Combinatorics, Probability and Computing (2012) 21, 942–951. © Cambridge University Press 2012
doi:10.1017/S0963548312000284

On (Not) Computing the Möbius Function Using Bounded Depth Circuits

BEN GREEN

Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WA, UK
(e-mail: b.j.green@dpmms.cam.ac.uk)

Received 25 March 2011; revised 1 June 2012; first published online 24 August 2012

Any function $F : \{0,\dots,N-1\} \to \{-1,1\}$ such that $F(x)$ can be computed from the binary digits of x using a bounded depth circuit is orthogonal to the Möbius function μ in the sense that

$$\frac{1}{N}\sum_{0\leqslant x\leqslant N-1}\mu(x)F(x) \to 0 \quad \text{as} \quad N\to\infty.$$

The proof combines a result of Linial, Mansour and Nisan with techniques of Kátai and Harman, used in their work on finding primes with specified digits.

AMS 2010 *Mathematics subject classification*: Primary 11N99

1. Introduction

This note arose from a question posed by Gil Kalai on Math Overflow [8], and discussed prior to that in blogs by Kalai [7] and Lipton [11]. This question was motivated by a general programme advanced by Peter Sarnak (see, for example, [15]), the aim of which is to rigorously establish instances of the Möbius randomness principle [6, p. 338].

Recall that the Möbius function $\mu : \mathbb{N} \to \{-1,0,1\}$ is defined as follows: $\mu(n) = 0$ if n has a non-trivial square factor, $\mu(1) = 1$, and $\mu(p_1 \dots p_k) = (-1)^k$ if $p_1,\dots,p_k$ are distinct primes. For the purposes of this paper set $\mu(0) = 0$. The Möbius randomness principle asserts that μ is asymptotically orthogonal to any 'low-complexity' function $F : \mathbb{N} \to [-1,1]$ in the sense that

$$\frac{1}{N}\sum_{x\leqslant N}\mu(x)F(x) = o(1).$$

Of course, the notion of 'low complexity' is not precisely defined. Sarnak has specifically asked about the case in which F arises from a zero-entropy dynamical system; we note that already the most trivial case $F \equiv 1$ is equivalent to the prime number theorem.

Suppose for simplicity that $N = 2^n$. Our aim here is to establish the Möbius randomness principle for a class of 'low-complexity' functions defined in a rather different way, using

https://doi.org/10.1017/S0963548312000284 Published online by Cambridge University Press

bounded depth circuits on the n binary digits of x. By a boolean circuit in this context we mean a directed acyclic graph in which every node is either an input node of in-degree 0 labelled by one of the binary digits of x, an AND gate, an OR or a NOT gate. The AND and OR gates are allowed to have arbitrary fan-in (number of inputs). One of these gates is designated as the output gate. Such a circuit naturally computes a function $F : \{0, \dots, N-1\} \to \{-1, 1\}$.

The *size* of a circuit is the total number of gates it contains and its *depth* is the maximal length of a path from an input gate to the output gate. The class $\mathrm{AC}^0(d)$ consists of all functions that can be computed using a circuit of depth at most d and size at most n^d.

Theorem 1.1. *Suppose $N = 2^n$. Let $F : \{0, \dots, N-1\} \to \{-1, 1\}$ be an $\mathrm{AC}^0(d)$ function. Then*

$$\mathbb{E}_{0 \leqslant x \leqslant N-1} \mu(x) F(x) = O(e^{d \log n - cn^{1/6d}}),$$

where $c > 0$ is an absolute constant.

Remark. Here, and throughout the paper, we write $\mathbb{E}_{x \in X} \psi(x)$ for the average of a function ψ over some finite set X. Note that the bound is $o(1)$ for $d \leqslant c' \log n / \log \log n$, and hence in particular for any fixed d.

Using a result of Linial, Mansour and Nisan [10], to be recalled in detail in the next section, the problem can be reduced to that of estimating certain of what Kalai calls the *Fourier–Walsh coefficients* of μ.

Definition. Suppose that $N = 2^n$, and for $x \in \{0, \dots, N-1\}$ write $x = x_1 + 2x_2 + \cdots + 2^{n-1}x_n$ in binary. Let $f : \{0, \dots, N-1\} \to \mathbb{C}$ be a function. Then we define the Fourier–Walsh coefficients $\hat{f}(S)$, $S \subseteq \{1, \dots, n\}$, by

$$\hat{f}(S) := \mathbb{E}_{0 \leqslant x \leqslant N-1} f(x)(-1)^{\sum_{i \in S} x_i}.$$

We remark that these are nothing more than the Fourier coefficients of f, considered as a function on the binary cube $\mathbb{F}_2^n$ instead of as a function on $\{0, \dots, N-1\}$.

The new content of this note is the following bound on Fourier–Walsh coefficients, which (given the result of Linial, Mansour and Nisan) rather easily implies Theorem 1.1.

Proposition 1.2. *Suppose that $S \subseteq \{1, \dots, n\}$ has size $|S| = k$. Then $\hat{\mu}(S) = O(ke^{-cn^{1/2}/k})$, where $c > 0$ is some absolute constant.*

This bound is non-trivial for $k = O(n^{1/2}/\log n)$, and gives a bound of shape $e^{-\log^{\Omega(1)} N}$ as soon as $k < n^{1/2-\eta}$.

It seems to be an interesting question in its own right to ask for a proof that $\hat{\mu}(S) = o(1)$ for all sets S. It seems that the methods of this paper cannot hope to handle sets S with $|S|$ bigger than about $n^{1/2}$ unconditionally, although assuming the generalized Riemann hypothesis (GRH) we obtain non-trivial bounds for $|S| = O(n/\log n)$. Interestingly, the

https://doi.org/10.1017/S0963548312000284 Published online by Cambridge University Press

most extreme case $S = \{1, \dots, n\}$ follows from the techniques of Mauduit and Rivat [12]. It is possible that by combining those ideas with the techniques in this paper one could indeed obtain a bound for all S, at least on GRH, but this is by no means a trivial matter. We hope to return to it in a future paper.[1]

In the author's opinion it is very slightly more natural to consider, in place of the Möbius function μ, the Liouville function λ. This function is the unique completely multiplicative function such that $\lambda(p) = -1$ for all primes p, or equivalently $\lambda(x)$ is ± 1 according to the parity of the number of prime factors of x, counted with multiplicity. All of the results in this paper hold equally well for the Liouville function, with very similar proofs.

Finally, we remark that there is a considerable literature concerning the difficulty of computing number-theoretic functions. Of particular relevance to this paper is the work [1], which shows that detecting primality does not lie in AC^0, and [3], which applies the result of Linial, Mansour and Nisan to show that squarefreeness cannot be detected using bounded depth circuits.

2. A result of Linial, Mansour and Nisan

The following result from [10] provides a link between functions in AC^0, that is to say computed by bounded depth circuits of polynomial size, and Fourier–Walsh coefficients.

Theorem 2.1 (Linial, Mansour and Nisan). *Suppose that $F : \{0, \dots, N-1\} \to \{-1, 1\}$ is computed using a circuit of depth d and size M. Then*

$$\sum_{|S| > t} |\hat{F}(S)|^2 \leqslant 2M2^{-t^{1/d}/20}.$$

Using this, and assuming Proposition 1.2, it is not a difficult matter to establish Theorem 1.1. We do this now. Let $F : \{0, \dots, N-1\} \to \{-1, 1\}$ be an $\mathrm{AC}^0(d)$ function; thus F is computed by a binary circuit of depth at most d and size at most n^d. Let $\gamma > 0$ be a small real number. By Parseval's identity on the cube $\mathbb{F}_2^n$, we have

$$\mathbb{E}_{0 \leqslant x \leqslant N-1} \mu(x) F(x) = \sum_S \hat{\mu}(S) \hat{F}(S).$$

Using the trivial bound $|\hat{F}(S)| \leqslant 1$ for $|S| \leqslant n^{1/6}$, this is bounded in modulus by

$$n^{n^{1/6}} \sup_{|S| \leqslant n^{1/6}} |\hat{\mu}(S)| + \sum_{|S| > n^{1/6}} |\hat{\mu}(S)||\hat{F}(S)|.$$

Applying Proposition 1.2 to the first term and the Cauchy–Schwarz inequality and Parseval's identity to the second, it follows that this is at most

$$O(e^{-cn^{1/3}}) + \left(\sum_{|S| > n^{1/6}} |\hat{F}(S)|^2 \right)^{1/2}.$$

[1] Added in proof: Jean Bourgain has since obtained such a bound.

https://doi.org/10.1017/S0963548312000284 Published online by Cambridge University Press

Finally, by the theorem of Linial, Mansour and Nisan, this is no more than

$$O(e^{-cn^{1/3}}) + (2n^d e^{-cn^{1/6d}})^{1/2} = O(e^{d\log n - cn^{1/6d}}),$$

as required.

3. An argument of Kátai

In this section we give a general version of an argument from [9] (see also [5]). In the language of this paper, it gives a link between the Fourier–Walsh coefficients $\hat{f}(S)$ and the 'traditional' Fourier coefficients

$$\hat{f}(\theta) := \mathbb{E}_{0\leqslant x\leqslant N-1} f(x)e(\theta x),$$

where $\theta \in [0,1]$ and here, as always, $e(u) := e^{2\pi iu}$. By a *dyadic* rational we mean a rational number with denominator a power of two.

Proposition 3.1. *Let $f : \{0,\dots,N-1\} \to [-1,1]$ be a function for which there exists some $S \subseteq \{1,\dots,n\}$, $|S| = k$, for which the Fourier–Walsh coefficient $\hat{f}(S)$ has magnitude at least δ, $0 < \delta < 1/2$. Then there is a dyadic rational θ such that the traditional Fourier coefficient $\hat{f}(\theta)$ has magnitude at least $(\delta/10k)^{4k}$. In fact, θ can be taken to be a* sparse *dyadic rational in the sense that it may be written as $\theta = \frac{r_1}{2^{i_1}} + \cdots + \frac{r_k}{2^{i_k}}$ with $r_i \in \mathbb{Z}$ and $|r_i| \leqslant (10k/\delta)^3$ for all i.*

Proof. We have

$$\hat{f}(S) = \mathbb{E}_{0\leqslant x\leqslant N-1} f(x) \prod_{i\in S} \psi\left(\frac{x}{2^i}\right), \tag{3.1}$$

where $\psi : \mathbb{R}/\mathbb{Z} \to [-1,1]$ is the function defined by $\psi(t) = 1$ if $0 \leqslant t < \frac{1}{2}$ and $\psi(t) = -1$ if $\frac{1}{2} \leqslant t < 1$.

We shall replace ψ by a smoothed version $\tilde{\psi} : \mathbb{R}/\mathbb{Z} \to [-1,1]$ with the property that

$$\mathbb{E}_{0\leqslant x\leqslant N-1} \left|\psi\left(\frac{x}{2^i}\right) - \tilde{\psi}\left(\frac{x}{2^i}\right)\right| \leqslant \varepsilon \tag{3.2}$$

for $i = 0,1,2,\dots,n$, and which has a Fourier expansion of the shape

$$\tilde{\psi}(t) = \sum_{|r|\leqslant 100\varepsilon^{-3}} a_r e(rt), \tag{3.3}$$

with $|a_r| \leqslant 1$ for all r.

Such a function may be constructed by a fairly standard type of smoothing procedure, which we now describe. Consider first of all the function $\psi_0 := \phi * \chi * \chi$, where $\phi : \mathbb{R}/\mathbb{Z} \to [-1,1]$ is defined by $\phi(t) = \psi\left(t + \frac{\varepsilon}{24}\right)$, that is to say $\phi(t) = 1$ if $-\frac{\varepsilon}{24} \leqslant t < \frac{1}{2} - \frac{\varepsilon}{24}$ and $\phi(t) = -1$ if $\frac{1}{2} - \frac{\varepsilon}{24} \leqslant t < 1 - \frac{\varepsilon}{24}$, and $\chi := \frac{24}{\varepsilon} 1_{[-\varepsilon/48,\varepsilon/48]}$. Note that ψ_0 takes values in $[-1,1]$ and that $\psi_0(t) = \psi(t)$ outside of the pairs of intervals $I_1 = \left[\frac{1}{2} - \frac{\varepsilon}{12}, \frac{1}{2}\right]$ and $I_2 = \left[1 - \frac{\varepsilon}{12}, 1\right]$.

The interval I_1, being situated adjacent to but not including the point $\frac{1}{2}$, contains at most its fair share (that is, $\varepsilon/12$) of rationals with denominator 2^i for any i. The same is

https://doi.org/10.1017/S0963548312000284 Published online by Cambridge University Press

true for I_2. It follows easily that

$$\mathbb{E}_{0\leqslant x\leqslant N-1}\left|\psi\left(\frac{x}{2^i}\right)-\psi_0\left(\frac{x}{2^i}\right)\right|<\varepsilon/3. \tag{3.4}$$

Now the Fourier coefficients of ψ_0 are given by $\hat{\psi}_0(r)=\hat{\phi}(r)\hat{\chi}(r)^2$, and in particular (computing $\hat{\chi}$ explicitly) we have the bound $|\hat{\psi}_0(r)|\leqslant|\hat{\chi}(r)|^2\leqslant\min(1,24/\varepsilon\pi|r|)^2$. It follows that

$$\sum_{|r|>100/\varepsilon^3}|\hat{\psi}_0(r)|<\frac{\varepsilon}{3}.$$

Define $\psi_1(t):=\sum_{|r|\leqslant 100/\varepsilon^3}\hat{\psi}_0(r)e(rt)$. This clearly has the shape (3.3). Furthermore, from the preceding analysis we have the bound

$$\|\psi_1-\psi_0\|_\infty\leqslant\sum_{|r|>100/\varepsilon^3}|\hat{\psi}_0(r)|<\varepsilon/3. \tag{3.5}$$

This also implies that $\|\psi_1\|_\infty\leqslant\|\psi_0\|_\infty+\frac{\varepsilon}{3}\leqslant 1+\frac{\varepsilon}{3}$. Finally set $\tilde{\psi}:=\psi_1/(1+\frac{\varepsilon}{3})$, so that $\tilde{\psi}$ takes values in $[-1,1]$. Then

$$\|\tilde{\psi}-\psi_1\|_\infty=\|\psi_1\|_\infty\left(1-\frac{1}{1+\varepsilon/3}\right)\leqslant\varepsilon/3. \tag{3.6}$$

This function $\tilde{\psi}$ is still of the form (3.3). Combining (3.4), (3.5) and (3.6) using the triangle inequality gives the desired property (3.2).

Choose $\varepsilon:=\delta/2k$ in this construction. Replacing each copy of ψ by $\tilde{\psi}$ in turn in (3.1) and applying the property (3.2) repeatedly, we obtain

$$\left|\mathbb{E}_{0\leqslant x\leqslant N-1}f(x)\prod_{i\in S}\tilde{\psi}\left(\frac{x}{2^i}\right)\right|\geqslant\delta-k\varepsilon\geqslant\delta/2.$$

Now develop each $\tilde{\psi}$ in its Fourier series to get

$$\left|\sum_{|r_1|,\dots,|r_k|\leqslant 100/\varepsilon^3}a_{r_1}a_{r_2}\dots a_{r_k}\mathbb{E}_{0\leqslant x\leqslant N-1}f(x)e\left(\left(\frac{r_1}{2^{i_1}}+\dots+\frac{r_k}{2^{i_k}}\right)x\right)\right|\geqslant\delta/2,$$

where $S=\{i_1,\dots,i_k\}$.

It follows immediately that there is some $\theta=\frac{r_1}{2^{i_1}}+\dots+\frac{r_k}{2^{i_k}}$ such that

$$|\hat{f}(\theta)|\geqslant\frac{\delta}{2}\left(\frac{\varepsilon^3}{300}\right)^k>\left(\frac{\delta}{10k}\right)^{4k},$$

which is the claimed bound.

The fact that θ is a *sparse* dyadic rational, in the sense claimed, is clear from the proof. □

On the assumption of the GRH, Proposition 3.1 already implies Theorem 1.1. Indeed on that hypothesis it is known, by work of Baker and Harman [2], that $|\hat{\mu}(\theta)|\ll_\varepsilon N^{-1/4+\varepsilon}$ for all $\varepsilon>0$. We note that this together with Proposition 3.1 gives a non-trivial estimate $\hat{\mu}(S)=o(1)$ for all $S\subseteq\{1,\dots,n\}$ with $|S|\leqslant cn/\log n$.

https://doi.org/10.1017/S0963548312000284 Published online by Cambridge University Press

Without some unproved hypothesis, however, the best available bounds for general θ are $|\hat{\mu}(\theta)| \ll_A \log^{-A} N$ for all $A > 0$, the implied constant being ineffective as a function of A. This 1937 result of Davenport [4], whilst it leads to a non-trivial bound on $\hat{\mu}(S)$ for $|S| \leqslant A \log n / \log\log n$ for all A, does not suffice for our main application.

To proceed further, some special use must be made of the sparse dyadic structure of θ. In this regard we will prove, in the next section, the following result.

Proposition 3.2. *There is some $c_1 > 0$ with the following property. Let $N = 2^n$, suppose that $k < n^{1/2}$, and suppose that $\theta = \frac{r_1}{2^{i_1}} + \cdots + \frac{r_k}{2^{i_k}}$ with $|r_i| \leqslant e^{c_1\sqrt{\log N}}$ for all i. Then $|\hat{\mu}(\theta)| = O(e^{-c_1\sqrt{\log N}})$.*

Proof of Proposition 1.2. Suppose Proposition 1.2 fails. Then there is some $S \subseteq \{1, \ldots, n\}$ such that $|\hat{\mu}(S)| \geqslant k e^{-cn^{1/2}/k}$. By Proposition 3.1 there is a sparse dyadic rational $\theta = \frac{r_1}{2^{i_1}} + \cdots + \frac{r_k}{2^{i_k}}$, $|r_i| \ll e^{3cn^{1/2}/k}$, such that $|\hat{\mu}(\theta)| \geqslant e^{-4cn^{1/2}}$. If c is chosen small enough, this is contrary to Proposition 3.2. □

4. Exponential sums over Möbius at sparse dyadic rationals

In this section we complete our remaining task, which is to establish Proposition 3.2. We begin by quoting the following result, which would be well known to experts in analytic number theory, but for which it is hard to find a really concise reference.

Theorem 4.1. *For some absolute constant $c_2 > 0$ the following is true. Suppose that χ is a Dirichlet character to modulus $q = 2^t$, $q \leqslant e^{c_2\sqrt{\log N}}$. Then*

$$\mathbb{E}_{0 \leqslant x \leqslant N-1} \mu(x)\chi(x) = O(e^{-c_2\sqrt{\log N}}).$$

Proof. By standard techniques of analytic number theory (Perron's formula and the classical zero-free region for Dirichlet L-functions) one may establish the bound

$$\mathbb{E}_{0 \leqslant x \leqslant N-1} \mu(x)\chi(x) = O(e^{-c_2\sqrt{\log N}})$$

for *all* Dirichlet characters χ to modulus $q \leqslant e^{c_2\sqrt{\log N}}$, provided only that $L(s, \chi)$ has no *exceptional zero*. This last possibility only occurs (if at all) when χ is real, and the zero in question lies on the segment $(1/2, 1]$.

For a proof of this bound the reader may consult the very comprehensive book [13], in which this precise statement is Exercise 11.3.7; the key ingredient, other than Perron's formula, is the upper bound for $1/L(s, \chi)$ given by Theorem 11.4 of that book, and specifically equation (11.7).

We now specialize to the case $q = 2^t$. Without loss of generality we may suppose that q is the conductor of χ. To rule out the possibility of exceptional zeros note that there *are* only three non-principal primitive real Dirichlet characters with conductor a power of two: the character χ_4 on $(\mathbb{Z}/4\mathbb{Z})^*$ with $\chi_4(-1) = -1$, and the characters χ_8 and $\chi_4\chi_8$, where χ_8 is the primitive character on $(\mathbb{Z}/8\mathbb{Z})^*$ defined by $\chi_8(3) = \chi_8(5) = -1$ and

https://doi.org/10.1017/S0963548312000284 Published online by Cambridge University Press

$\chi_8(1) = \chi_8(7) = 1$. This follows from the well-known fact that

$$(\mathbb{Z}/2^e\mathbb{Z})^* \cong \{\pm 1\} \times \{1, 5, 5^2, \dots, 5^{2^{e-2}-1}\}$$

for $e \geqslant 3$, which means that any Dirichlet character of conductor dividing 2^e is determined by its values at -1 and 5.

For each of these three characters it is known that there are no real zeros of the corresponding $L(s, \chi)$ on $\left(\frac{1}{2}, 1\right]$; see for example [14]. (In fact it suffices to know that $L(1, \chi) \neq 0$, which is of course true for *all* Dirichlet characters χ. This implies that $L(s, \chi) \neq 0$ for $s \in [1 - c', 1]$ for some c' by continuity, which already means that there are no exceptional zeros.) □

Corollary 4.2. *Let $c_3 := c_2/2$. Then we have the estimate*

$$\mathbb{E}_{0 \leqslant x \leqslant N-1} \mu(x) e(ax/2^t) = O(e^{-c_3\sqrt{\log N}}),$$

uniformly for $2^t \leqslant e^{c_3\sqrt{\log N}}$ and $a \in \mathbb{Z}$.

Proof. We use Fourier analysis on $(\mathbb{Z}/2^t\mathbb{Z})^*$. If $x \in (\mathbb{Z}/2^t\mathbb{Z})^*$ then $\sum_\chi \chi(x)$ equals 2^{t-1} if $x = 1$ and vanishes otherwise, where the sum is over all characters $\chi : (\mathbb{Z}/2^t\mathbb{Z})^* \to \mathbb{C}^*$. It follows that

$$e\left(\frac{ax}{2^t}\right) = \frac{1}{2^{t-1}} \sum_{r \in (\mathbb{Z}/2^t\mathbb{Z})^*} \sum_\chi \overline{\chi(r)} e\left(\frac{ar}{2^t}\right) \chi(x)$$

for all odd x.

It follows from the preceding equation, the triangle inequality and Theorem 4.1 that

$$\sum_{\substack{0 \leqslant x \leqslant N-1 \\ 2 \nmid x}} \mu(x) e\left(\frac{ax}{2^t}\right) \leqslant 2^{t-1} \sup_\chi \left| \sum_{0 \leqslant x \leqslant N-1} \mu(x)\chi(x) \right| = O(Ne^{-c_3\sqrt{\log N}}).$$

We could have estimated the Gauss sum here less trivially, but there is no need. By the same argument (using the fact that $\mu(2x) = -\mu(x)$ when x is odd), we have

$$\sum_{\substack{0 \leqslant x \leqslant N-1 \\ 2|x \\ 4 \nmid x}} \mu(x) e\left(\frac{ax}{2^t}\right) = - \sum_{0 \leqslant x < \frac{1}{2}N : 2 \nmid x} \mu(x) e\left(\frac{ax}{2^{t-1}}\right) = O(Ne^{-c_3\sqrt{\log N}}).$$

This concludes the proof of the corollary. □

Finally we give a further standard deduction, allowing us to bound $\hat{\mu}(\theta)$ when θ is *near* a dyadic rational.

Corollary 4.3. *Let $c_4 := c_3/3$. Suppose that $|\theta - a/q| \leqslant e^{c_4\sqrt{\log N}}/N$, where $q \leqslant e^{c_4\sqrt{\log N}}$ is a power of two. Then $\hat{\mu}(\theta) = O(e^{-c_4\sqrt{\log N}})$.*

https://doi.org/10.1017/S0963548312000284 Published online by Cambridge University Press

Proof. Let L, $1 < L < N$, be a quantity to be specified. If $P \subseteq \{0, \dots, N-1\}$ is any interval of integers of length L and if x_0 lies in P, then we have

$$\begin{aligned}\left|\sum_{x\in P}\mu(x)e(\theta x)\right| &= \left|\sum_{x\in P}\mu(x)e(ax/q)e((x-x_0)(\theta-a/q))\right| \\ &= \left|\sum_{x\in P}\mu(x)e(ax/q)\right| + O\left(\frac{L^2}{N}e^{c_4\sqrt{\log N}}\right) \\ &= O(Ne^{-c_3\sqrt{\log N}}) + O\left(\frac{L^2}{N}e^{c_4\sqrt{\log N}}\right),\end{aligned}$$

the latter estimate following immediately from Corollary 4.2. Dividing $\{0, \dots, N-1\}$ into $O(N/L)$ such progressions, we obtain

$$\hat{\mu}(\theta) = O\left(\frac{N}{L}e^{-c_3\sqrt{\log N}}\right) + O\left(\frac{L}{N}e^{c_4\sqrt{\log N}}\right).$$

Choosing $L := Ne^{-2c_4\sqrt{\log N}}$ gives the result. □

Next, we recall a standard estimate on exponential sums over the Möbius function. This may be established using the method of Type I/II sums or bilinear forms, perhaps most easily by utilizing Vaughan's identity. The estimate provides an excellent bound for $\hat{\mu}(\theta)$ if θ is not well approximated by a rational with small denominator.

Proposition 4.4. *Suppose that $|\hat{\mu}(\theta)| \geqslant \delta$. Then there is some $q \ll \left(\frac{\log N}{\delta}\right)^{16}$ such that $|\theta - a/q| \ll \left(\frac{\log N}{\delta}\right)^{16} N^{-1}$.*

Sketch of proof. Let $Q = cN\left(\frac{\log N}{\delta}\right)^{-16}$ for some small $c > 0$ to be specified shortly. By Dirichlet's theorem on diophantine approximation there is some q, $1 \leqslant q \leqslant Q$ such that $|\theta - a/q| \leqslant 1/qQ$. In particular $|\theta - a/q| \leqslant 1/q^2$, and so we may apply [6, Theorem 13.9] to conclude that $\delta(\log N)^{-4} \ll \max(q^{1/4}N^{-1/4}, q^{-1/4}, N^{-1/10})$. If $\delta < N^{-1/12}$ (say) then the result is trivial, so we have either $\delta(\log N)^{-4} \ll q^{1/4}N^{-1/4} \leqslant Q^{1/4}N^{-1/4}$ or $\delta(\log N)^{-4} \ll q^{-1/4}$. If c is small enough then the first of these is impossible by the choice of Q, and so the second must hold. This implies that $q \ll \left(\frac{\log N}{\delta}\right)^{16}$, thereby concluding the proof. □

Corollary 4.3 and Proposition 4.4 between them provide good estimates on $\hat{\mu}(\theta)$ in two cases: when θ is close to a rational with denominator a power of two, and when θ is not very close to any rational with small denominator.

Of course, there are values of θ (such as $\theta = \frac{1}{3}$) not covered by either proposition. However, we have the following key observation of Harman and Kátai [5], allowing one to conclude that none of these exceptional values of θ are sparse dyadic rationals. Here is a precise formulation of their idea.

Lemma 4.5. *Suppose that $\theta = \frac{r_1}{2^{i_1}} + \cdots + \frac{r_k}{2^{i_k}}$, where $i_1 < \cdots < i_k \leqslant n$ and $|r_i| \leqslant Q$ for all i. Suppose furthermore that there is some $q \leqslant Q$ and an a coprime to q such that $|\theta - a/q| \leqslant Q/N$, and that we have $2^{n/2k} > 4Q^2$. Then q is a power of two.*

https://doi.org/10.1017/S0963548312000284 Published online by Cambridge University Press

Proof. Set $i_0 := 0$ and $i_{k+1} := n$. By the pigeonhole principle there is some index $j \in \{0, 1, \dots, k\}$ such that $|i_j - i_{j+1}| \geqslant n/2k$. Now we note that θ is very close to a rational with denominator $q' = 2^{i_j}$. Specifically, writing $a' := r_1 2^{i_j - i_1} + \cdots + r_{j-1} 2^{i_j - i_{j-1}} + r_j$, we have

$$\left|\theta - \frac{a'}{q'}\right| \leqslant Q(2^{-i_{j+1}} + 2^{-i_{j+2}} + \dots) \leqslant 2^{-n/2k}\frac{2Q}{q'}.$$

Note also that $q' \leqslant 2^{-n/2k}N$, and so (by the hypothesis) $Q/N < 1/4Qq'$. It follows that

$$\left|\frac{a}{q} - \frac{a'}{q'}\right| \leqslant \left|\theta - \frac{a'}{q'}\right| + \left|\theta - \frac{a}{q}\right| \leqslant 2^{-n/2k}\frac{2Q}{q'} + \frac{Q}{N} < \frac{1}{2Qq'} + \frac{Q}{N} < \frac{1}{Qq'} \leqslant \frac{1}{qq'},$$

which of course implies that $q = q'$ and $a = a'$. □

We are now ready to prove Proposition 3.2 which, as we remarked earlier, completes the proof of our main theorem. Let us recall the statement.

Proposition 3.2. *There is some $c_1 > 0$ with the following property. Let $N = 2^n$, suppose that $k < n^{1/2}$, and suppose that $\theta = \frac{r_1}{2^{i_1}} + \cdots + \frac{r_k}{2^{i_k}}$ with $|r_i| \leqslant e^{c_1\sqrt{\log N}}$ for all i. Then $\hat{\mu}(\theta) = O(e^{-c_1\sqrt{\log N}})$.*

Proof. Set $\delta := e^{-c_1\sqrt{\log N}}$ and take $c_1 = c_4/32$. Suppose that there is some θ of the above sparse dyadic form with $|\hat{\mu}(\theta)| \geqslant \delta$. By Proposition 4.4 (and the fact that δ is much smaller than $1/\log N$), there is some $q \ll \delta^{-32} = e^{c_4\sqrt{\log N}}$ such that $|\theta - a/q| \ll e^{c_4\sqrt{\log N}}N^{-1}$. Consider Lemma 4.5 with $Q = e^{c_4\sqrt{\log N}}$. Clearly $|r_i| \leqslant Q$ for all i, and the hypothesis $2^{n/2k} > 4Q^2$ is satisfied. It follows that q is a power of two.

But then Proposition 4.3 may be applied to conclude that $\hat{\mu}(\theta) = O(e^{-c_3\sqrt{\log N}})$, which is what we wanted to prove. □

Acknowledgements

It is a pleasure to thank Gil Kalai for bringing this question to my attention and for encouragement, and for drawing attention to the work of Linial, Mansour and Nisan. It is also my pleasure to thank Andrew Granville for several helpful conversations concerning the distribution of primes in progressions. Finally, I thank the anonymous referee and the editors of *Combinatorics, Probability and Computing* for a careful reading of the paper.

References

[1] Allender, E., Saks, M. and Shparlinski, I. (2001) A lower bound for primality. *J. Comput. System Sci.* (*Special Issue on the Fourteenth Annual IEEE Conference on Computational Complexity*) **62** 356–366.

[2] Baker, R. C. and Harman, G. (1991) Exponential sums formed with the Möbius function. *J. London Math. Soc.* (2) **43** 193–198.

[3] Bernasconi, A., Damm, C. and Shparlinski, I. (1999) On the average sensitivity of testing square-free numbers. In *Computing and Combinatorics: Tokyo 1999*, Vol. 1627 of *Lecture Notes in Computer Science*, Springer, pp. 291–299.

https://doi.org/10.1017/S0963548312000284 Published online by Cambridge University Press

[4] Davenport, H. (1937) On some infinite series involving arithmetical functions II. *Quart. J. Math. Oxford* **8** 313–320.
[5] Harman, G. and Kátai, I. (2008) Primes with preassigned digits II. *Acta Arith.* **133** 171–184.
[6] Iwaniec, H. and Kowalski, E. (2004) *Analytic Number Theory*, Vol. 53 of *American Mathematical Society Colloquium Publications*, AMS.
[7] Kalai, G. (2011) The AC0 prime number conjecture. Blog post, available at: http://gilkalai.wordpress.com/2011/02/21/the-ac0-prime-number-conjecture/
[8] Kalai, G. (2011) Walsh Fourier transform of the Möbius function. *Math Overflow* question, available at: http://mathoverflow.net/questions/57543/walsh-fourier-transform-of-mobius-functions
[9] Kátai, I. (1986) Distribution of digits of primes in q-ary canonical form. *Acta Math. Hungar.* **47** 341–359.
[10] Linial, N., Mansour, Y. and Nisan, N. (1993) Constant depth circuits, Fourier transform, and learnability. *J. Assoc. Comput. Mach.* **40** 607–620.
[11] Lipton, R. J. (2011) The depth of the Möbius function. Blog post, available at: http://rjlipton.wordpress.com/2011/02/23/the-depth-of-the-mobius-function/
[12] Mauduit, C. and Rivat, J. (2010) Sur un probléme de Gelfond: La somme des chiffres des nombres premiers. *Ann. of Math.* (2) **171** 1591–1646.
[13] Montgomery, H. and Vaughan, R. C. (2007) *Multiplicative Number Theory I: Classical Theory*, Vol. 97 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press.
[14] Ramaré, O. and Rumely, R. (1996) Primes in arithmetic progressions. *Math. Comp.* **65** 397–425.
[15] Sarnak, P. (2010) *Möbius Randomness and Dynamics*. Lecture notes, available at: http://www.math.princeton.edu/sarnak/Mobius lectures Summer 2010.pdf

https://doi.org/10.1017/S0963548312000284 Published online by Cambridge University Press