{(\ell)})_{0\le\ell<M_0}$ of G, not necessarily distinct, and written as matrices $D^{(\ell)} = (d_{i,j}^{(\ell)})_{i,j}$, such that for any $f : G \to \mathbb{C}$ there exist coefficients (c_ℓ) and indices (i_ℓ), (j_ℓ) with*

$$f(g) = \sum_{0\le\ell<M_0} c_\ell d_{i_\ell j_\ell}^{(\ell)}(g)$$

for all $g \in G$ and $\sum |c_\ell| \ll \|f\|_1$.

4. Van der Corput differentiation. The following proposition reduces the study of automatic sequences with strongly connected underlying automaton to bounds on correlation sums.

Proposition 13. *Let $g : \mathbb{N}_{>0} \to \mathbb{C}$ be a function with $|g(n)| \le 1$, let $x \ge 1$ and $y \ge 0$ be real numbers, and let (a_n) be an automatic sequence in base k, with strongly connected underlying automaton $\mathcal{A}$. Set*

$$U(x,y;h;q,a) := \sum_{\substack{y<n\le y+x \\ n\equiv a \,(\mathrm{mod}\, q)}} g(n)\overline{g(n+h)}. \tag{4.1}$$

Then for some $\eta > 0$ depending on $\mathcal{A}$, and all $\lambda_1, \lambda_2 \in \mathbb{N}$, with $M := k^{\lambda_1}$, $R := k^{\lambda_2}$ satisfying $RM^2 \le x/10$, we have

$$\Big|\sum_{y<n\le y+x} a_n g(n)\Big| \ll_{\mathcal{A}} xM^{-\eta} + \sum_{0\le m<M} \bigg(\frac{x}{RM} \sum_{0\le r<R} \sum_{\substack{0\le m'<RM^2 \\ m'\equiv m \,(\mathrm{mod}\, M)}} |U(x,y;rM;RM^2,m')|\bigg)^{1/2}.$$

Remark. It was proved by Sarnak that his Möbius randomness conjecture for all deterministic flows would follow from the Chowla conjecture (see [Sar12, Tao12]) concerning correlations of the Möbius function. Proposition 13 could be interpreted as a quantified version of this phenomenon for automatic sequences; we see that in this case, binary correlations provide sufficient information. Note however that the moduli $q = RM^2$ of the arithmetic progressions involved in our statement are rather large compared with the shifts $h = rM$.

We prove Proposition 13 in the remainder of this section.

4.1. Naturally induced transducer. We use the concept of naturally induced transducer to rewrite the sequence (a_n). We (still) consider a naturally induced transducer which fulfills Theorem 7. By (3.1), we can rewrite $a_n = \tau(\pi_1(T(q_0,(n)_k) \cdot \delta(q_0,(n)_k)))$. Therefore,

$$a_n = \sum_{q\in Q}\sum_{\sigma\in G} \tau(\pi_1(\sigma\cdot q))\, \mathbf{1}_{[T(q_0,(n)_k)=\sigma]}\, \mathbf{1}_{[\delta(q_0,(n)_k)=q]}\,.$$

Let

$$\mathcal{I} = \mathbb{Z} \cap (y, y+x]$$

with $y \in \mathbb{N}_{\geq 0}$ and $x \in \mathbb{N}_{>0}$. The above allows us to rewrite

$$S_0(\mathcal{I}) := \sum_{y<n\leq y+x} a_n g(n) = \sum_{q\in Q}\sum_{\sigma\in G} \tau(\pi_1(\sigma\cdot q)) S_1(\mathcal{I};\sigma,q), \tag{4.2}$$

where

$$S_1(\mathcal{I};\sigma,q) := \sum_{y<n\leq y+x} \mathbf{1}_{[T(q_0,(n)_k)=\sigma]}\, \mathbf{1}_{[\delta(q_0,(n)_k)=q]}\, g(n).$$

This implies

$$|S_0(\mathcal{I})| \ll_{\mathcal{A}} \sum_{q\in Q}\sum_{\sigma\in G} |S_1(\mathcal{I};\sigma,q)|.$$

4.2. Van der Corput differencing and the carry property. Let $1 \leq M \leq x$, $M = k^{\lambda_1}$ be a power of k, to be determined later. We use the fact that it is usually sufficient to read the last few digits of $(n)_k$ to determine $\delta(q,(n)_k)$ (see Lemma 8). This allows us to rewrite

$$\begin{aligned} S_1(\mathcal{I};\sigma,q) &= \sum_{y<n\leq y+x} \mathbf{1}_{[T(q_0,(n)_k)=\sigma]}\, \mathbf{1}_{[\delta(q_0,(n)_k)=q]}\, g(n) \\ &= \sum_{0\leq m<M} \mathbf{1}_{[\delta(q_0,(m)_k)=q]}\, S_2(\mathcal{I};m,\sigma) + O(xM^{-\eta}), \end{aligned} \tag{4.3}$$

where $\eta > 0$ only depends on the length of the synchronizing word $\mathbf{w}_0$ of the naturally induced transducer $\mathcal{T}_A$, and

$$S_2(\mathcal{I};m,\sigma) := \sum_{\substack{y<n\leq y+x\\ n\equiv m \,(\mathrm{mod}\, M)}} \mathbf{1}_{[T(q_0,(n)_k)=\sigma]}\, g(n).$$

We use ideas of representation theory to deal with $\mathbf{1}_{[T(q_0,(n)_k)=\sigma]}$. By Lemma 12, we can write

$$\mathbf{1}_{[T(q_0,(n)_k)=\sigma]} = \sum_{0\le \ell < M_0} c_\ell d_{i_\ell j_\ell}^{(m_\ell)}(T(q_0,(n)_k))$$

for some irreducible unitary representations $D^{(m')}$. This gives

$$\sum_{\substack{y<n\le y+x\\ n\equiv m \,(\mathrm{mod}\, M)}} \mathbf{1}_{[T(q_0,(n)_k)=\sigma]}\, g(n) = \sum_{0\le \ell<M_0} c_\ell \sum_{\substack{y<n\le y+x\\ n\equiv m \,(\mathrm{mod}\, M)}} d_{i_\ell j_\ell}^{(m_\ell)}(T(q_0,(n)_k))g(n)$$

and

$$\Big|\sum_{\substack{y<n\le y+x\\ n\equiv m \,(\mathrm{mod}\, M)}} d_{i_\ell j_\ell}^{(m_\ell)}(T(q_0,(n)_k))g(n)\Big| \le \Big\|\sum_{\substack{y<n\le y+x\\ n\equiv m \,(\mathrm{mod}\, M)}} D^{(m_\ell)}(T(q_0,(n)_k))g(n)\Big\|_F,$$

where we let $\|\cdot\|_F$ denote the Frobenius norm.

Thus, we find

$$|S_2(\mathcal{I};m,\sigma)| \le \sum_{0\le\ell<M_0} |c_\ell|\, \|S_3(\mathcal{I};m,D^{(m_\ell)})\|_F,$$

where

$$S_3(\mathcal{I};m,D) := \sum_{\substack{y<n\le y+x\\ n\equiv m \,(\mathrm{mod}\, M)}} D(T(q_0,(n)_k))g(n).$$

This gives in total

$$|S_0(\mathcal{I})| \ll_{\mathcal{A}} \max_{D} \sum_{0\le m<M} \|S_3(\mathcal{I};m,D)\|_F + O(xM^{-\eta}). \tag{4.4}$$

We use Lemma 11 for the sequence

$$Z(n) = D(T(q_0,(nM+m)_k))g(nM+m)$$

to get

$$\|S_3(\mathcal{I};m,D)\|_F^2 \le \frac{xM^{-1}+M(R-1)+1}{R} \sum_{|r|<R}\Big(1-\frac{|r|}{R}\Big)\mathrm{tr}(S_4(\mathcal{J}_r;m,D,r)),$$

where $\mathcal{J}_r := \{n : y<n, n+rM\le y+x\}$ and

$$S_4(\mathcal{J};m,D,r) := \sum_{\substack{n\in\mathcal{J}\\ n\equiv m \,(\mathrm{mod}\, M)}} \big(D(T(q_0,(n+rM)_k))^H D(T(q_0,(n)_k))\big)g(n)\overline{g(n+rM)}.$$

We choose $R = k^{\lambda_2}$ and $\lambda_2 \in \mathbb{N}$ subject to $RM^2 < x/10$, which gives

$$\|S_3(\mathcal{I}; m, D)\|_F^2 \ll \frac{x}{RM} \sum_{0 \le r < R} \|S_4(\mathcal{I}; m, D, r)\|_F + O(Rx/M), \tag{4.5}$$

where the error term is due to the replacement of $\mathcal{J}_r$ by $\mathcal{I}$.

Letting temporarily $a = y + 1$, we rewrite $n = n_1 RM + n_2 M + m + a$ to find

$$\begin{aligned} D(T(q_0, (n + rM)_k))^H D(T(q_0, (n)_k)) \\ &= D\big(T(q_0, (n_1 RM + (n_2 M + m + a) + rM)_k)\big)^H \\ &\quad \times D\big(T(q_0, (n_1 RM + (n_2 M + m + a))_k)\big). \end{aligned}$$

We apply Lemma 10 with $\alpha = \lambda_1 + \lambda_2, \rho = \lambda_1$ and $\ell = n_1$. This gives

$$\begin{aligned} D(T(q_0, (n + rM)_k))^H D(T(q_0, (n)_k)) \\ &= D\big(T_{2\lambda_1+\lambda_2}(q_0, (n_1 RM + (n_2 M + m + a) + rM)_k)\big)^H \\ &\quad \times D\big(T_{2\lambda_1+\lambda_2}(q_0, (n_1 RM + (n_2 M + m + a))_k)\big) \\ &= D(T_{2\lambda_1+\lambda_2}(q_0, (n + rM)))^H D(T_{2\lambda_1+\lambda_2}(q_0, (n)_k)), \end{aligned}$$

for all but $O(xR^{-1}M^{-1-\eta})$ values of $n_1 \in [0, x/RM)$, and therefore for all but $O(xM^{-1-\eta})$ values of $n \in \mathcal{I}$ (for fixed m).

Thus, we find

$$\begin{aligned} &S_4(\mathcal{I}; m, D, r) \\ &= \sum_{\substack{0 \le m' < RM^2 \\ m' \equiv m \,(\mathrm{mod}\, M)}} D(T_{2\lambda_1+\lambda_2}(q_0, m' + rM))^H D(T_{2\lambda_1+\lambda_2}(q_0, m')) S_5(\mathcal{I}; m', r) \\ &\quad + O(xM^{-1-\eta}), \end{aligned} \tag{4.6}$$

where

$$S_5(\mathcal{I}; m', r) := \sum_{\substack{y < n \le y + x \\ n \equiv m' \,(\mathrm{mod}\, RM^2)}} g(n) \overline{g(n + rM)}. \tag{4.7}$$

Note that the trivial estimate $S_5 = O(x/(RM^2))$ gives back the trivial estimate $S_0 \ll x$, so a non-trivial bound on S_5 gives a non-trivial bound on S_0.

Combining (4.5) and (4.6) gives

$$\begin{aligned} \|S_3(\mathcal{I}; m, D)\|_F^2 &\ll \frac{x}{RM} \sum_{0 \le r < R} \|S_4(\mathcal{I}; m, D, r)\|_F + O(x) \\ &\ll_{\mathcal{A}} \frac{x}{RM} \sum_{0 \le r < R} \sum_{\substack{0 \le m' < RM^2 \\ m' \equiv m \,(\mathrm{mod}\, M)}} |S_5(\mathcal{I}; m', r)| + O(x^2 M^{-2-\eta}). \end{aligned}$$

This together with the definition (4.1) finishes the proof of Proposition 13.

5. Proof of Theorem 2 in the strongly connected case. From Proposition 13, we will deduce Theorem 2 in the following special case.

Proposition 14. *Theorem 2 holds for sequences (a_n) whose underlying automata are strongly connected.*

The proof is split in two cases, according to whether or not the rational fraction f is a quadratic polynomial.

5.1. The non-quadratic case. We assume first that f is not a quadratic polynomial. Let $R = M = k^\lambda$, and

$$q_1 = \prod_{\substack{p\| q,\, p\nmid k \\ p\notin \mathcal{Q}_f}} p.$$

We also assume that $x \geq q q_1^{-1/2}$ without loss of generality, since otherwise the right-hand side of (1.2) is larger than the trivial bound $O(x)$ for the left-hand side. Recall the definition (4.1). We use Lemma 4 with $g(n) = \mathrm{e}_q(f(n))$ and our choice of R and M to find that

$$\begin{aligned}\sum_{0\le r<k^\lambda} \sum_{\substack{0\le m'<k^{3\lambda} \\ m'\equiv m \,(\mathrm{mod}\, k^\lambda)}} &|U(x,y;rM;RM^2,m')| \\ &\ll_\varepsilon \sum_{0\le r<k^\lambda} k^{2\lambda} q^\varepsilon \Big(\frac{x}{k^{3\lambda}} + q\Big) \prod_{\substack{p\mid q,\, p\nmid rk \\ p\notin T_f}} p^{-1/2} \\ &\ll k^{2\lambda}\Big(\frac{x}{k^{3\lambda}} + q\Big) q_1^{-1/2} q^\varepsilon \sum_{0\le r<k^\lambda} (r,q)^{1/2}.\end{aligned}$$

Thus, Proposition 13 implies that for some $\eta > 0$ depending on $\mathcal{A}$,

$$\Big|\sum_{n\in\mathcal{I}} a_n \mathrm{e}_q(f(n))\Big| \ll_{\mathcal{A},\varepsilon} x\Big(\frac{k^\lambda}{q_1^{1/2}} + \frac{qk^{4\lambda}}{xq_1^{1/2}}\Big)^{1/2} q^{\varepsilon/2} + O(xk^{-\lambda\eta/2})$$

uniformly in λ such that $k^{3\lambda} < x/10$. We choose λ such that

$$k^\lambda \asymp_k \min((q_1^{1/2} q^{-1} x)^{1/8}, (q_1)^{1/4}).$$

This gives

$$|S_0(\mathcal{I})| \ll_{\mathcal{A},k,\varepsilon,d} xq^\varepsilon \Big(\frac{1}{q_1^{1/4}} + \Big(\frac{q}{q_1^{1/2}x}\Big)^{1/8}\Big)^{1/2} + x\Big(\frac{1}{q_1^{1/4}} + \Big(\frac{q}{q_1^{1/2}x}\Big)^{1/8}\Big)^{\eta}, \tag{5.1}$$

and implies our claimed bound (1.2) for $c = \min(\eta/16, 1/32)$.

5.2. The quadratic case. Here again we assume that $g(n) = \mathrm{e}_q(f(n))$. If f is quadratic, then for the purpose of bounding (4.1) we may assume

$f(X) = \frac{u}{v}X^2$ with $v \neq 0$ and $(qu, v) = 1$. Let $s = RM^2$, where R and M are powers of k satisfying $1 \leq RM < x/10$. By Lemma 4, we have

$$|U(x, y; rM; RM^2, m')| \ll \min\biggl(\frac{x}{RM^2}, \biggl\| \frac{2u\bar{v}rRM^2}{q} \biggr\|^{-1}\biggr).$$

Assume now that $(RM)^2 < q/(4u)$, which does not contradict the hypotheses $R, M \geq 1$ if we let q be large enough in terms of u. Then

$$\frac{2u\bar{v}rRM^2}{q} \equiv \frac{2urRM^2}{qv} - \frac{2u\bar{q}rRM^2}{v} \pmod 1.$$

By our hypothesis $(RM)^2 < q/(4|u|)$, as soon as $v \nmid 2rRM^2$ we obtain

$$\biggl\| \frac{2u\bar{v}rRM^2}{q} \biggr\| \geq \frac{1}{v} - \biggl| \frac{2urRM^2}{qv} \biggr| \geq \frac{1}{2v} \gg_f 1.$$

If, on the other hand, $v \mid 2rRM^2$, then

$$\biggl\| \frac{2u\bar{v}rRM^2}{q} \biggr\| = \biggl| \frac{2urRM^2}{qv} \biggr| = \frac{2|u|rRM^2}{q|v|}$$

since the latter is less than $1/2$, again by our hypothesis $(RM)^2 < q/(4|u|)$. In any case,

$$|U(x, y; rM; RM^2, m')| \ll \min\biggl(\frac{x}{RM^2}, \frac{q}{rRM^2}\biggr),$$

and therefore

$$\sum_{\substack{0 \leq m' < RM^2 \\ m' \equiv m \,(\mathrm{mod}\, M)}} |U(x, y; rM; RM^2, m')| \ll \min\biggl(\frac{x}{M}, \frac{q}{rM}\biggr).$$

We sum the previous bound over $r < R$. We obtain

$$\begin{aligned} \sum_{r<R} \sum_{\substack{0 \leq m' < RM^2 \\ m' \equiv m \,(\mathrm{mod}\, M)}} |U(x, y; rM; RM^2, m')| &\ll \frac{x}{M} + \sum_{1 \leq r < R} \frac{q}{rM} \\ &\ll \frac{x + q \log R}{M}. \end{aligned}$$

We now pick $R \asymp_k \min(x/M^2, \sqrt{q}/M)$, and find by Proposition 13 that

$$\Bigl|\sum_{n \in \mathcal{I}} a_n \mathrm{e}_q(f(n))\Bigr| \ll_{\mathcal{A},k,\varepsilon,d} (xq)^{\varepsilon} \biggl(x(x+q)\biggl(\frac{M^2}{x} + \frac{M}{q^{1/2}}\biggr)\biggr)^{1/2} + xM^{-\eta/2}.$$

If $x \leq q$, we pick $M \asymp_k (x/\sqrt{q})^{1/(1+2\eta)}$, and if $x > q$, we pick $M \asymp_k q^{1/(2+4\eta)}$. In any case we get

$$\Bigl|\sum_{n \in \mathcal{I}} a_n \mathrm{e}_q(f(n))\Bigr| \ll x^{1+\varepsilon}\biggl(\frac{1}{q} + \frac{q}{x^2}\biggr)^{c}$$

with $c = \eta/(2 + 4\eta)$, and our claimed bound follows.

6. Proof for non-strongly connected automata. We will deduce the full generality of Theorem 2 from Proposition 14 and the following fact.

PROPOSITION 15. *Let $g:\mathbb{N}\to\mathbb{C}$ be a function with $|g(n)|\le 1$, and assume that for every strongly connected automatic sequence $\mathbf{b}=(b_n)$, there is a non-decreasing function $E(\mathbf{b},\cdot):\mathbb{R}_+\to\mathbb{R}_+$ such that*

$$\Big|\sum_{y<n\le y+x} b_n g(n+r)\Big| \le E(\mathbf{b},x) \qquad (r\in\mathbb{Z},\ y\ge 0,\ x\ge 1). \tag{6.1}$$

Then with any automatic sequence (a_n), not necessarily strongly connected, we may associate a finite set $\{\mathbf{b}^{(j)}=(b_n^{(j)})\}_{j=1}^J$ of strongly connected automatic sequences and a positive number $\delta>0$ such that for all $y\ge 0$, $x\ge 1$ and $\sigma\in\mathbb{N}$ with $K:=k^\sigma\in[1,x]$, we have

$$\Big|\sum_{y<n\le y+x} a_n g(n)\Big| \ll x^{1-\delta}K^\delta + xK^{-1}\max_j E(\mathbf{b}^{(j)},K). \tag{6.2}$$

REMARK. It is important to note the requirement that the hypothesized upper bound (6.1) is uniform with respect to r.

Proof of Proposition 15. Let $\mathcal{A}=(Q,\Sigma,\delta,q_0,\tau)$ be the automaton underlying (a_n), and define

$$\mathcal{R}:=\{r\in\mathbb{N}:\delta(q,(r)_k)\text{ belongs to a final component of }\mathcal{A}\text{ for any }q\in Q\}.$$

Then we have the uniform bound

$$|(y,y+x]\cap\mathbb{N}\smallsetminus\mathcal{R}|\ll x^{1-\delta} \qquad (y\ge 0,\ x\ge 1) \tag{6.3}$$

for some $\delta>0$ depending on $\mathcal{A}$. We let $\{(b_n^{(j)})\}_{j=1}^J$ be the finite set of all automatic sequences associated with final components of $\mathcal{A}$ (as described in [Mül17, Proposition 2.25]), with the same output function τ.

We consider some fixed $y\ge 0$ and $x\ge 1$. In proving (6.2), we may assume that x is large enough in terms of $\mathcal{A}$. Let $\sigma\in\mathbb{N}$ with $1\le K:=k^\sigma\le x$. We split the sum on the left-hand side of (6.2) into congruence classes modulo K, getting

$$\sum_{y\le n<y+x} a_n g(n) = \sum_{r\ge 0}\ \sum_{\substack{0\le n<K\\ y\le rK+n<y+x}} a_{rK+n}g(rK+n).$$

Note that the sum over n is void unless $r\in(y/K-1,(y+x)/K)$. From this fact, the bound (6.3) and our hypothesis $\|g\|_\infty\le 1$, we obtain

$$\sum_{r\ge 0}\ \sum_{\substack{0\le n<K\\ y\le rK+n<y+x}} a_{rK+n}g(rK+n) = \sum_{\substack{r\ge 0\\ r\in\mathcal{R}}}\ \sum_{\substack{0\le n<K\\ y\le rK+n<y+x}} a_{rK+n}g(rK+n) + O(x^{1-\delta}K^\delta).$$

For $r \in \mathcal{R}$, our automaton reads numbers from left to right, so that $a_{rK+n} = b_n^{(j)}$ for some j (depending on r); we recall that there are only finitely many possibilities for j. Therefore,

$$\Big|\sum_{\substack{r\geq 0\\ r\in\mathcal{R}}}\ \sum_{\substack{0\leq n<K\\ y\leq rK+n<y+x}} a_{rK+n}g(rK+n)\Big| \leq \sum_{y/K-1<r<(y+x)/K} \max_j \Big|\sum_{\substack{0\leq n<K\\ y\leq rK+n<y+x}} b_n^{(j)} g(rK+n)\Big|.$$

In the inner sum, the size conditions on n describe an interval of length K, for all but at most two values of r. Gathering the above and using our hypothesis (6.1), we find

$$\Big|\sum_{y\leq n<y+x} a_n g(n)\Big| \ll \sum_{y/K-1\leq r<(y+x)/K} \max_j E(\mathbf{b}^{(j)}, K) + x^{1-\delta}K^{\delta} \ll xK^{-1}\max_j E(\mathbf{b}^{(j)},K) + x^{1-\delta}K^{\delta}. \ \blacksquare$$

Proof of Theorem 2. We prove (1.2); the argument for (1.3) is similar and slightly simpler. Proposition 14 shows that (1.2) holds when (a_n) is associated with a strongly connected automaton. Note that the upper bound (1.2) only depends on the degree of f (while (1.3) only depends on the leading coefficient of f). Moreover, if $r \in \mathbb{Z}$ and $\widetilde{f}(X) := f(X+r)$, then $\mathcal{Q}_{\widetilde{f}} = \mathcal{Q}_f$. We deduce that (1.2) also holds, with the same implied constant, for the quantity

$$\sum_{n\in\mathcal{I}} a_n \mathrm{e}_q(f(n+r))$$

uniformly in $r \in \mathbb{Z}$, when the automaton underlying (a_n) is strongly connected. The hypothesis (6.1) is therefore satisfied with

$$E((a_n),x) = B_{\mathcal{A},\varepsilon}x^{1+\varepsilon}\left(\frac{1}{q_1} + \frac{q^2}{q_1x^2}\right)^c,$$

where $c > 0$ depends on $\mathcal{A}$, and $B_{\mathcal{A},\varepsilon}$ depends at most on $\mathcal{A}$ and ε.

Assume now that (a_n) is not associated with a strongly connected automaton. For any $K \in [1, x]$ which is a power of x, we obtain by Proposition 15 the bound

$$\Big|\sum_{y<n\leq y+x} a_n \mathrm{e}_q(f(n))\Big| \ll x^{1-\delta}K^{\delta} + xK^{\varepsilon}\left(\frac{1}{q_1} + \frac{q^2}{q_1K^2}\right)^{c_1}$$

for some $c_1 > 0$ depending on $\mathcal{A}$. We optimize by letting

$$K \asymp_k \min(x, (xq^2q_1^{-1})^{1/3}).$$

The claimed bound (1.2) follows with c replaced by $\min(c_1/3, \delta/3)$. $\blacksquare$

Acknowledgements. Both authors acknowledge support by the project MuDeRa (Multiplicativity, Determinism and Randomness), which is a joint project between the ANR (Agence Nationale de la Recherche) and the FWF (Austrian Science Fund). Moreover, the second author was supported by FWF, project F5502-N26, which is a part of the Special Research Program "Quasi Monte Carlo Methods: Theory and Applications". The authors thank C. Mauduit, É. Fouvry and I. Shparlinski for helpful discussions and remarks, and an anonymous referee for useful remarks on an earlier version of the manuscript.

References

[AS03] J.-P. Allouche and J. Shallit, *Automatic Sequences. Theory, Applications, Generalizations*, Cambridge Univ. Press, Cambridge, 2003.

[BCS02] W. D. Banks, A. Conflitti, and I. E. Shparlinski, *Character sums over integers with restricted g-ary digits*, Illinois J. Math. 46 (2002), 819–836.

[Blo04] V. Blomer, *Shifted convolution sums and subconvexity bounds for automorphic L-functions*, Int. Math. Res. Notices 2004, 3905–3926.

[CFH+14] W. Castryck, É. Fouvry, G. Harcos, E. Kowalski, P. Michel, P. Nelson, E. Paldi, J. Pintz, A. V. Sutherland, T. Tao, and X.-F. Xie, *New equidistribution estimates of Zhang type*, Algebra Number Theory 8 (2014), 2067–2199.

[DDM15] J.-M. Deshouillers, M. Drmota, and C. Müllner, *Automatic sequences generated by synchronizing automata fulfill the Sarnak conjecture*, Studia Math. 231 (2015), 83–95.

[Drm14] M. Drmota, *Subsequences of automatic sequences and uniform distribution*, in: Uniform Distribution and Quasi-Monte Carlo Methods, Radon Ser. Comput. Appl. Math. 15, de Gruyter, Berlin, 2014, 87–104.

[DM12] M. Drmota and J. F. Morgenbesser, *Generalized Thue–Morse sequences of squares*, Israel J. Math. 190 (2012), 157–193.

[FKP+16] S. Ferenczi, J. Kułaga-Przymus, M. Lemańczyk, and C. Mauduit, *Substitutions and Möbius disjointness*, in: Ergodic Theory, Dynamical Systems, and the Continuing Influence of John C. Oxtoby, Contemp. Math. 678, Amer. Math. Soc., Providence, RI, 2016, 151–173.

[FKM14] É. Fouvry, E. Kowalski, and P. Michel, *Algebraic trace functions over the primes*, Duke Math. J. 163 (2014), 1683–1736.

[FKM15] É. Fouvry, E. Kowalski, and P. Michel, *A study in sums of products*, Philos. Trans. Roy. Soc. A 373 (2015), no. 2040, 20140309, 26 pp.

[FKM+17] É. Fouvry, E. Kowalski, P. Michel, C. S. Raju, J. Rivat, and K. Soundararajan, *On short sums of trace functions*, Ann. Inst. Fourier (Grenoble) 67 (2017), 423–449.

[FM98] É. Fouvry et P. Michel, *Sur certaines sommes d'exponentielles sur les nombres premiers*, Ann. Sci. École Norm. Sup. (4) 31 (1998), 93–130.

[Han17] G. Hanna, *Sur les occurrences des mots dans les nombres premiers*, Acta Arith. 178 (2017), 15–42.

[Irv15] A. J. Irving, *The divisor function in arithmetic progressions to smooth moduli*, Int. Math. Res. Notices 2015, 6675–6698.

[IK04] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloq. Publ. 53, Amer. Math. Soc., Providence, RI, 2004.

[Kor00] M. A. Korolev, *Incomplete Kloosterman sums and their applications*, Izv. Ross. Akad. Nauk Ser. Mat. 64 (2000), no. 6, 41–64 (in Russian).

[KN74] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Pure Appl. Math., Wiley-Interscience, New York, 1974.

[Mau86] C. Mauduit, *Automates finis et ensembles normaux*, Ann. Inst. Fourier (Grenoble) 36 (1986), no. 2, 1–25.

[MR10] C. Mauduit et J. Rivat, *Sur un problème de Gelfond : la somme des chiffres des nombres premiers*, Ann. of Math. (2) 171 (2010), 1591–1646.

[MR15] C. Mauduit and J. Rivat, *Prime numbers along Rudin–Shapiro sequences*, J. Eur. Math. Soc. 17 (2015), 2595–2642.

[May16] J. A. Maynard, *Primes with restricted digits*, arXiv:1604.01041 (2016).

[Mül17] C. Müllner, *Automatic sequences fulfill the Sarnak conjecture*, Duke Math. J. 166 (2017), 3219–3290.

[OS12a] A. Ostafe and I. E. Shparlinski, *Exponential sums over points of elliptic curves with reciprocals of primes*, Mathematika 58 (2012), 21–33.

[OS12b] A. Ostafe and I. E. Shparlinski, *Multiplicative character sums and products of sparse integers in residue classes*, Period. Math. Hungar. 64 (2012), 247–255.

[Sar12] P. Sarnak, *Möbius randomness and dynamics*, Not. S. Afr. Math. Soc. 43 (2012), 89–97.

[Ser77] J.-P. Serre, *Linear Representations of Finite Goups*, Grad. Texts in Math. 42, Springer, New York, 1977.

[Tao12] T. Tao, *The Chowla conjecture and the Sarnak conjecture*, https://terrytao.wordpress.com/2012/10/14/the-chowla-conjecture-and-the-sarnak-conjecture, 2012.

[Wei48] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204–207.

Sary Drappeau
Aix Marseille Université
CNRS, Centrale Marseille
I2M UMR 7373
13453 Marseille, France
E-mail: sary-aurelien.drappeau@univ-amu.fr

Clemens Müllner
Institut für Diskrete Mathematik
und Geometrie
TU Wien
Wiedner Hauptstr. 8–10
1040 Wien, Austria
E-mail: clemens.muellner@tuwien.ac.at