A PAUCITY PROBLEM ASSOCIATED WITH A SHIFTED INTEGER ANALOGUE OF THE DIVISOR FUNCTION

WINSTON HEAP, ANURAG SAHAY, AND TREVOR D. WOOLEY

Abstract. Suppose that θ is irrational. Then almost all elements $\nu \in \mathbb{Z}[\theta]$ that may be written as a k-fold product of the shifted integers $n+\theta$ ($n \in \mathbb{N}$) are thus represented essentially uniquely.

1. Introduction

Given a complex number θ, the shifted integer analogue of the natural numbers $\mathbb{N}+\theta = \{n+\theta : n \in \mathbb{N}\}$ possesses, at a superficial level, many additive properties in common with its unshifted cousin $\mathbb{N}$. For multiplicative problems, the close connections plausible in the additive setting rapidly evaporate. In this note we examine a shifted analogue of the restricted divisor function. Thus, when $\nu \in \mathbb{Z}[\theta]$, we consider the function

$$\tau_k(\nu; X, \theta) = \sum_{\substack{1\leqslant d_1\leqslant X \\ (d_1+\theta)\cdots(d_k+\theta)=\nu}} \cdots \sum_{1\leqslant d_k\leqslant X} 1.$$

The mean value

$$\sum_{\nu\in\mathbb{Z}[\theta]} \tau_k(\nu; X, \theta)^2$$

counts the number of integral solutions of the equation

$$(x_1+\theta)\cdots(x_k+\theta) = (y_1+\theta)\cdots(y_k+\theta), \tag{1.1}$$

with $1 \leqslant x_i, y_i \leqslant X$ ($1 \leqslant i \leqslant k$). We show that when $\theta \notin \mathbb{Q}$, then almost all solutions of (1.1) are the diagonal ones in which $(x_1, \ldots, x_k)$ is a permutation of $(y_1, \ldots, y_k)$. Thus, almost all elements $\nu \in \mathbb{Z}[\theta]$ that may be written as a k-fold product of shifted integers $n+\theta$ ($n \in \mathbb{N}$) are represented essentially uniquely in this manner.

In order to describe our conclusions in more detail, it is convenient to introduce some notation. Denote by $T_k(X)$ the number of k-tuples $\mathbf{x}$ and $\mathbf{y}$ in which $1 \leqslant x_i, y_i \leqslant X$ ($1 \leqslant i \leqslant k$), and $(x_1, \ldots, x_k)$ is a permutation of $(y_1, \ldots, y_k)$. Thus $T_k(X) = k!X^k + O(X^{k-1})$. We begin with the simplest situation in which $\theta \in \mathbb{C}$ is either transcendental, or else algebraic of large degree over $\mathbb{Q}$.

2010 *Mathematics Subject Classification.* 11N37, 11D45.

Key words and phrases. Paucity problems, divisor functions, shifted integers.

Theorem 1.1. *Let $k \in \mathbb{N}$ and $\varepsilon > 0$. Suppose that $\theta \in \mathbb{C}$ is either transcendental, or else algebraic of degree d over $\mathbb{Q}$, where $d \geqslant k$. Then one has*

$$\sum_{\nu \in \mathbb{Z}[\theta]} \tau_k(\nu; X, \theta)^2 = T_k(X).$$

The situation in which θ is algebraic of small degree is more complicated.

Theorem 1.2. *Let $k \in \mathbb{N}$ and $\varepsilon > 0$. Suppose that $\theta \in \mathbb{C}$ is algebraic of degree d over $\mathbb{Q}$, where $2 \leqslant d < k$. Then one has*

$$\sum_{\nu \in \mathbb{Z}[\theta]} \tau_k(\nu; X, \theta)^2 = T_k(X) + O(X^{k-d+1+\varepsilon}).$$

Here, the implicit constant in Landau's notation may depend on k, ε and θ.

It follows that when $\theta \notin \mathbb{Q}$, then there is a paucity of non-diagonal solutions in the equation (1.1). Moreover, one has the asymptotic formula

$$\sum_{\nu \in \mathbb{Z}[\theta]} \tau_k(\nu; X, \theta)^2 = k! X^k + O(X^{k-1+\varepsilon}).$$

These conclusions are in marked contrast with the corresponding situation in which $\theta \in \mathbb{Q}$. When θ is rational, experts will recognise that a straightforward exercise employing the circle method yields the lower bound

$$\sum_{\nu \in \mathbb{Q}} \tau_k(\nu; X, \theta)^2 \gg_{\theta,k} X^k (\log X)^{(k-1)^2}.$$

Indeed, additional work would exhibit an asymptotic formula in place of this lower bound. In this regard, we note that the contour integral methods of [1, 2] would also be accessible. The inquisitive reader interested in paucity problems for diagonal Diophantine systems will find a representative slice of the relevant literature in [4, 5, 6, 7].

One motivation for considering this problem is that such multiplicative equations arise naturally when studying the higher moments of zeta and L-functions. In particular, equation (1.1) is intimately related to the moments and value distribution of the Hurwitz zeta function $\zeta(s, \theta)$ with shift parameter $0 < \theta \leqslant 1$. For irrational shifts θ, this forms the focus of an ongoing project of the first and second author. For rational shifts θ, see [3].

Perhaps it is worth stressing that the equation (1.1) corresponds to a system of polynomial equations with integral variables. In order to illustrate this point, consider the situation in which $k = 3$ and $\theta = \sqrt{2}$. We make use of the linear independence of 1 and $\sqrt{2}$ over $\mathbb{Q}$. On noting that

$$(x_1+\sqrt{2})(x_2+\sqrt{2})(x_3+\sqrt{2}) = x_1x_2x_3+2(x_1+x_2+x_3)+\sqrt{2}(x_1x_2+x_2x_3+x_3x_1+2),$$

we find that the equation (1.1) holds if and only if

$$\begin{aligned} x_1x_2x_3 + 2(x_1+x_2+x_3) &= y_1y_2y_3 + 2(y_1+y_2+y_3) \\ x_1x_2 + x_2x_3 + x_3x_1 &= y_1y_2 + y_2y_3 + y_3y_1. \end{aligned} \tag{1.2}$$

In this scenario, we conclude from Theorem 1.2 that the number $N(X)$ of integral solutions of the system (1.2) with $1 \leqslant x_i, y_i \leqslant X$ $(1 \leqslant i \leqslant 3)$ satisfies

$$N(X) = 6X^3 + O(X^{2+\varepsilon}).$$

The basic strategy that we employ in the proofs of Theorems 1.1 and 1.2 is based on the generation of multiplicative polynomial identities. These are inspired by an examination of the polynomial

$$\prod_{i=1}^{k}(t - x_i) - \prod_{i=1}^{k}(t - y_i).$$

There are parallels here with the third author's treatment of the Vinogradov system in joint work with Vaughan [6]. We also interpret the function $\tau_k(\nu; X, \theta)$ as the number of integral solutions of the equation

$$(x_1 + \theta)(x_2 + \theta)\cdots(x_k + \theta) = \nu, \tag{1.3}$$

with $1 \leqslant x_i \leqslant X$ $(1 \leqslant i \leqslant k)$. This can be seen as a restriction of the k-fold divisor function in the ring of integers $\mathfrak{O}_K$ of the number field $K = \mathbb{Q}(\theta)$. Immediate appeal to such ideas is limited by the observation that the divisors occurring on the left hand side of (1.3) come from a thin subset of all the algebraic integers in $\mathfrak{O}_K$. Nonetheless, a crude bound $\tau_k(\nu; X, \theta) = O(X^\varepsilon)$ stemming from such ideas plays a role in the concluding phase of our proof of Theorem 1.2.

Our basic parameter is X, a sufficiently large positive number. Whenever ε appears in a statement, either implicitly or explicitly, we assert that the statement holds for each $\varepsilon > 0$. In this paper, implicit constants in the notations of Landau and Vinogradov may depend on ε, k, and θ. We make frequent use of vector notation in the form $\mathbf{x} = (x_1, \ldots, x_k)$. Here, the dimension k is permitted to depend on the course of the argument.

Acknowledgements: The second author is grateful to his PhD advisor, Steve Gonek, for support and encouragement. The third author's work is supported by NSF grants DMS-2001549 and DMS-1854398. The second and third authors also benefitted from activities hosted by the American Institute of Mathematics, San Jose supported via the latter grant.

2. The proof of Theorem 1.1

We begin in this section by considering the situation in which $\theta \in \mathbb{C}$ is either transcendental, or else is algebraic of degree $d \geqslant k$ over $\mathbb{Q}$. In such circumstances, we rewrite the equation (1.1) by using elementary symmetric polynomials $\sigma_j(\mathbf{z}) \in \mathbb{Z}[z_1, \ldots, z_k]$. These may be defined for $j \geqslant 0$ by means of the generating function identity

$$\sum_{j=0}^{k} \sigma_j(\mathbf{z}) t^{k-j} = \prod_{i=1}^{k}(t + z_i).$$

The equation (1.1) may thus be rewritten in the form

$$\sum_{j=0}^{k} \sigma_j(\mathbf{x})\theta^{k-j} = \sum_{j=0}^{k} \sigma_j(\mathbf{y})\theta^{k-j}.$$

Since $\sigma_0(\mathbf{x}) = 1 = \sigma_0(\mathbf{y})$, we find that

$$\sum_{j=1}^{k} (\sigma_j(\mathbf{x}) - \sigma_j(\mathbf{y}))\theta^{k-j} = 0. \tag{2.1}$$

In our present situation with θ either transcendental, or else algebraic of degree $d \geqslant k$ over $\mathbb{Q}$, the complex numbers $1, \theta, \ldots, \theta^{k-1}$ are linearly independent over $\mathbb{Q}$. Then it follows from (2.1) that $\sigma_j(\mathbf{x}) = \sigma_j(\mathbf{y})$ $(1 \leqslant j \leqslant k)$. In particular, one obtains the polynomial identity

$$\prod_{j=1}^{k} (t - x_j) = \prod_{j=1}^{k} (t - y_j). \tag{2.2}$$

The polynomial relation (2.2) implies that left and right hand sides must have the same zeros with identical multiplicities. Hence $(x_1, \ldots, x_k)$ must be a permutation of $(y_1, \ldots, y_k)$. The conclusion

$$\sum_{\nu \in \mathbb{Z}[\theta]} \tau_k(\nu; X, \theta)^2 = T_k(X)$$

is then immediate on considering the Diophantine interpretation (1.1) of the mean value on the left hand side. This completes the proof of Theorem 1.1.

3. The proof of Theorem 1.2

We now assume that $\theta \in \mathbb{C}$ is an algebraic number of degree d over $\mathbb{Q}$, with $2 \leqslant d < k$. In this situation the equation (1.1) simplifies, since θ^d may be expressed as a $\mathbb{Q}$-linear combination of $1, \theta, \ldots, \theta^{d-1}$. However, the equation (2.1) no longer delivers k independent polynomial equations, but instead d such equations with $d < k$. The strategy of §2 is thus no longer applicable.

Let $\mathbf{x}, \mathbf{y}$ be an integral solution of the equation (1.1) with $1 \leqslant x_i, y_i \leqslant X$ $(1 \leqslant i \leqslant k)$, in which $(x_1, \ldots, x_k)$ is not a permutation of $(y_1, \ldots, y_k)$. Observe first that if $x_i = y_j$ for any indices i and j with $1 \leqslant i, j \leqslant k$, then we may cancel the factors $x_i + \theta$ and $y_j + \theta$, respectively, from the left and right hand sides of (1.1). It thus suffices to establish the conclusion of Theorem 1.2 with k replaced by $k - 1$. Here, of course, if $d \geqslant k - 1$, then the desired conclusion follows from Theorem 1.1. By repeatedly cancelling pairs of equal factors in this way, it is apparent that there is no loss of generality in supposing henceforth that $x_i = y_j$ for no indices i and j with $1 \leqslant i, j \leqslant k$.

Consider the polynomial

$$F(t) = \prod_{i=1}^{k} (t + x_i) - \prod_{i=1}^{k} (t + y_i). \tag{3.1}$$

This polynomial has degree at most $k-1$, and so for suitable integers $a_j = a_j(\mathbf{x},\mathbf{y})$ $(0 \leqslant j \leqslant k-1)$, we may write

$$F(t) = a_0 + a_1 t + \ldots + a_{k-1}t^{k-1}.$$

Note that for $0 \leqslant j \leqslant k-1$, one has

$$|a_j| = |\sigma_{k-j}(\mathbf{x}) - \sigma_{k-j}(\mathbf{y})| \ll X^{k-j}. \tag{3.2}$$

Next, denote by $m_\theta \in \mathbb{Z}[t]$ the minimal polynomial of θ over $\mathbb{Z}$. Then m_θ is irreducible of degree d over $\mathbb{Z}$, and if m_θ has leading coefficient $c_d \neq 0$, then $c_d^{-1} m_\theta \in \mathbb{Q}[t]$ is the usual minimal polynomial of θ over $\mathbb{Q}$. We may write

$$m_\theta(t) = c_0 + c_1 t + \ldots + c_d t^d,$$

in which $|c_j| \ll_\theta 1$ $(0 \leqslant j \leqslant d)$. We observe from (1.1) and (3.1) that

$$F(\theta) = \prod_{i=1}^{k}(x_i+\theta) - \prod_{i=1}^{k}(y_i+\theta) = 0,$$

whence $m_\theta(t)$ divides $F(t)$. Consequently, there is a polynomial $\Psi(t) = \Psi_\theta(t;\mathbf{x},\mathbf{y}) \in \mathbb{Z}[t]$ having the property that

$$F(t) = m_\theta(t)\Psi(t). \tag{3.3}$$

Since $\deg(\Psi) = \deg(F) - \deg(m_\theta) \leqslant k-1-d$, we may write

$$\Psi(t) = b_0 + b_1 t + \ldots + b_{k-1-d}t^{k-1-d},$$

where $b_m \in \mathbb{Z}$ $(0 \leqslant m \leqslant k-1-d)$. Our immediate goal is to bound the coefficients b_m.

We claim that for $0 \leqslant m \leqslant k-d-1$, one has

$$|b_m| \ll X^{k-d-m}. \tag{3.4}$$

This we establish by considering the formal Laurent series for $m_\theta(t)^{-1}$. Thus, we have $m_\theta(t)^{-1} = e(t) \in \mathbb{Q}((1/t))$, where for suitable rational coefficients $e_j \in \mathbb{Q}$ $(j \geqslant d)$ one has

$$e(t) = \sum_{j=d}^{\infty} e_j t^{-j} = \frac{1}{c_d t^d}(1 + c_d^{-1}c_{d-1}t^{-1} + \ldots + c_d^{-1}c_0 t^{-d})^{-1}.$$

Note here that $c_d \neq 0$, and further that $e_j \ll_{\theta,j} 1$. We may therefore infer from (3.3) that $\Psi(t) = e(t)F(t)$, whence

$$\sum_{m=0}^{k-1-d} b_m t^m = \left(\sum_{j=d}^{\infty} e_j t^{-j}\right)\left(\sum_{i=0}^{k-1} a_i t^i\right).$$

In view of the bound (3.2), we deduce that for $0 \leqslant m \leqslant k-1-d$ one has

$$\begin{aligned} b_m &= e_d a_{m+d} + e_{d+1}a_{m+d+1} + \ldots + e_{k-1-m}a_{k-1} \\ &\ll X^{k-d-m} + X^{k-d-m-1} + \ldots + X \ll X^{k-d-m}. \end{aligned}$$

This confirms the bound (3.4). We may suppose henceforth that there is a positive number $C = C(k, \theta)$ having the property that

$$|b_m| \leqslant CX^{k-d-m} \quad (0 \leqslant m \leqslant k-d-1). \tag{3.5}$$

We now arrive at the polynomial identity that does the heavy lifting in the proof of Theorem 1.2.

Lemma 3.1. *Suppose that* $\mathbf{x}, \mathbf{y}$ *is an integral solution of the equation (1.1) with* $1 \leqslant x_i, y_i \leqslant X$ $(1 \leqslant i \leqslant k)$*, in which* $x_i = y_j$ *for no indices* i *and* j *with* $1 \leqslant i, j \leqslant k$*. Then, for each index* j *with* $1 \leqslant j \leqslant k$*, there is an integer* ρ_j*, with* $1 \leqslant |\rho_j| \leqslant kCX^{k-d}$*, having the property that*

$$\prod_{i=1}^{k} (x_i - y_j) = \rho_j m_\theta(-y_j).$$

Proof. Recalling (3.1) and (3.3), we see that

$$F(-y_j) = \prod_{i=1}^{k} (x_i - y_j) = m_\theta(-y_j)\Psi(-y_j).$$

But in view of (3.5), one has

$$|\Psi(-y_j)| \leqslant \sum_{m=0}^{k-1-d} |b_m| y_j^m \leqslant (k-d)CX^{k-d}.$$

Thus, there is an integer $\rho_j = \Psi(-y_j)$ with $|\rho_j| \leqslant kCX^{k-d}$ for which

$$\prod_{i=1}^{k} (x_i - y_j) = m_\theta(-y_j)\rho_j.$$

Notice here that since the left hand side is a non-zero integer, then so too are both factors on the right hand side. The conclusion of the lemma follows. □

We may now complete the proof of Theorem 1.2. Our previous discussion ensures that it is sufficient to count solutions $\mathbf{x}, \mathbf{y}$ of (1.1) with $1 \leqslant x_i, y_i \leqslant X$ $(1 \leqslant i \leqslant k)$, in which $x_i = y_j$ for no indices i and j with $1 \leqslant i, j \leqslant k$. Given any such solution, an application of Lemma 3.1 with $j = k$ shows that, for some integer ρ_k with $1 \leqslant |\rho_k| \leqslant kCX^{k-d}$, one has

$$\prod_{i=1}^{k} (x_i - y_k) = \rho_k m_\theta(-y_k). \tag{3.6}$$

Fix any one of the $O(X)$ possible choices for y_k, and likewise any one of the $O(X^{k-d})$ possible choices for ρ_k. Then we see from (3.6) that each of the factors $x_i - y_k$ $(1 \leqslant i \leqslant k)$ must be a divisor of the non-zero integer $N = \rho_k m_\theta(-y_k)$. It therefore follows from an elementary estimate for the divisor function that there are $O(N^\varepsilon)$ possible choices for $x_i - y_k$ $(1 \leqslant i \leqslant k)$. Fix any one such choice. Then since y_k has already been fixed, we see that $x_1, \ldots, x_k$ and y_k are now all fixed.

At this point we return to the equation (1.1). By taking norms from $\mathbb{Q}(\theta)$ down to $\mathbb{Q}$, we see that

$$\prod_{i=1}^{k} m_\theta(-y_i) = \prod_{i=1}^{k} m_\theta(-x_i).$$

The right hand side here is already fixed and non-zero. A divisor function estimate therefore shows that there are $O(X^\varepsilon)$ possible choices for integers $n_1, \ldots, n_k$ having the property that

$$m_\theta(-y_i) = n_i \quad (1 \leqslant i \leqslant k).$$

Fixing any one such choice for the k-tuple $\mathbf{n}$, we find that when $1 \leqslant i \leqslant k$, there are at most d choices for the integer solution y_i of the polynomial equation $m_\theta(-t) = n_i$. Altogether then, the number of possible choices for $\mathbf{x}$ and $\mathbf{y}$ given a fixed choice for y_k and ρ_k is $O((NX)^\varepsilon)$. Thus we conclude that the total number of possible choices for $\mathbf{x}$ and $\mathbf{y}$ is $O(X^{k-d+1+\varepsilon})$, and hence

$$\sum_{\nu \in \mathbb{Z}[\theta]} \tau_k(\nu; X, \theta)^2 - T_k(X) \ll X^{k-d+1+\varepsilon}.$$

This completes the proof of Theorem 1.2.

References

[1] A. J. Harper, A. Nikeghbali and M. Radziwiłł, *A note on Helson's conjecture on moments of random multiplicative functions*, in Analytic Number Theory (Springer, Cham, 2015), 145–169.

[2] W. P. Heap and S. Lindqvist, *Moments of random multiplicative functions and truncated characteristic polynomials*, Q. J. Math. **67** (2016), no. 4, 683–714.

[3] A. Sahay, *Moments of the Hurwitz zeta function on the critical line*, submitted, arXiv:2103.13542.

[4] P. Salberger, *Rational points of bounded height on threefolds*, Analytic Number Theory, Clay Math. Proc. **7** (2007), pp. 207–216, Amer. Math. Soc., Providence, RI.

[5] C. M. Skinner and T. D. Wooley, *On the paucity of non-diagonal solutions in certain diagonal Diophantine systems*, Quart. J. Math. Oxford (2) **48** (1997), 255–277.

[6] R. C. Vaughan and T. D. Wooley, *A special case of Vinogradov's mean value theorem*, Acta Arith. **79** (1997), no. 3, 193–204.

[7] T. D. Wooley, *Paucity problems and some relatives of Vinogradov's mean value theorem*, submitted, arXiv:2107.12238.

WH: Department of Mathematics, Shandong University, Jinan, Shandong 250100, China

E-mail address: winstonheap@gmail.com

AS: Department of Mathematics, University of Rochester, 908 Hylan Building, P.O. Box 270138, Rochester, NY 14627, USA

E-mail address: asahay@ur.rochester.edu

TDW: Department of Mathematics, Purdue University, 150 N. University Street, West Lafayette, IN 47907-2067, USA

E-mail address: twooley@purdue.edu