Canad. J. Math. Vol. **69** (3), 2017 pp. 595–612
http://dx.doi.org/10.4153/CJM-2016-007-2
© Canadian Mathematical Society 2016

# On the Digits of Sumsets

Christian Mauduit, Joël Rivat, and András Sárközy

*Abstract.* Let $\mathcal{A}$ and $\mathcal{B}$ be large subsets of $\{1,\dots,N\}$. We study the number of pairs $(a,b)\in\mathcal{A}\times\mathcal{B}$ such that the sum of binary digits of $a+b$ is fixed.

## 1 Introduction

Throughout this paper we will use the following notation: $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{R}$, and $\mathbb{C}$ denote the set of positive integers, non-negative integers, real numbers, and complex numbers, respectively, and $\|x\|$ denotes the distance from $x$ to the nearest integer. We will denote the sum of digits of an integer $n\ge 0$ written in base $g$ by $\mathrm{s}_g(n)$ and will write $\mathrm{s}_2(n)=\mathrm{s}(n)$.

There are more than 40 papers in which arithmetic properties of sumsets of "dense" sets of positive integers have been studied (most of these papers appeared in the last 40 years). A list of these papers is presented in [2]. In particular, in [16] the first and third authors studied the arithmetic structure of the set

$$\mathcal{U}_r(N)=\left\{n:\ n\in\mathbb{N},\ n\le N,\ \mathrm{s}_g(n)\equiv r \bmod m\right\} \tag{1.1}$$

(for fixed $g$, $r$, $m$ and large $N$), and they showed that these sets contain "many" sums $a+b$ with $a\in\mathcal{A}$, $b\in\mathcal{B}$, where $\mathcal{A}$, $\mathcal{B}$ are "dense" subsets of $\{1,\dots,N\}$.

***Theorem A*** *If $g\in\mathbb{N}$, $g\ge 2$, $m\in\mathbb{N}$, $(m,g-1)=1$, $r\in\mathbb{Z}$ and $\mathcal{A},\mathcal{B}\subset\{1,\dots,N\}$, then we have*

$$\left|\left|\left\{(a,b)\in\mathcal{A}\times\mathcal{B},\ s_g(a+b)\equiv r \bmod m\right\}\right|-\frac{|\mathcal{A}||\mathcal{B}|}{m}\right|\le 2\gamma N^{\lambda}\big(|\mathcal{A}||\mathcal{B}|\big)^{1/2},$$

*where $\lambda=\lambda(g,m)$ and $\gamma=\gamma(g,m)$ are defined by*

$$\lambda=\frac{1}{2\log g}\log\frac{g\sin(\pi/2m)}{\sin(\pi/2mg)}(<1),\qquad \gamma=\gamma(g,m)=\frac{g^2}{g^{\lambda}-1}.$$

So if $(|\mathcal{A}|\,|\mathcal{B}|)^{1/2}\gg N^{\lambda}$, then the set of the numbers $s_g(a+b)$ meets every residue class modulo $m$, and if $(|\mathcal{A}|\,|\mathcal{B}|)^{1/2}N^{-\lambda}\to+\infty$, then the numbers $s_g(a+b)$ are well distributed modulo $m$.

Received by the editors August 12, 2015.
Published electronically May 10, 2016.
Research partially supported by the Hungarian National Foundation for Scientific Research, Grants No K100291 and NK104183, the Agence Nationale de la Recherche project ANR-10-BLAN 0103 called MUNUM and ANR-FWF project ANR-14-CE34-0009 called MuDeRA, and Ciência sem Fronteiras (projet PVE 407308/2013-0).
AMS subject classification: **11A63**, 11B13.
Keywords: sumset, digits.

The study of the arithmetic structure of the set (1.1) was relatively easy, since this set is "dense"; *i.e.*, for fixed $g$, $r$, $m$, it contains a positive proportion of the integers up to $N$. Thus the first and third authors wrote in [17]:

> Since the integers characterized by a simple digit property have a very specific structure and they can be studied very efficiently by the generating function principle, one expects that it can be proved that much "thinner" sets of this type all have a nice arithmetic structure. The most natural way to construct "thin" sets of this type is to consider the sets
>
> $$\mathcal{V}_k = \{n : n \in \mathbb{N},\ n \le N,\ s_g(n) = k\} \tag{1.2}$$
>
> where $k \in \mathbb{N}$, $0 \le k \le (g-1)((\log N)/(\log g) + 1)$.

Indeed, we showed in [17] that for every $k$ we have

$$|\mathcal{V}_k| \ll_g N(\log N)^{-1/2},$$

so that these sets are much thinner than the set in (1.1). Motivated by this consideration, our goal in [17] was to study the arithmetic structure of the sets $\mathcal{V}_k$ in (1.2). We succeeded in proving some results similar to the ones proved in the easier situation studied in [16]. However, as we wrote in [17] (here we change the notation slightly):

> ...one would like to prove the $\mathcal{V}_k$ analogue of our result Theorem A. Unfortunately, we have not been able to prove such a theorem...

Thus, in particular, we have not been able to prove the following conjecture:

***Conjecture 1.1*** *If $\varepsilon > 0$, $N > N_0(\varepsilon)$, $\mathcal{A}, \mathcal{B} \subset \{1, 2, \dots, N\}$ and $|\mathcal{A}|, |\mathcal{B}| > \varepsilon N$, then there are integers $a$, $b$ such that $a \in \mathcal{A}$, $b \in \mathcal{B}$ and*

$$s_g(a+b) = \lfloor (g-1)\nu/2 \rfloor,$$

*where $\nu = \nu(N) \in \mathbb{N}$ is defined by $g^\nu \le N \le g^{\nu+1} - 1$.*

The set of the integers $n$ such that

$$s_g(n) = \left\lfloor \frac{g-1}{2} \left\lfloor \frac{\log n}{\log g} \right\rfloor \right\rfloor$$

can be generated by an infinite automaton (or an infinite substitution of constant length $g$) on the alphabet $\{0, \dots, g-1\}$ (see [10] for a precise definition of infinite automata and infinite substitutions). Fouvry and Mauduit [6] described the statistical properties of this set, and the goal of this paper is to study more deeply the statistical properties in order to be able to understand how it intersects sumsets.

The paper [17] appeared in 1997, and no advance has been made towards this conjecture since then. However, many papers have been published on integers characterized by digit properties [3–6,8,9,11–15,19]. In some of these papers (mostly in [6,8,12]) there are new ideas, methods, and results that can be used for attacking Conjecture 1.1. Indeed, by adapting, extending, and combining these ideas, we have been able to prove the conjecture. In order to shorten the discussion here we will restrict ourselves to the $g = 2$ special case. (The case $g > 2$ could be handled similarly; however, there are certain technical difficulties; thus, we expect that the proof would be much

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press

longer.) In this paper our goal is to present the proof of the following slightly more general form of the $g = 2$ case of the conjecture.

***Theorem 1.2*** *For any $L > 0$ and $\varepsilon > 0$ there is a number $N_0 = N_0(L, \varepsilon)$ such that if $N \in \mathbb{N}$, $N > N_0$, $k \in \mathbb{N}$,*

$$\left| k - \frac{\log N}{2\log 2} \right| < L(\log N)^{1/4}, \tag{1.3}$$

$$\mathcal{A}, \mathcal{B} \subset \{1, 2, \dots, N\},$$

*then, writing $\rho = \left(\frac{\log 2}{8}\right)^{1/2}$, we have*

$$\left| \left| \{(a,b) : a \in \mathcal{A},\ b \in \mathcal{B},\ \mathrm{s}(a+b) = k\} \right| - \left(\frac{\log 4}{\pi}\right)^{1/2} \frac{|\mathcal{A}||\mathcal{B}|}{(\log N)^{1/2}} \right| < \frac{N}{(\log N)^{1/2} \exp((\rho - \varepsilon)(\log\log N)^{1/2})} (|\mathcal{A}|\,|\mathcal{B}|)^{1/2}.$$

Note that if $\nu$ is defined as in Conjecture 1.1 (with $g = 2$), then we have $\frac{\log N}{2\log 2} = \frac{\nu}{2} + O(1)$ so that (1.3) holds with $\lfloor \nu/2 \rfloor$ in place of $k$. It follows from Theorem 1.2 that if

$$(|\mathcal{A}|\,|\mathcal{B}|)^{1/2} > \left(\frac{\pi}{\log 4}\right)^{1/2} \frac{N}{\exp((\rho - \varepsilon)(\log\log N)^{1/2})},$$

then there are $a \in \mathcal{A}$, $b \in \mathcal{B}$ with

$$\mathrm{s}(a+b) = \lfloor \nu/2 \rfloor, \tag{1.4}$$

and, indeed (applying Theorem 1.2 with $\frac{\varepsilon}{2}$ in place of $\varepsilon$) it also follows that the number of solutions of (1.4) in $a$ and $b$ is about as large as expected:

$$\left| \{(a,b) : a \in \mathcal{A},\ b \in \mathcal{B},\ \mathrm{s}(a+b) = k\} \right| = (1 + o(1)) \left(\frac{\log 4}{\pi}\right)^{1/2} \frac{|\mathcal{A}|\,|\mathcal{B}|}{(\log N)^{1/2}}.$$

In Section 6 we will also present an estimate from the opposite side.

## 2 Structure of the Proof of the Theorem

We will use the circle method. Define the positive integer $\nu$ by

$$2^{\nu-1} \leq 2N < 2^{\nu}. \tag{2.1}$$

Now define $\mathcal{V}_k$ by

$$\{n : n \leq 2^{\nu} - 1,\ \mathrm{s}(n) = k\}; \tag{2.2}$$

for $\alpha \in \mathbb{R}$, write

$$F(\alpha) = \sum_{n \in \mathcal{V}_k} \mathrm{e}(n\alpha), \quad G(\alpha) = \sum_{a \in \mathcal{A}} \mathrm{e}(a\alpha), \quad H(\alpha) = \sum_{b \in \mathcal{B}} \mathrm{e}(b\alpha), \tag{2.3}$$

and consider the integral

$$J = \int_{-1/2}^{1/2} G(\alpha) H(\alpha) F(-\alpha)\, d\alpha. \tag{2.4}$$

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press

Then

$$J = \int_{-1/2}^{1/2} \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \sum_{n\in\mathcal{V}_k} \mathrm{e}((a+b-n)\alpha)d\alpha \tag{2.5}$$
$$= \sum_{\substack{a+b-n=0\\ a\in\mathcal{A},\ b\in\mathcal{B},\ n\in\mathcal{V}_k}} 1 = \sum_{\substack{a\in\mathcal{A},\ b\in\mathcal{B}\\ \mathrm{s}(a+b)=k}} 1$$
$$= \big|\{(a,b) :\ a\in\mathcal{A},\ b\in\mathcal{B},\ \mathrm{s}(a+b)=k\}\big| .$$

Thus, it suffices to estimate the integral $J$. In order to do this we will first estimate $F(\alpha)$ defined in (2.3) for "large" $\|\alpha\|$ in Section 3. Next we will estimate it for "small" $\|\alpha\|$ in Section 4; finally, we will complete the proof of the theorem by using these estimates in Section 5.

## 3 Estimate of $F(\alpha)$ for Large $\|\alpha\|$

The study of the trigonometric product $\prod_{j=0}^{\nu-1}\left|\sin \pi 2^j \frac{a}{d}\right|$ for $(d,a,\nu)\in\mathbb{N}\times\mathbb{N}_0^2$ plays an important role in many works concerning the sum of digits function. For example the main results from [7] and [18] are based on the fact that this trigonometric product is uniformly bounded by $(\sqrt{3}/2)^{\nu-1}$. Results from [12,16,17] are based on upper bounds uniform in $a$ of the kind $e^{-c\nu/\log d}$ with $c>0$, and those from [11] on the upper bound on average

$$\frac{1}{d}\sum_{0\le a<d}\sum_{0\le j<\nu}\left|\sin \pi 2^j \frac{a}{d}\right| \le \left(\frac{\sqrt{3}}{2}\right)^{\nu} \frac{\sqrt{3}}{d^{\log(3/2)/\log 2}}.$$

The situation becomes much more complicated when the rational number $a/d$ is replaced by a real number $\alpha$. In Lemma 3.4 we give an explicit upper bound for the trigonometric product

$$\prod_{j=0}^{\nu-1}\left|\cos \pi(\theta+2^j\alpha)\right| = 2^{-\nu}\prod_{j=0}^{\nu-1}\left|1+\mathrm{e}(\theta+2^j\alpha)\right|$$

with $(\theta,\alpha)\in\mathbb{R}^2$ depending on $\|\theta\|$ and on the first non zero digit in the dyadic expansion of the real number $\alpha$ and in Lemma 3.6 we give a $L^1$ estimate for this trigonometric product.

***Lemma 3.1*** *For $(\theta,\alpha)\in\mathbb{R}^2$ we have*

$$\|\theta+\alpha\|^2 + \|\theta+2\alpha\|^2 \ge \tfrac{1}{5}\|\theta\|^2, \tag{3.1}$$

$$\left|1+\mathrm{e}(\theta+\alpha)\right|\cdot\left|1+\mathrm{e}(\theta+2\alpha)\right| \le 4\,e^{-2c\|\theta\|^2} \tag{3.2}$$

*with*

$$c = \pi^2/20. \tag{3.3}$$

***Remark*** Taking $\alpha = -3\theta/5$ we observe that (3.1) is optimal and (3.3) is also optimal (compare Taylor expansions in (3.2) when $\alpha=-3\theta/5$).

**Proof** We want to determine the minimum $m_\theta$ of $\alpha\mapsto\|\theta+\alpha\|^2+\|\theta+2\alpha\|^2$ when $\alpha$ runs over $\mathbb{R}$. By symmetry and periodicity we can assume that $0\le\theta\le 1/2$. Put $t=$

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press

$\theta+\alpha$ and $g(t) = \|t\|^2 + \|2t-\theta\|^2$. We have $m_\theta = g(t_0)$ for some $t_0 \in [-1/2, 1/2]$. Since $m_\theta \le g(\theta/2) = \theta^2/4$, we can assume that both $t_0 \in [-\theta/2, \theta/2]$ and $\|2t_0 - \theta\| \le \theta/2$. For $t \in [-1/2, (2\theta-1)/4]$ we have $-3/2 \le 2t-\theta \le -1/2$, thus $g(t) = t^2 + (2t-\theta+1)^2$, so that in this interval $g(t) \ge g(2(\theta-1)/5) = (1-\theta)^2/5$. For $t \in [(2\theta-1)/4, \theta/2]$ we have $g(t) = t^2 + (2t-\theta)^2$, so that in that interval $g(t) \ge g(2\theta/5) = \theta^2/5$. Observing that $\theta^2 \le (1-\theta)^2$, we conclude that the minimum is reached for $t_0 = 2\theta/5$ and get equation (3.1).

For $x \in [-1/2, 1/2]$, we have

$$0 \le \cos(\pi x) \le 1 - \frac{\pi^2 x^2}{2} + \frac{\pi^4 x^4}{24} \le 1 - \frac{\pi^2 x^2}{2} + \frac{\pi^4 x^4}{8} - \frac{\pi^6 x^6}{48} \le e^{-\frac{\pi^2 x^2}{2}}.$$

Observing that $|1+\mathrm{e}(u)| = 2\cos(\pi\|u\|)$, we deduce from the inequality above that

$$|1+\mathrm{e}(\theta+\alpha)| \cdot |1+\mathrm{e}(\theta+2\alpha)| \le 4\, e^{-\frac{\pi^2}{2}(\|\theta+\alpha\|^2 + \|\theta+2\alpha\|^2)},$$

and applying (3.1), we get (3.2). ■

***Lemma 3.2*** *For $(\theta,\alpha) \in \mathbb{R}^2$, $\nu \in \mathbb{N}$, and $c$ defined by (3.3), we have*

$$2^{-\nu} \prod_{j=0}^{\nu-1} \left|1+\mathrm{e}(\theta+2^j\alpha)\right| \le e^{-c\|\theta\|^2(\nu - 2\|\nu/2\|)} \le e^{c/4} e^{-c\|\theta\|^2\nu}. \tag{3.4}$$

**Proof** Notice that $\nu - 2\|\nu/2\|$ is an even integer $2\nu'$ with $2\nu' \le \nu \le 2\nu'+1$. Hence,

$$2^{-\nu} \prod_{j=0}^{\nu-1} \left|1+\mathrm{e}(\theta+2^j\alpha)\right| \le 2^{-2\nu'} \prod_{j=0}^{\nu'-1} \left|1+\mathrm{e}(\theta+2^{2j}\alpha)\right| \left|1+\mathrm{e}(\theta+2^{2j+1}\alpha)\right|$$

and applying Lemma 3.1 with $\alpha$ replaced by $2^j\alpha$ for $j = 0, \dots, \nu'-1$, we get the result. ■

***Lemma 3.3*** *For $0 \le \theta_0 \le \frac{1}{2}$, $\alpha \in \mathbb{R}$, $\nu \in \mathbb{N}$, and $c$ defined by (3.3), we have*

$$2^{-\nu} \int_{\|\theta\|\ge\theta_0} \prod_{j=0}^{\nu-1} \left|1+\mathrm{e}(\theta+2^j\alpha)\right| d\theta \le \sqrt{\pi}\, e^{c/4} \frac{e^{-c\theta_0^2\nu}}{\sqrt{c\nu}}. \tag{3.5}$$

**Proof** By (3.4) it is enough to observe that

$$\int_{\|\theta\|\ge\theta_0} e^{-c\|\theta\|^2\nu} d\theta = 2\, e^{-c\theta_0^2\nu} \int_{\theta_0}^{1/2} e^{-c(\theta^2-\theta_0^2)\nu} d\theta,$$

and writing $\theta = \theta_0 + t$, we have

$$\int_{\theta_0}^{1/2} e^{-c(\theta^2-\theta_0^2)\nu} d\theta \le \int_0^{+\infty} e^{-c(t^2+2\theta_0 t)\nu} dt \le \int_0^{+\infty} e^{-ct^2\nu} dt = \frac{\sqrt{\pi}}{2\sqrt{c\nu}},$$

which gives (3.5). ■

***Lemma 3.4*** *Let $\nu_1 \in \mathbb{N}$, $(\theta,\alpha) \in \mathbb{R}^2$ such that $\|\theta\| < \frac{1}{4}$ and $2^{-\nu_1} \le \|\alpha\| < 2^{1-\nu_1}$. For $\nu \ge \nu_1$ and $c$ defined by (3.3), we have*

$$2^{-\nu} \prod_{j=0}^{\nu-1} |1+\mathrm{e}(\theta+2^j\alpha)| \ll \|\theta\| e^{-c\|\theta\|^2\nu} + 2^{\nu_1-\nu} + \exp\left(-\sigma(\theta)\sqrt{\nu-\nu_1}\right), \tag{3.6}$$

*where* $\sigma(\theta) = \sqrt{-\frac{1}{2}(\log 2)\log\big(\sin\pi(\|\theta\| + \frac{1}{4})\big)}$.

**Proof** If $\nu_1 = 1$, *i.e.* $\|\alpha\| = 1/2$ then for $j = 0$ we observe that

$$\tfrac{1}{2}\big|1 + \mathrm{e}(\theta + \tfrac{1}{2})\big| = \big|\sin\pi\theta\big| \le \pi\,\|\theta\|$$

and for $1 \le j \le \nu - 1$ we have $\frac{1}{2}\,\big|1 + \mathrm{e}(\theta + 2^j\alpha)\big| = \frac{1}{2}\,|1 + \mathrm{e}(\theta)| \le e^{-c\|\theta\|^2}$ (using (3.2) with $\alpha = 0$), and we obtain that (3.6) is satisfied. Therefore, we can assume that $\nu_1 \ge 2$.

By periodicity, we can assume that $-1/2 < \alpha < 1/2$. Then if $-1/2 < \alpha < 0$, observing that $\big|1 + \mathrm{e}(\theta + 2^j\alpha)\big| = \big|1 + \mathrm{e}(-\theta - 2^j\alpha)\big|$, we can replace $(\theta, \alpha)$ by $(-\theta, -\alpha)$, so that we can assume that $0 \le \alpha < 1/2$. We can write

$$\alpha = \sum_{i=1}^{\infty} a_i 2^{-i}$$

with $a_1 = \cdots = a_{\nu_1 - 1} = 0$, $a_{\nu_1} = 1$ and $a_i \in \{0, 1\}$ for $i \ge \nu_1 + 1$.

In the word $a_1 \cdots a_{\nu+1}$, let us consider the length $\ell_1$ of the largest subword of the shape $01\cdots1$. This means that $\ell_1$ is the greatest element of $\{2, \ldots, \nu - \nu_1 + 3\}$ with the property that there exist an integer $j_0$ with $0 \le \nu_1 - 2 \le j_0 \le \nu + 1 - \ell_1 \le \nu - 1$ such that $a_{j_0+1} = 0$ and $a_{j_0+2} = \cdots = a_{j_0+\ell_1} = 1$ (taking $j_0 = \nu_1 - 2$ and $\ell_1 = 2$ show that the set of such $\ell_1$'s is not empty). Under these conditions we have

$$\Big\|2^{j_0}\alpha - \tfrac{1}{2}\Big\| = \Big\|\sum_{i \ge j_0+2} a_i 2^{j_0 - i} - \sum_{i \ge j_0+2} 2^{j_0 - i}\Big\| = \sum_{i \ge j_0+\ell_1+1} (1 - a_i) 2^{j_0 - i} \le 2^{-\ell_1}.$$

For $\|\theta\| \le \frac{1}{4}$ we have

$$\big\|\theta + 2^{j_0}\alpha - \tfrac{1}{2}\big\| \le \|\theta\| + \big\|2^{j_0}\alpha - \tfrac{1}{2}\big\| \le \|\theta\| + 2^{-\ell_1} \le \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2};$$

thus, observing that the sinus is increasing over $[0, \pi/2]$ we obtain for $\|\theta\| \le \frac{1}{4}$:

$$\tfrac{1}{2}\,\big|1 + \mathrm{e}(\theta + 2^{j_0}\alpha)\big| = \sin\pi\,\big\|\theta + 2^{j_0}\alpha - \tfrac{1}{2}\big\| \le \sin\pi\big(\|\theta\| + 2^{-\ell_1}\big).$$

Applying (3.4) to the products for $0 \le j < j_0$ and for $j_0 < j \le \nu - 1$, we get

$$2^{-\nu}\prod_{j=0}^{\nu-1}\big|1 + \mathrm{e}(\theta + 2^j\alpha)\big| \le \sin\pi\big(\|\theta\| + 2^{-\ell_1}\big)\, e^{c/2} e^{-c\|\theta\|^2(\nu-1)}. \tag{3.7}$$

In the special case where $a_{\nu_1} = a_{\nu_1+1} = \cdots = a_{\nu+1} = 1$, we have $j_0 = \nu_1 - 2$ and $\ell_1 = \nu - \nu_1 + 3$ and we get (3.6). From now on we can assume that there exists $i \in \{\nu_1 + 1, \ldots, \nu + 1\}$ such that $a_i = 0$. In the word $a_1 \cdots a_{\nu+1}$, let us consider the length $\ell_0$ of the largest subword of the shape $10\cdots0$. That means that $\ell_0$ is the greatest element of $\{2, \ldots, \nu - \nu_1 + 2\}$ with the property that there exist $j_0 \in \{\nu_1 - 1, \ldots, \nu + 1 - \ell_0\}$ such that $a_{j_0+1} = 1$ and $a_{j_0+2} = \cdots = a_{j_0+\ell_0} = 0$. Then

$$\big\|2^{j_0}\alpha - \tfrac{1}{2}\big\| = \sum_{i \ge j_0+\ell_0+1} a_i 2^{j_0 - i} \le \sum_{i \ge j_0+\ell_0+1} 2^{j_0 - i} = 2^{-\ell_0}$$

and as above we obtain for $\|\theta\| \le \frac{1}{4}$:

$$2^{-\nu}\prod_{j=0}^{\nu-1}\big|1 + \mathrm{e}(\theta + 2^j\alpha)\big| \le \sin\pi\big(\|\theta\| + 2^{-\ell_0}\big)\, e^{c/2} e^{-c\|\theta\|^2(\nu-1)}. \tag{3.8}$$

Let $\ell = \ell_0 + \ell_1$. Since $\max(\ell_0, \ell_1) \geq \ell/2$, combining (3.7) and (3.8), we get for $\|\theta\| \leq \frac{1}{4}$:

$$2^{-\nu} \prod_{j=0}^{\nu-1} \left|1 + \mathrm{e}(\theta + 2^j \alpha)\right| \leq \sin \pi\big( \|\theta\| + 2^{-\ell/2} \big) e^{c/2} e^{-c\|\theta\|^2 (\nu-1)}. \tag{3.9}$$

In the word $a_{\nu_1 - 1} \cdots a_{\nu+1}$, we observe that each subword of length $\ell$ contains the subword 10. Since there is no subword $0 \cdots 0$ of length $\geq \ell_0$, there need be a 1 in the first $\ell_0$ positions, and then there need be a 0 in the next $\ell_1$ positions. This implies that the number $\kappa$ of integers $j \in \{0, \dots, \nu - 1\}$ such that $(a_{j+1}, a_{j+2}) = (1, 0)$ is at least the number of disjoint intervals of $\ell$ integers in $[\nu_1 - 1, \nu + 1]$ and therefore satisfies $\kappa \geq \lfloor (\nu - \nu_1 + 3)/\ell \rfloor$. For such $j$ we have

$$\left\|2^j \alpha - \tfrac{1}{2}\right\| = \sum_{i \geq j+3} a_i 2^{j-i} \leq \tfrac{1}{4},$$

so that picking only those $j$'s in the product as above, we get for $\|\theta\| \leq \frac{1}{4}$

$$2^{-\nu} \prod_{j=0}^{\nu-1} \left|1 + \mathrm{e}(\theta + 2^j \alpha)\right| \leq \big( \sin \pi(\|\theta\| + \tfrac{1}{4}) \big)^{\kappa} \ll \big( \sin \pi(\|\theta\| + \tfrac{1}{4}) \big)^{(\nu - \nu_1)/\ell}.$$

In order to combine this bound with (3.9) we first observe that the right-hand side of (3.9) is estimated by $\|\theta\| e^{-c\|\theta\|^2 \nu} + 2^{-\ell/2}$, and this implies

$$2^{-\nu} \prod_{j=0}^{\nu-1} |1 + \mathrm{e}(\theta + 2^j \alpha)| \ll \|\theta\| e^{-c\|\theta\|^2 \nu} + \min\Big( 2^{-\ell/2}, \big( \sin \pi(\|\theta\| + \tfrac{1}{4}) \big)^{(\nu - \nu_1)/\ell} \Big).$$

The term $2^{-\ell/2}$ is decreasing with $\ell$, while for $\|\theta\| < \frac{1}{4}$ we have $0 < \sin \pi(\|\theta\| + \frac{1}{4}) < 1$ so that the other term is increasing with $\ell$. The minimum of these two bounds can be estimated by a uniform bound in $\ell$ by taking the worst possible value of $\ell$ (where the two bounds involving $\ell$ are equal):

$$\frac{-\ell^2}{2} \log 2 = (\nu - \nu_1) \log \sin \pi(\|\theta\| + \tfrac{1}{4}),$$

and finally we get (3.6). ■

***Lemma 3.5*** *For $c$ defined by (3.3), $0 < \theta_0 < \frac{1}{4}$, $1 \leq \nu_1 \leq \nu$, $2^{-\nu_1} \leq \|\alpha\| < 2^{1-\nu_1}$, we have*

$$2^{-\nu} \int_{\|\theta\| \leq \theta_0} \prod_{j=0}^{\nu-1} |1 + \mathrm{e}(\theta + 2^j \alpha)| d\theta \ll \frac{1 - e^{-c\theta_0^2 \nu}}{\nu} + \theta_0 2^{\nu_1 - \nu} + \theta_0 \exp\Big( -\sigma(\theta_0) \sqrt{\nu - \nu_1} \Big).$$

**Proof** Applying (3.6), it is enough to observe that $\sigma(\theta) \geq \sigma(\theta_0)$ for $\|\theta\| \leq \theta_0$ and integrate. ■

***Lemma 3.6*** *For $1 \leq \nu_1 \leq \nu$ and $2^{-\nu_1} \leq \|\alpha\| < 2^{1-\nu_1}$, we have*

$$2^{-\nu} \int_{-1/2}^{1/2} \prod_{j=0}^{\nu-1} \left|1 + \mathrm{e}(\theta + 2^j \alpha)\right| d\theta \ll \frac{1}{\nu} + \Big( \frac{\log \nu}{\nu} \Big)^{1/2} \exp\Big( -\Big( \frac{\log 2}{2} + O\Big( \sqrt{\frac{\log \nu}{\nu}} \Big) \Big) \sqrt{\nu - \nu_1} \Big).$$

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press

**Proof** Without loss of generality we can assume that $\nu \geq 30/c$, where $c$ is defined by (3.3). We combine Lemmas 3.3 and 3.5, and take

$$\theta_0 = \sqrt{\frac{\log(1+\sqrt{c\nu})}{c\nu}},$$

which is admissible, since for $30 \leq c\nu$, we have

$$0 < \theta_0 \leq \Big(\frac{\log(1+\sqrt{30})}{30}\Big)^{1/2} < \tfrac{1}{4}.$$

For this choice of $\theta_0$ we have

$$\frac{e^{-c\theta_0^2\nu}}{\sqrt{c\nu}} = \frac{1-e^{-c\theta_0^2\nu}}{c\nu} = \frac{1}{c\nu+\sqrt{c\nu}} \ll \frac{1}{\nu}$$

and we observe that

$$\sigma(\theta_0) = \sqrt{-\tfrac{1}{2}(\log 2)\log\Big(\sin\big(\tfrac{\pi}{4} + O(\sqrt{\nu^{-1}\log\nu})\big)\Big)} = \frac{\log 2}{2} + O(\sqrt{\nu^{-1}\log\nu}),$$

so that $2^{\nu_1-\nu} \ll \exp(-\sigma(\theta_0)\sqrt{\nu-\nu_1})$, and we get the expected estimate. ■

***Remark*** The term $\frac{1}{\nu}$ is optimal apart from the implied constant. Indeed, taking $\alpha = 1/2$, we have

$$2^{-\nu}\int_{-1/2}^{1/2}\prod_{j=0}^{\nu-1}\left|1+\mathrm{e}(\theta+2^j\alpha)\right| d\theta = \int_{-1/2}^{1/2}|\sin\pi\theta|\,|\cos\pi\theta|^{\nu-1}\,d\theta = \frac{2}{\pi\nu}.$$

We are now ready to estimate $|F(\alpha)|$ for large $\|\alpha\|$.

***Lemma 3.7*** *For $\nu_1 \in \mathbb{N}$, $\nu_1 \leq \nu$, and $2^{-\nu_1} \leq \|\alpha\| < 2^{1-\nu_1}$, we have*

$$|F(\alpha)| \ll N\Big(\tfrac{1}{\nu} + \big(\tfrac{\log\nu}{\nu}\big)^{1/2}\exp\Big(-\big(\tfrac{\log 2}{2} + O\big(\sqrt{\tfrac{\log\nu}{\nu}}\big)\big)\sqrt{\nu-\nu_1}\Big)\Big). \tag{3.10}$$

**Proof** Clearly, we have

$$\begin{aligned} F(\alpha) &= \sum_{n\in\mathcal{V}_k}\mathrm{e}(n\alpha) = \sum_{\substack{0\leq n\leq 2^\nu-1\\ s(n)=k}}\mathrm{e}(n\alpha)\\ &= \sum_{n=0}^{2^\nu-1}\mathrm{e}(n\alpha)\int_{-1/2}^{1/2}\mathrm{e}((s(n)-k)\theta)\,d\theta\\ &= \int_{-1/2}^{1/2}\sum_{n=0}^{2^\nu-1}\mathrm{e}(n\alpha+(s(n))\theta)\,\mathrm{e}(-k\theta)\,d\theta, \end{aligned}$$

so that

$$|F(\alpha)| \leq \int_{-1/2}^{1/2}\Big|\sum_{n=0}^{2^\nu-1}\mathrm{e}(n\alpha+(s(n))\theta)\Big|\,d\theta = \int_{-1/2}^{1/2}\Big|\prod_{j=0}^{\nu-1}(1+\mathrm{e}(\theta+2^j\alpha))\Big|\,d\theta.$$

Applying Lemma 3.6 and using (2.1), we get (3.10). ■

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press

## 4 Estimate of $F(\alpha)$ for Small $\|\alpha\|$

We will need the following lemma.

***Lemma 4.1*** *Assume that the function $b\colon \mathbb{N} \to \mathbb{R}$ satisfies the conditions*

$$\frac{1}{2}\mu + b(\mu) \in \mathbb{N} \text{ for every } \mu \in \mathbb{N} \tag{4.1}$$

*and*

$$\text{there is a } K \geq 1 \text{ such that for every } \mu \in \mathbb{N} \text{ we have } |b(\mu)| \leq K\mu^{1/4}, \tag{4.2}$$

*and define the set $\mathcal{E}_b$ by*

$$\mathcal{E}_b = \Big\{ n : n \in \mathbb{N},\ s(n) = \frac{1}{2}\Big\lfloor \frac{\log n}{\log 2} \Big\rfloor + b\Big( \Big\lfloor \frac{\log n}{\log 2} \Big\rfloor \Big) \Big\}.$$

*Write*

$$\eta = \Big( \frac{\log 4}{\pi} \Big)^{1/2}. \tag{4.3}$$

*Then we have*

$$E_b(x) := |\mathcal{E}_b \cap [1, x]| = \eta \frac{x}{(\log x)^{1/2}} + O_K\Big( \frac{x}{\log x} \Big)$$

*uniformly for $x \geq 2$.*

**Proof** This is the $g = 2$ special case of [6, Theorem 1.1]. ■

***Lemma 4.2*** *If $L$, $N$, and $k$ are defined as in the theorem, $\nu$, $\mathcal{V}_k$ and $\eta$ are defined by* (2.1), (2.2) *and* (4.3), *then we have*

$$V_k(x) = |\mathcal{V}_k \cap [1, x]| = \eta \frac{x}{(\log x)^{1/2}} + O_L\Big( \frac{N}{\log N} \Big). \tag{4.4}$$

*uniformly for $2 \leq x \leq 2^\nu - 1$.*

**Proof** If $x \leq \frac{N}{\log N}$, then (4.4) holds trivially, thus we may restrict ourselves to

$$\frac{N}{\log N} < x \leq 2^\nu - 1 (< 4N)$$

(where the last inequality follows from (2.1)). Define the integer $\nu_2$ by

$$2^{\nu_2} \leq \frac{N}{\log N} < 2^{\nu_2 + 1}, \tag{4.5}$$

and define the function $b\colon \mathbb{N} \to \mathbb{R}$ in the following way. Let

$$b(\mu) = k - \frac{1}{2}\mu \quad \text{if } \mu \in \mathbb{N}, \quad \nu_2 \leq \mu \leq \nu \tag{4.6}$$

and

$$b(\mu) = \begin{cases} \frac{1}{2} & \text{for } \mu \text{ odd}, \\ 1 & \text{for } \mu \text{ even}, \end{cases} \quad \text{if } \mu \in \mathbb{N} \text{ and } \mu \notin [\nu_2, \nu]. \tag{4.7}$$

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press

For this function $b$, condition (4.1) holds trivially. Equation (4.2) also holds trivially for $\mu \notin [\nu_2, \nu]$ for any fixed $K$ and large enough $N$, while if

$$\nu_2 \leq \mu \leq \nu, \tag{4.8}$$

then by (2.1), (4.5), and (4.8) we have

$$\frac{N}{2\log N} < 2^{\nu_2} \leq 2^{\mu} \leq 2^{\nu} \leq 4N,$$

whence

$$\frac{\log N}{\log 2} - \frac{\log\log N}{\log 2} + O(1) < \nu_2 \leq \mu \leq \nu < \frac{\log N}{\log 2} + O(1). \tag{4.9}$$

It follows from (1.3), (2.1), (4.6), (4.8), and (4.9) that for $N$ large enough, we have

$$\begin{aligned}|b(\mu)| = \Big|k - \frac{1}{2}\mu\Big| &\leq \Big|k - \frac{1}{2}\frac{\log N}{\log 2}\Big| + \frac{1}{2}\Big|\frac{\log N}{\log 2} - \mu\Big| \\ &< L(\log N)^{1/4} + \frac{1}{2}\frac{\log\log N}{\log 2} + O(1) \\ &< (L+1)(\log N)^{1/4},\end{aligned}$$

so that (4.2) holds with $K = L + 1$ and the function $b$ defined by (4.6) and (4.7). Thus, by Lemma 4.1, we have

$$\begin{aligned}E_b(x) &= \eta\frac{x}{(\log x)^{1/2}} + O_K\Big(\frac{x}{\log x}\Big) \\ &= \eta\frac{x}{(\log x)^{1/2}} + O_L\Big(\frac{x}{\log x}\Big) \qquad (\text{for } 2 \leq x \leq 2^{\nu}).\end{aligned} \tag{4.10}$$

Assume now that $2^{\nu_2} \leq n \leq 2^{\nu}$. Then writing $\mu = \big\lfloor \frac{\log n}{\log 2} \big\rfloor$, clearly we have $\nu_2 \leq \mu \leq \nu$; thus, by (4.6) we have

$$b(\mu) = b\Big(\Big\lfloor \frac{\log n}{\log 2}\Big\rfloor\Big) = k - \frac{1}{2}\mu = k - \frac{1}{2}\Big\lfloor\frac{\log n}{\log 2}\Big\rfloor,$$

whence

$$k = \frac{1}{2}\Big\lfloor\frac{\log n}{\log 2}\Big\rfloor + b\Big(\Big\lfloor\frac{\log n}{\log 2}\Big\rfloor\Big) \qquad (\text{for } 2^{\nu_2} \leq n \leq 2^{\nu}). \tag{4.11}$$

It follows from (4.11) and the definitions of $\mathcal{V}_k$ and $\mathcal{E}_b$ that

$$\mathcal{V}_k \cap [2^{\nu_2}, 2^{\nu} - 1] = \mathcal{E}_b \cap [2^{\nu_2}, 2^{\nu} - 1].$$

Thus, for $2^{\nu_2} \leq x \leq 2^{\nu} - 1$, we have

$$V_k(x) - V_k(2^{\nu_2}) = E_b(x) - E_b(2^{\nu_2}),$$

whence, by (4.5), (4.10), and the definitions of $\mathcal{V}_k$ and $\mathcal{E}_b$,

$$\begin{aligned}V_k(x) = E_b(x) + V_k(2^{\nu_2}) - E_b(2^{\nu_2}) &= \eta\frac{x}{(\log x)^{1/2}} + O_L\Big(\frac{x}{\log x}\Big) + O(2^{\nu_2}) \\ = \eta\frac{x}{(\log x)^{1/2}} + O_L\Big(\frac{x}{\log x}\Big) + O\Big(\frac{N}{\log N}\Big) &= \eta\frac{x}{(\log x)^{1/2}} + O_L\Big(\frac{N}{\log N}\Big). \qquad \blacksquare\end{aligned}$$

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press

***Lemma 4.3*** *Write*

$$\phi(\alpha) = \eta \frac{1}{(\log N)^{1/2}} \sum_{n=1}^{2^\nu - 1} \mathrm{e}(n\alpha). \tag{4.12}$$

*Then, using the same assumptions and notations as in Lemma 4.2, we have*

$$|F(\alpha) - \phi(\alpha)| = O_L\Big( \frac{N}{\log N} (N \|\alpha\| + 1) \Big) \tag{4.13}$$

*uniformly for all $\alpha$.*

**Proof** By partial summation, we write

$$\begin{aligned} F(\alpha) &= \sum_{n \in \mathcal{V}_k} \mathrm{e}(n\alpha) = \sum_{n=1}^{2^\nu - 1} \big( V_k(n) - V_k(n-1) \big) \, \mathrm{e}(n\alpha) \\ &= \sum_{n=1}^{2^\nu - 2} V_k(n) \big( \mathrm{e}(n\alpha) - \mathrm{e}((n+1)\alpha) \big) + V_k(2^\nu - 1) \, \mathrm{e}\big( (2^\nu - 1)\alpha \big). \end{aligned}$$

Then by Lemma 4.2, we get

$$\begin{aligned} F(\alpha) = \sum_{n=2}^{2^\nu - 2} \Big( \eta \frac{n}{(\log n)^{1/2}} + O_L\Big( \frac{N}{\log N} \Big) \Big) \big( \mathrm{e}(n\alpha) - \mathrm{e}((n+1)\alpha) \big) \\ + \Big( \eta \frac{2^\nu - 1}{(\log(2^\nu - 1))^{1/2}} + O_L\Big( \frac{N}{\log N} \Big) \Big) \mathrm{e}\big( (2^\nu - 1)\alpha \big) + O(1), \end{aligned}$$

so that, reversing the partial summation we obtain

$$\begin{aligned} F(\alpha) = \eta \sum_{n=3}^{2^\nu - 1} \Big( \frac{n}{(\log n)^{1/2}} - \frac{n-1}{(\log(n-1))^{1/2}} \Big) \mathrm{e}(n\alpha) \\ + O_L\Big( \frac{N}{\log N} \Big( \sum_{n=2}^{2^\nu - 2} |1 - \mathrm{e}(\alpha)| + 1 \Big) \Big) + O(1). \end{aligned}$$

Thus,

$$\begin{aligned} F(\alpha) = \eta \sum_{n=3}^{2^\nu - 1} \Big( \frac{1}{(\log n)^{1/2}} + O\Big( \frac{1}{(\log n)^{3/2}} \Big) \Big) \mathrm{e}(n\alpha) \\ + O_L\Big( \frac{N}{\log N} \Big( N \|\alpha\| + 1 \Big) \Big), \end{aligned} \tag{4.14}$$

where we used (2.1) and $|1 - \mathrm{e}(\alpha)| \leq 2\pi \|\alpha\|$. A little computation shows that we have

$$\sum_{n=3}^{2^\nu - 1} \frac{1}{(\log n)^{1/2}} \mathrm{e}(n\alpha) = \frac{1}{(\log N)^{1/2}} \sum_{n=3}^{2^\nu - 1} \mathrm{e}(n\alpha) + O\Big( \frac{N}{\log N} \Big), \tag{4.15}$$

$$\sum_{n=3}^{2^\nu - 1} \frac{1}{(\log n)^{3/2}} = O\Big( \frac{N}{(\log N)^{3/2}} \Big). \tag{4.16}$$

Equation (4.13) follows from (4.12), (4.14), (4.15), and (4.16). ■

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press

## 5 Completion of the Estimate of the Integral $J$

We will prove the following lemma.

***Lemma 5.1*** *Under the assumptions in the theorem and using the notation above, we have*

$$|F(\alpha)-\phi(\alpha)| = O_L\Big(\frac{N}{(\log N)^{1/2}\exp((\rho-\frac{\varepsilon}{2})(\log\log N)^{1/2})}\Big) \tag{5.1}$$

*uniformly for all* $\alpha$.

**Proof** Define $\tau$ by

$$\tau = \frac{(\log N)^{1/2}}{N\exp((\rho-\frac{\varepsilon}{3})(\log\log N)^{1/2})}.$$

Assume first that $\|\alpha\| \le \tau$. Then if $N$ is large enough in terms of $L$ and $\varepsilon$, then it follows from (4.13) in Lemma 4.3 that

$$\begin{aligned}|F(\alpha)-\phi(\alpha)| &= O_L\Big(\frac{N}{\log N}(N\|\alpha\|+1)\Big) \le O_L\Big(\frac{N}{\log N}(N\tau+1)\Big)\\ &= O_L\Big(\frac{N}{(\log N)^{1/2}\exp((\rho-\frac{\varepsilon}{3})(\log\log N)^{1/2})}\Big) \quad (\text{for } \|\alpha\|\le\tau),\end{aligned}$$

so that now (5.1) holds whenever $\|\alpha\| \le \tau$.

Assume now that

$$\|\alpha\| > \tau. \tag{5.2}$$

Clearly, we have

$$|F(\alpha)-\phi(\alpha)| \le |F(\alpha)| + |\phi(\alpha)|. \tag{5.3}$$

First, we will estimate $|F(\alpha)|$ by using Lemma 3.7. Define the positive integer $\nu_1$ as in Lemma 3.7:

$$2^{-\nu_1} \le \|\alpha\| < 2^{1-\nu_1}. \tag{5.4}$$

Then by (2.1), (5.2), and (5.4) we have

$$2^{\nu-\nu_1} = 2^{\nu}\cdot 2^{-\nu_1} > 2N\cdot\tfrac{1}{2}\|\alpha\| > N\tau$$

whence, by the definition of $\tau$,

$$\begin{aligned}\nu-\nu_1 > \frac{\log(N\tau)}{\log 2} &= \frac{1}{\log 2}\Big(\frac{1}{2}\log\log N - \Big(\rho-\frac{\varepsilon}{3}\Big)(\log\log N)^{1/2}\Big)\\ &= \frac{\log\log N}{2\log 2}\Big(1-2\Big(\rho-\frac{\varepsilon}{3}\Big)(\log\log N)^{-1/2}\Big).\end{aligned}$$

It follows that

$$\sqrt{\nu-\nu_1} > \frac{(\log\log N)^{1/2}}{(2\log 2)^{1/2}}\Big(1-\frac{\rho-\frac{\varepsilon}{3}}{(\log\log N)^{1/2}} + O\Big(\frac{1}{\log\log N}\Big)\Big)$$

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press

and

$$(5.5)\qquad \Big(\frac{\log 2}{2}+o(1)\Big)\sqrt{\nu-\nu_1} > \bigg(\Big(\frac{\log 2}{8}\Big)^{1/2}+o(1)\bigg)\big((\log\log N)^{1/2}+O(1)\big) = (\rho+o(1))(\log\log N)^{1/2}.$$

By (2.1), (5.4), and (5.5) we get from Lemma 3.7 that

$$(5.6)\qquad \begin{aligned}|F(\alpha)| &\ll N\Big(\frac{1}{\log N}+\frac{(\log\log N)^{1/2}}{(\log N)^{1/2}}\exp\big(-(\rho+o(1))(\log\log N)^{1/2}\big)\Big)\\ &\ll \frac{N}{(\log N)^{1/2}\exp((\rho-\frac{\varepsilon}{2})(\log\log N)^{1/2})}.\end{aligned}$$

Moreover, by (4.12), (5.2), and the inequality $|1-\mathrm{e}(\alpha)|\geq 4\,\|\alpha\|$ we have

$$(5.7)\qquad \begin{aligned}|\phi(\alpha)| &= \eta\frac{1}{(\log N)^{1/2}}\Big|\frac{1-\mathrm{e}((2^\nu-1)\alpha)}{1-\mathrm{e}(\alpha)}\Big|\\ &\ll \frac{1}{(\log N)^{1/2}}\cdot\frac{1}{\|\alpha\|} < \frac{1}{(\log N)^{1/2}}\cdot\frac{1}{\tau}\\ &= \frac{N\exp((\rho-\frac{\varepsilon}{3})(\log\log N)^{1/2})}{\log N}.\end{aligned}$$

By (5.3), (5.6), and (5.7) it follows that (5.1) also holds in the case (5.2). ■

Now we are ready to complete the proof of the theorem. The integral $J$ in (2.4) can be rewritten in the form

$$(5.8)\qquad J = J_1 + J_2,$$

where

$$J_1 = \int_{-1/2}^{1/2} G(\alpha)H(\alpha)\phi(-\alpha)\,d\alpha,\qquad J_2 = \int_{-1/2}^{1/2} G(\alpha)H(\alpha)\big(F(-\alpha)-\phi(-\alpha)\big)\,d\alpha.$$

Here we clearly have

$$(5.9)\qquad \begin{aligned}J_1 &= \int_{-1/2}^{1/2}\sum_{a\in\mathcal{A}}\mathrm{e}(a\alpha)\sum_{b\in\mathcal{B}}\mathrm{e}(b\alpha)\frac{\eta}{(\log N)^{1/2}}\sum_{n=1}^{2^\nu-1}\mathrm{e}(-n\alpha)\,d\alpha\\ &= \frac{\eta}{(\log N)^{1/2}}\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{n=1}^{2^\nu-1}\int_{-1/2}^{1/2}\mathrm{e}((a+b-n)\alpha)\,d\alpha\\ &= \frac{\eta}{(\log N)^{1/2}}\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}1 = \frac{\eta}{(\log N)^{1/2}}|\mathcal{A}||\mathcal{B}|,\end{aligned}$$

and by Lemma 5.1 we have

$$|J_2| \leq O_L\bigg(\frac{N}{(\log N)^{1/2}\exp((\rho-\frac{\varepsilon}{2})(\log\log N)^{1/2})}\bigg)\int_{-1/2}^{1/2}|G(\alpha)H(\alpha)|\,d\alpha.$$

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press

If $N$ is large enough in terms of $L$ and $\varepsilon$, then by using the Cauchy–Schwarz inequality we get that

(5.10)

$$\begin{aligned}|J_2| &\leq \frac{N}{(\log N)^{1/2}\exp((\rho-\varepsilon)(\log\log N)^{1/2})}\Big(\int_{-1/2}^{1/2}|G(\alpha)|^2\,d\alpha\int_{-1/2}^{1/2}|H(\alpha)|^2\,d\alpha\Big)^{1/2}\\ &= \frac{N}{(\log N)^{1/2}\exp((\rho-\varepsilon)(\log\log N)^{1/2})}\big(|\mathcal{A}||\mathcal{B}|\big)^{1/2}.\end{aligned}$$

By (2.5), (5.8), (5.9), and (5.10) we have

$$\begin{aligned}&\Big|\big|\{(a,b): a\in\mathcal{A},\ b\in\mathcal{B},\ s(a+b)=k\}\big| - \frac{\eta}{(\log N)^{1/2}}|\mathcal{A}||\mathcal{B}|\Big| =\\ &\qquad |J-J_1| = |J_2| < \frac{N}{(\log N)^{1/2}\exp((\rho-\varepsilon)(\log\log N)^{1/2})}\big(|\mathcal{A}||\mathcal{B}|\big)^{1/2},\end{aligned}$$

which completes the proof of the theorem. ■

## 6 Estimates From the Opposite Side

One might like to know how far Theorem 1.2 could be improved upon. In other words, what can be said from the opposite side? In this direction we will show the following theorem.

***Theorem 6.1*** *For $N\in\mathbb{N}$, $N\to\infty$ there are sets*

(6.1) $$\mathcal{A},\ \mathcal{B}\subset\{0,1,2,\dots,N\}$$

*such that*

(6.2) $$|\mathcal{A}| = |\mathcal{B}| = N\exp\Big(-\frac{4}{(\log 2)^{1/2}}(\log N)^{1/2}\log\log N + O(1)\Big)$$

*and*

$$\begin{aligned}\Big|\Big\{(a,b):\ a\in\mathcal{A},\ b\in\mathcal{B},\ s(a+b)\leq \frac{1}{2}\frac{\log N}{\log 2}\\ +\Big(\frac{1}{(\log 2)^{1/2}}-\frac{C}{\log\log N}\Big)(\log N)^{1/2}\log\log N\Big\}\Big|\\ < |\mathcal{A}|\,|\mathcal{B}|\exp\big(-2(\log\log N)^2 + O(\log\log N)\big)\end{aligned}$$

*(where $C$ is a positive absolute constant large enough).*

It can easily be deduced from this theorem that for these sets $\mathcal{A}$, $\mathcal{B}$, except for "very few" sums $a+b$ with $a\in\mathcal{A}$, $b\in\mathcal{B}$, the sum of digits of the sums $a+b$ is much greater than expected. For any $c>0$ and large $N$, there are much less than $\frac{|\mathcal{A}||\mathcal{B}|}{(\log N)^c}$ pairs $(a,b)$ with

$$s(a+b)\leq\frac{1}{2}\frac{\log N}{\log 2}+\Big(\frac{1}{(\log 2)^{1/2}}-\frac{C}{\log\log N}\Big)(\log N)^{1/2}\log\log N.$$

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press

**Proof** Write

$$\nu = \left\lfloor \frac{\log N}{\log 2} - \frac{4}{(\log 2)^{1/2}}(\log N)^{1/2}\log\log N \right\rfloor, \tag{6.3}$$

$$\mu = \left\lfloor \frac{4}{(\log 2)^{1/2}}(\log N)^{1/2}\log\log N - 1 \right\rfloor, \tag{6.4}$$

and let

$$\mathcal{A} = \{m\cdot 2^{\mu} + (2^{\mu}-1) : \ 0 \le m < 2^{\nu-1}\},$$
$$\mathcal{B} = \{n\cdot 2^{\mu} : 0 \le n < 2^{\nu-1}\}.$$

Then by (6.3) and (6.4), it follows from

$$a = m\cdot 2^{\mu} + (2^{\mu}-1) \in \mathcal{A},\ b = n\cdot 2^{\mu} \in \mathcal{B} \tag{6.5}$$

that we have

$$\begin{aligned} 0 < a+b &< 2^{\nu-1}\cdot 2^{\mu} + (2^{\mu}-1) + 2^{\nu-1}\cdot 2^{\mu} = 2^{\mu+\nu} + (2^{\mu}-1) \\ &\le 2^{\frac{\log N}{\log 2}-1} + 2^{O((\log N)^{1/2}\log\log N)} < \frac{1}{2}N + o(N) < N \end{aligned}$$

for $N$ large enough, so that both (6.1) and $\mathcal{A}+\mathcal{B} \subset \{1,2,\dots,N\}$ hold. Moreover, we have

$$|A| = |\mathcal{B}| = 2^{\nu-1}, \tag{6.6}$$

whence (6.2) follows from (6.3).

It also follows from (6.5) that

$$a+b = (m+n)\cdot 2^{\mu} + (2^{\mu}-1), \tag{6.7}$$

whence, by the $q$-additive property of the sum of digits function, we have

$$\begin{aligned} \mathrm{s}(a+b) &= \mathrm{s}((m+n)\cdot 2^{\mu} + (2^{\mu}-1)) = \mathrm{s}((m+n)\cdot 2^{\mu}) + \mathrm{s}(2^{\mu}-1) \\ &= \mathrm{s}(m+n) + \mathrm{s}(1\dots 1) = \mathrm{s}(m+n) + \mu \quad (\text{with } 0 < m+n < 2^{\nu}). \end{aligned} \tag{6.8}$$

We will call an integer $0 \le t < 2^{\nu}$ "bad" if

$$\mathrm{s}(t) \ge \frac{\nu}{2} - (\log\nu)\nu^{1/2},$$

and denote the set of these bad integers $t$ by $\mathcal{T}$. Indeed, if a sum $a+b$ with $a, b$ of form (6.5) is such that $m+n = t$ is a "bad" number, then by (6.7) and (6.8) we have

$$\mathrm{s}(a+b) = \mathrm{s}(t) + \mu \ge \left(\frac{\nu}{2} - (\log\nu)\nu^{1/2}\right) + \mu,$$

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press

while by (6.3) and (6.4), we have

$$\begin{aligned}\frac{\nu}{2}+\mu &\geq \frac{1}{2}\frac{\log N}{\log 2}-\frac{2(\log N)^{1/2}}{(\log 2)^{1/2}}\log\log N+\frac{4(\log N)^{1/2}}{(\log 2)^{1/2}}\log\log N-3\\ &= \frac{1}{2}\frac{\log N}{\log 2}+\frac{2(\log N)^{1/2}}{(\log 2)^{1/2}}\log\log N-3,\\ \log\nu &\leq \log\frac{\log N}{\log 2}+\log\Big(1-\frac{4(\log 2)^{1/2}}{(\log N)^{1/2}}\log\log N\Big)=\log\log N+O(1),\\ \nu^{1/2} &\leq \frac{(\log N)^{1/2}}{(\log 2)^{1/2}}\Big(1-\frac{4(\log 2)^{1/2}}{(\log N)^{1/2}}\log\log N\Big)^{1/2}=\frac{(\log N)^{1/2}}{(\log 2)^{1/2}}+O(\log\log N).\end{aligned}$$

Thus,

$$\begin{aligned}(\log\nu)\nu^{1/2} &\leq \frac{(\log N)^{1/2}}{(\log 2)^{1/2}}\log\log N+O((\log N)^{1/2}),\\ \mathrm{s}(a+b) &\geq \frac{1}{2}\frac{\log N}{\log 2}+\frac{(\log N)^{1/2}}{(\log 2)^{1/2}}\log\log N+O((\log N)^{1/2}),\end{aligned}$$

so that $\mathrm{s}(a+b)$ is "large" for such a pair $(a,b)$:

$$\mathrm{s}(a+b)>\frac{1}{2}\frac{\log N}{\log 2}+\Big(\frac{1}{(\log 2)^{1/2}}-\frac{C}{\log\log N}\Big)(\log N)^{1/2}\log\log N \tag{6.9}$$

where $C$ is a positive absolute constant large enough. Thus, if $a+b$ is a "good" sum, *i.e.*, the opposite of (6.9) holds, then

$$m+n=t \tag{6.10}$$

satisfies $\mathrm{s}(t)<\frac{\nu}{2}-(\log\nu)\nu^{1/2}$, so that $t\in\{0,1,\dots,2^{\nu}-1\}\smallsetminus\mathcal{T}$. The number of these $t$'s is $2^{\nu}-|\mathcal{T}|$, and if such a $t$ is fixed, and $m$, $n$ (with $0\leq m,n<2^{\nu-1}$) satisfy (6.10), then $m$, $n$, and thus also $a$, $b$ (with $a\in\mathcal{A}$, $b\in\mathcal{B}$) unique determine each other. Thus, the number of solutions of both (6.10) in $(m,n)$ and (6.7) in $(a,b)$ is at most

$$\min(|\mathcal{A}|,|\mathcal{B}|)=|\mathcal{A}|=|\mathcal{B}|=\sqrt{|\mathcal{A}||\mathcal{B}|}.$$

Thus, the number of "good" pairs $(a,b)$ for which the opposite of inequality (6.9) holds is at most the product of the number of such $t$'s multiplied by the upper bound

$$\begin{aligned}\Big|\Big\{(a,b):\ a\in\mathcal{A},\ b\in\mathcal{B},\ \mathrm{s}(a+b)\leq\frac{1}{2}\frac{\log N}{\log 2}\\ +\Big(\frac{1}{(\log 2)^{1/2}}-\frac{C}{\log\log N}\Big)(\log N)^{1/2}\log\log N\Big\}\Big|\\ \leq\sqrt{|\mathcal{A}||\mathcal{B}|}(2^{\nu}-|\mathcal{T}|).\end{aligned} \tag{6.11}$$

It remains to give a lower bound for $|\mathcal{T}|$. In order to do this we need two lemmas.

***Lemma 6.2*** *Let $X_1,\dots,X_\nu$ be independent random variables such that $\mathbb{P}(X_j=1)=\frac{1}{2}$ and $\mathbb{P}(X_j=0)=\frac{1}{2}$ for $j=1,\dots,\nu$. Then for any $t>0$, we have*

$$\mathbb{P}\Big(|X_1+\cdots+X_\nu-\tfrac{\nu}{2}|>t\Big)<2\exp(-2t^2/\nu).$$

**Proof** This is a special case of the so called "Chernoff bounds"; *i.e.*, apply [1, Corollary A.1.2] to the random variables $1 - 2X_1, \dots, 1 - 2X_\nu$ with $a = 2t$. ■

***Lemma 6.3*** *For $\nu \in \mathbb{N}$ and $\xi_\nu > 0$ we have*

$$\operatorname{card}\Big\{ 0 \le n < 2^\nu,\ \big|\mathrm{s}(n) - \tfrac{\nu}{2}\big| > \xi_\nu \sqrt{\nu} \Big\} < 2^{\nu+1} \exp(-2\,\xi_\nu^2).$$

**Proof** Apply Lemma 6.2 with $t = \xi_\nu \sqrt{\nu}$. ■

Using Lemma 6.3 (with $\log \nu$ in place of $\xi_\nu$), we get that

$$\begin{aligned} |\mathcal{T}| &= \Big| \Big\{ 0 \le t < 2^\nu,\ \mathrm{s}(t) \ge \frac{\nu}{2} - (\log \nu)\sqrt{\nu} \Big\} \Big| \\ &\ge |\{0 \le t < 2^\nu\}| - \Big|\Big\{0 \le t < 2^\nu,\ \Big|\mathrm{s}(t) - \frac{\nu}{2}\Big| > (\log \nu)\sqrt{\nu}\Big\}\Big| \\ &> 2^\nu - 2^{\nu+1}\exp(-2(\log \nu)^2). \end{aligned} \tag{6.12}$$

It follows from (6.6), (6.11), and (6.12) that

$$\begin{aligned} &\Bigg| \Bigg\{ (a,b) :\ a \in \mathcal{A},\ b \in \mathcal{B},\ \mathrm{s}(a+b) \le \frac{1}{2}\frac{\log N}{\log 2} \\ &\qquad + \Big( \frac{1}{(\log 2)^{1/2}} - \frac{C}{\log\log N} \Big) (\log N)^{1/2} \log\log N \Bigg\} \Bigg| \\ &\le \sqrt{|\mathcal{A}||\mathcal{B}|}\, 2^{\nu+1} \exp(-2(\log \nu)^2) \\ &\le |\mathcal{A}|\,|\mathcal{B}| \exp\big( -2(\log\log N)^2 + O(\log\log N) \big) \end{aligned}$$ ■

We have seen that there are large subsets $\mathcal{A}$, $\mathcal{B} \in \{1, 2, \dots, N\}$ with the property that

$$\mathrm{s}(a+b) = \Big\lfloor \frac{\nu}{2} \Big\rfloor \qquad \Big( = \Big\lfloor \frac{1}{2}\frac{\log N}{\log 2} \Big\rfloor \Big) \tag{6.13}$$

has much less solutions than expected. But how large can be $\mathcal{A}$, $\mathcal{B}$ so that (6.13) has no solution at all? It is trivial that there are $\mathcal{A}$, $\mathcal{B}$ with $|\mathcal{A}||\mathcal{B}| \gg N$ such that (6.13) has no solution. On the other hand, we have not been able to answer the following question.

***Problem 6.4*** Are there sets $\mathcal{A}$, $\mathcal{B} \in \{1, 2, \dots, N\}$ such that $|\mathcal{A}||\mathcal{B}|N \to \infty$ and (6.13) has no solution?

## References

[1] N. Alon and J. H. Spencer, *The probabilistic method*. Third ed., Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, Inc., Hoboken, NJ, 2008. http://dx.doi.org/10.1002/9780470277331

[2] A. Balog, J. Rivat, and A. Sárközy, *On arithmetic properties of sumsets*. Acta Math. Hungar. **144**(2014), no. 1, 18–42. http://dx.doi.org/10.1007/s10474-014-0436-y

[3] 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, pp. 87–104.

[4] M. Drmota, C. Mauduit, and J. Rivat, *The sum-of-digits function of polynomial sequences*. J. Lond. Math. Soc. (2) **84**(2011), no. 1, 81–102. http://dx.doi.org/10.1112/jlms/jdr003

[5] M. Drmota and J. F. Morgenbesser, *Generalized Thue-Morse sequences of squares*. Israel J. Math. **190**(2012), 157–193. http://dx.doi.org/10.1007/s11856-011-0186-2

[6] E. Fouvry and C. Mauduit, *Sur les entiers dont la somme des chiffres est moyenne*. J. Number Theory **114**(2005), no. 1, 135–152. http://dx.doi.org/10.1016/j.jnt.2005.03.007

[7] A. O. Gel'fond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*. Acta Arith. **13**(1967/1968), 259–265.

[8] B. Martin, C. Mauduit, and J. Rivat, *Théorème des nombres premiers pour les fonctions digitales*. Acta Arith. **165**(2014), no. 1, 11–45. http://dx.doi.org/10.4064/aa165-1-2

[9] ———, *Fonctions digitales le long des nombres premiers*. Acta Arith. **170**(2015), no. 2, 175–197. http://dx.doi.org/10.4064/aa170-2-5

[10] C. Mauduit, *Propriétés arithmétiques des substitutions et automates infinis*. Ann. Inst. Fourier **56**(2006), no. 7, 2525–2549. http://dx.doi.org/10.5802/aif.2248

[11] C. Mauduit and C. G. Moreira, *Phénomène de Moser–Newman pour les nombres sans facteur carré*. Bull. Soc. Math. France **143**(2015), no. 3, 599–617.

[12] C. Mauduit, C. Pomerance, and A. Sárközy, *On the distribution in residue classes of integers with a fixed sum of digits*. Ramanujan J. **9**(2005), no. 1–2, 45–62. http://dx.doi.org/10.1007/s11139-005-0824-6

[13] C. Mauduit and J. Rivat, *Propriétés q-multiplicatives de la suite* $\lfloor n^c \rfloor$, $c > 1$. Acta Arith. **118**(2005), no. 2, 187–203. http://dx.doi.org/10.4064/aa118-2-6

[14] ———, *La somme des chiffres des carrés*. Acta Math. **203**(2009), no. 1, 107–148. http://dx.doi.org/10.1007/s11511-009-0040-0

[15] ———, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*. Ann. of Math. (2) **171**(2010), no. 3, 1591–1646. http://dx.doi.org/10.4007/annals.2010.171.1591

[16] C. Mauduit and A. Sárközy, *On the arithmetic structure of sets characterized by sum of digits properties*. J. Number Theory **61**(1996), no. 1, 25–38. http://dx.doi.org/10.1006/jnth.1996.0134

[17] ———, *On the arithmetic structure of the integers whose sum of digits is fixed*. Acta Arith. **81**(1997), no. 2, 145–173.

[18] D. J. Newman and M. Slater, *Binary digit distribution over naturally defined sequences*. Trans. Amer. Math. Soc. **213**(1975), 71–78. http://dx.doi.org/10.1090/S0002-9947-1975-0384734-3

[19] L. Spiegelhofer, *Piatetski-Shapiro sequences via Beatty sequences*. Acta Arith. **166**(2014), no. 3, 201–229. http://dx.doi.org/10.4064/aa166-3-1

*Université d'Aix-Marseille and Institut Universitaire de France, Institut de Mathématiques de Marseille, CNRS UMR 7373, 163, avenue de Luminy, Case 907, 13288 MARSEILLE Cedex 9, France*
*e-mail*: mauduit@iml.univ-mrs.fr

*Université d'Aix-Marseille, Institut de Mathématiques de Marseille, CNRS UMR 7373, 163, avenue de Luminy, Case 907, 13288 MARSEILLE Cedex 9, France*
*e-mail*: joel.rivat@univ-amu.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

https://doi.org/10.4153/CJM-2016-007-2 Published online by Cambridge University Press