Uniform Distribution Theory 2 (2007), no.1, 39–52

uniform distribution theory

KLOOSTERMAN SUMS FOR MODIFIED VAN DER CORPUT SEQUENCES

William Banks — Filip Saidak — Mayumi Sakata

ABSTRACT. For every integer $n \in \mathbb{N}$, let $R(n)$ be the integer obtained by reversing the order of the base-g digits of n and call $R(n)$ the *reversal* of n (with respect to g). In this paper, we introduce and study a sequence $\widetilde{\mathcal{C}}(g) = \{R(n)\}_{n=1}^{\infty}$ which is closely related to the van der Corput sequence. We establish a few fundamental divisibility properties of reversals that lead to sharp estimates for the number of solutions to a system of congruences of the form $n \equiv s \pmod{v}$ and $R(n) \equiv t \pmod{w}$ $(s, v, t, w \in \mathbb{N})$.

Communicated by Florian Luca

Dedicated to Professor Robert F. Tichy on his 50th birthday

1. Introduction

In this paper we study divisibility properties of *reversals*, and using methods from the theory of exponential sums, we study their distribution over congruence classes and as solutions to systems of linear congruences. The close connection between reversals and *van der Corput sequences* (first defined in [8]), which is explained in this introduction, makes these investigations relevant to problems in several areas of applied probability and numerical integration theory.

We begin with some definitions. Let $\mathcal{X} = \{x_n\}_{n=1}^{\infty}$ be an infinite sequence of points in the interval $[0, 1)$, and let $\mathcal{X}_k$ denote the finite subsequence $\{x_n\}_{n=1}^{k}$ for each $k \in \mathbb{N}$. The *discrepancy* $\delta_k(\mathcal{X}) = \delta(\mathcal{X}_k)$ of the set $\mathcal{X}_k$ is defined by

$$\delta_k(\mathcal{X}) = \sup_{0 \leqslant A < B < 1} \left| \frac{\#(\mathcal{X}_k \cap [A, B))}{k} - (B - A) \right|.$$

2000 Mathematics Subject Classification: 11B83, 11K31, 11L07.
Keywords: van der Corput sequences, integer sequences, congruences, exponential sums, Kloosterman sums, primes.

The sequence $\mathcal{X}$ is said to be *uniformly distributed* if $\lim_{k\to\infty} \delta_k(\mathcal{X}) = 0$, and $\mathcal{X}$ is said to have *low discrepancy* if $\delta_k(\mathcal{X})$ is small for all $k \in \mathbb{N}$ (see [19]). As is well known, classical Monte Carlo methods used in numerical integration give relatively small errors for estimates using *random* sets of points or vertices (see [22]); however, pure randomness is hard to come by in practice. If the vertices are not completely random but are chosen as terms of a low discrepancy sequence, then one talks about *quasi-Monte Carlo methods* ([20, 22]), with Koksma-Hlawka and Erdős-Turán-Koksma type inequalities (see [10, 14, 15, 16, 17]) bounding the error terms of the approximations (see also [23, 25]).

One of the most useful one-dimensional examples of a sequence of *quasi-random numbers* is the famous *van der Corput sequence* (see [8] and also [5, 9, 22]), which is defined as follows. For a fixed base $g \geqslant 2$, consider the *base-g representation* of an integer $n > 0$:

$$n = \sum_{k=0}^{L-1} a_k(n) g^k. \tag{1}$$

Here, each digit $a_k(n)$ lies in $\{0, 1, \dots, g-1\}$, and the leading digit $a_{L-1}(n) \neq 0$. The integer $\ell(n) = L$ is called the *length* of n; we also say that $\ell(n)$ is the *number of digits* of n. The van der Corput sequence is the sequence $\mathcal{C}(g) = \{c_n\}_{n=1}^{\infty}$, where

$$c_n = \sum_{k=0}^{L-1} a_k(n) g^{-1-k}. \tag{2}$$

In other words, each term c_n of the van der Corput sequence is obtained by a symmetric reflection of the base-g digit expansion of n about the decimal point. The discrepancy of $\mathcal{C}(2)$ was first investigated by Haber [12], who showed that

$$\limsup_{k\to\infty} \frac{\delta_k^*(\mathcal{C}(2))\, k}{\log k} = \frac{1}{3\log 2},$$

where

$$\delta_k^*(\mathcal{X}) = \sup_{0\leqslant A<1} \left| \frac{\#(\mathcal{X}_k \cup [0, A))}{k} - A \right|.$$

This work was later improved by Béjian and Faure [4]. For an arbitrary base $g \geqslant 2$, Faure [11] proved that

$$\limsup_{k\to\infty} \frac{\delta_k(\mathcal{C}(g))\, k}{\log k} = \limsup_{k\to\infty} \frac{\delta_k^*(\mathcal{C}(g))\, k}{\log k} = \begin{cases} \dfrac{g-1}{4\log g} & \text{if } g \text{ is odd,} \\ \dfrac{g^2}{4(g+1)\log g} & \text{if } g \text{ is even.} \end{cases}$$

In this paper, we introduce and study a sequence $\widetilde{\mathcal{C}}(g) = \{R(n)\}_{n=1}^{\infty}$, which is closely related to the van der Corput sequence. For every integer $n \in \mathbb{N}$, let $R(n)$ be the integer obtained by reversing the order of the base-g digits of n. More explicitly, using the representation (1) we define

$$R(n) = \sum_{k=0}^{L-1} a_{L-1-k}(n) g^k = \sum_{k=0}^{L-1} a_k(n) g^{L-1-k} \tag{3}$$

and call $R(n)$ the *reversal* of n (with respect to g). Note that $R(n) = c_n g^L$, where c_n is given by (2). It is easy to see that $R(ng) = R(n)$ for all $n \geqslant 1$, and $\ell(R(n)) = \ell(n)$ if and only if $a_0(g) \neq 0$ (that is, $g \nmid n$).

One of the advantages of working with the sequence $\widetilde{\mathcal{C}}(g)$ rather than $\mathcal{C}(g)$ is that every reversal $R(n)$ is an *integer*, hence a variety of number theoretic tools can be brought to bear on questions about the arithmetic structure of $\widetilde{\mathcal{C}}(g)$. In particular, instead of studying the distribution of the van der Corput sequence in $[0, 1)$, our focus in this paper is on the arithmetic of reversals, a point of view that has not been previously considered.

In this paper we establish a few fundamental divisibility properties of reversals (see Lemma 3.1 and Lemma 3.2 in Section 3) that lead to sharp estimates for the number of solutions to a system of congruences of the form

$$n \equiv s \pmod{v} \quad \text{and} \quad R(n) \equiv t \pmod{w} \quad (s, v, t, w \in \mathbb{N});$$

see Theorem 3.3 and Theorem 3.4 below. In particular, we show that if s, t, v, w are integers with $v, w \geqslant 1$ and $\gcd(vw, g(g^2-1)) = 1$, and $\mathcal{A} \subseteq \{0, 1, \dots, g-1\}$, then

$$\left| \#\mathcal{N}(\mathcal{A}; s, t, v, w; x) - \frac{\#\mathcal{A}}{gvw}\, x \right| \ll x \exp\left(-\frac{\log x}{2(vw)^2 \log g} \right),$$

where

$$\mathcal{N}(\mathcal{A}; s, t, v, w; x) = \big\{ n \leqslant x : n \in \mathcal{N}(\mathcal{A}),\ n \equiv s \pmod{v},\ R(n) \equiv t \pmod{w} \big\}$$

and

$$\mathcal{N}(\mathcal{A}) = \{ n \in \mathbb{N} : n \equiv a \pmod{g} \text{ for some } a \in \mathcal{A} \}.$$

These results on uniformity of solutions of congruence systems of similar form are equivalent to generalizations of the van der Corput type problems to subsequences created by various arithmetic progressions (see [2, 24, 26]).

We remark that our methods rely heavily on ideas from the paper of Banks, Hart and Sakata [1] on palindromes; the results of that paper provided inspiration for the present work.

Acknowledgements. The authors would like to thank Igor Shparlinski for his comments on the original version of the manuscript, especially for pointing out

to us the relevance of our results to the study of van der Corput sequences. We also thank the referee for a careful reading of the manuscript and for bringing to our attention some recent work of Sylvain Col [7].

2. Estimates on exponential sums

We need the following simplified version of Lemma 2.2 of [1]:

Lemma 2.1. *Let us write $e(x) = \exp(2\pi i x)$ for all $x \in \mathbb{R}$. For all integers q, k, m with $q, k \geqslant 2$ (where $q \nmid m$), we have:*

$$\left|\sum_{a=0}^{k-1} e(am/q)\right| \leqslant k \exp(-4/q^2).$$

For every integer $L \geqslant 1$ and every subset $\mathcal{A} \subseteq \{0, 1, \dots, g-1\}$, let us define

$$\mathcal{N}_L(\mathcal{A}) = \{n : \ell(n) = L \text{ and } n \equiv a \pmod g \text{ for some } a \in \mathcal{A}\}.$$

Note that the condition $\ell(n) = L$ is equivalent to $g^{L-1} \leqslant n < g^L$. Clearly

$$\#\mathcal{N}_L(\mathcal{A}) = \begin{cases} \#\mathcal{A}(g-1)g^{L-2} & \text{if } L \geqslant 2, \\ \#(\mathcal{A}\backslash\{0\}) & \text{if } L = 1. \end{cases} \tag{4}$$

Lemma 2.2. *For all integers s, t, v, w, L with $v, w, L \geqslant 1$ and an arbitrary subset $\mathcal{A} \subseteq \{0, 1, \dots, g-1\}$, let*

$$S_L(\mathcal{A}; s, t, v, w) = \sum_{n \in \mathcal{N}_L(\mathcal{A})} e\left(\frac{sn}{v} + \frac{tR(n)}{w}\right).$$

If $v \nmid s$ or $w \nmid t$, $\gcd(vw, g(g^2-1)) = 1$, and $L \geqslant 6$, then

$$\big|S_L(\mathcal{A}; s, t, v, w)\big| \leqslant \#\mathcal{N}_L(\mathcal{A}) \cdot \exp(-L/(vw)^2).$$

Proof. Let $\mathcal{D} = \{0, 1, \dots, g-1\}$, and fix $L \geqslant 6$. Using (1) and (3), we have

$$\begin{aligned} S_L(\mathcal{A}; s, t, v, w) &= \sum_{n \in \mathcal{N}_L(\mathcal{A})} e\left(\frac{s}{v}\sum_{k=0}^{L-1} a_k(n) g^k + \frac{t}{w}\sum_{k=0}^{L-1} a_k(n) g^{L-1-k}\right) \\ &= \sum_{\substack{a_0, a_1, \dots, a_{L-1} \in \mathcal{D} \\ a_0 \in \mathcal{A},\ a_{L-1} \neq 0}} e\left(\frac{s}{v}\sum_{k=0}^{L-1} a_k g^k + \frac{t}{w}\sum_{k=0}^{L-1} a_k g^{L-1-k}\right) \\ &= \sum_{\substack{a_0, a_1, \dots, a_{L-1} \in \mathcal{D} \\ a_0 \in \mathcal{A},\ a_{L-1} \neq 0}} \prod_{k=0}^{L-1} e\left(a_k\left(\frac{sg^k}{v} + \frac{tg^{L-1-k}}{w}\right)\right) = \prod_{k=0}^{L-1} T_k, \end{aligned}$$

where

$$T_0 = \sum_{a\in\mathcal{A}} e\left(\frac{a(sw+tvg^{L-1})}{vw}\right), \quad T_{L-1} = \sum_{\substack{a\in\mathcal{D}\\ a\neq 0}} e\left(\frac{a(swg^{L-1}+tv)}{vw}\right),$$

$$T_k = \sum_{a\in\mathcal{D}} e\left(\frac{a(swg^k+tvg^{L-1-k})}{vw}\right), \qquad 1\leqslant k\leqslant L-2.$$

Let us define

$$\mathcal{B} = \{1\leqslant k\leqslant L-2 : vw \,|\, (swg^k+tvg^{L-1-k})\},$$
$$\mathcal{G} = \{1\leqslant k\leqslant L-2 : vw \nmid (swg^k+tvg^{L-1-k})\}.$$

Using Lemma 2.1 to estimate each term T_k in the product $\prod_{k=0}^{L-1} T_k$ when $k\in\mathcal{G}$ (note that $vw\geqslant 2$ since $v\nmid s$ or $w\nmid t$), and using the trivial estimate for the remaining terms, we derive the bound

$$\begin{aligned}\left|S_L(\mathcal{A};s,t,v,w)\right| &\leqslant \#\mathcal{A}\cdot(g-1)\cdot g^{\#\mathcal{B}}\cdot g^{\#\mathcal{G}}\exp(-4\#\mathcal{G}/(vw)^2)\\ &= \#\mathcal{N}_L(\mathcal{A})\exp(-4\#\mathcal{G}/(vw)^2). \end{aligned} \tag{5}$$

If $\mathcal{B}=\varnothing$, then $\#\mathcal{G}=L-2$ and the desired bound follows immediately from (5); hence, we may assume that $\mathcal{B}\neq\varnothing$.

Let $u=\gcd(vw,sw,tv)$. Note that $u<vw$ since $v\nmid s$ or $w\nmid t$; therefore, as $\gcd(vw,g)=1$, the condition $vw\,|\,(swg^k+tvg^{L-1-k})$ is equivalent to

$$swu^{-1}g^{2k}\equiv -tvu^{-1}g^{L-1} \pmod{vwu^{-1}}. \tag{6}$$

If $\gcd(vwu^{-1},swu^{-1})=d>1$, this congruence (for any $k\in\mathcal{B}$) implies that $d\,|\,tvu^{-1}$, which is impossible as $\gcd(vwu^{-1},swu^{-1},tvu^{-1})=1$. Thus, $\gcd(vwu^{-1},swu^{-1})=1$, and we see that (6) is equivalent to

$$(g^2)^k\equiv -tvu^{-1}(swu^{-1})^{-1}g^{L-1} \pmod{vwu^{-1}}. \tag{7}$$

Since $u<vw$ and $\gcd(vw,(g^2-1))=1$, it follows that $vwu^{-1}\nmid(g^2-1)$, hence the multiplicative order of g^2 in the group $(\mathbb{Z}/vwu^{-1}\mathbb{Z})^*$ is at least 2, which implies that the number of integers k with $1\leqslant k\leqslant L-2$ and satisfying (7) (that is, the cardinality of $\mathcal{B}$) is at most $\lceil (L-2)/2\rceil$. Then

$$\#\mathcal{G}\geqslant\lfloor (L-2)/2\rfloor\geqslant (L-3)/2,$$

and the desired bound again follows from (5). □

For $v\geqslant 1$ with $\gcd(v,g)=1$, we denote by Θ_v the order of g in the multiplicative group modulo v. We now turn our attention to sums of the form:

$$K_v(a,b)=\sum_{k=1}^{\Theta_v} e\left(\frac{ag^k+bg^{-k}}{v}\right),$$

where a, b are arbitrary, and the inversion g^{-k} is taken in the residue ring $\mathbb{Z}/v\mathbb{Z}$.

We say that a set of primes $\mathcal{S}$ is *good* if every prime $p \in \mathcal{S}$ satisfies the conditions $p \equiv 3 \pmod 4$, $p \nmid g(g-1)$, and $\Theta_p = \Omega(\log^2 p)$, and we have $\gcd(\Theta_{p_1}, \Theta_{p_2}) \leqslant 2$ for all $p_1, p_2 \in \mathcal{S}$, $p_1 \neq p_2$. A modulus v is said to be *special* if $v = v(\mathcal{S}) = \prod_{p \in \mathcal{S}} p$ for some good set of primes $\mathcal{S}$.

The following result, whose proof is based on Theorem 1.1 of [6], occurs as Lemma 2 of [3]:

Lemma 2.3. *Let $\mathcal{S}$ be a good set of primes, and let $v = v(\mathcal{S})$ be the special modulus corresponding to $\mathcal{S}$. There exist absolute constants $A, B > 0$ such that if $\min\{p \in \mathcal{S}\} \geqslant B$, then for all $a, b \in \mathbb{Z}$, the following bound holds:*

$$\big|K_v(a,b)\big| \leqslant \Theta_v \prod_{\substack{p \in \mathcal{S} \\ \gcd(a,b,p)=1}} \left(1 - \frac{A}{\log p (\log\log p)^5}\right).$$

The preceding lemma is complemented by the following result, a simplified form of Lemma 3 of [3] whose proof depends in an essential way on Lemma 1 of [13]:

Lemma 2.4. *If y is sufficiently large, there exists a good set of primes $\mathcal{S}$ in the interval $[y(\log y)^{-2}, y]$ of cardinality at least $\#\mathcal{S} = \Omega(y^{1/4}(\log y)^{-2})$.*

We now prove an analogue of Lemma 2.2 for $v = w$ being a special modulus:

Lemma 2.5. *For all integers s, t, v, L with $v, L \geqslant 1$ and an arbitrary subset $\mathcal{A} \subseteq \{0, 1, \dots, g-1\}$, let*

$$S_L(\mathcal{A}; s, t, v) = \sum_{n \in \mathcal{N}_L(\mathcal{A})} e\left(\frac{sn + tR(n)}{v}\right).$$

Suppose further that $\mathcal{S}$ is a good set of primes, and $v = v(\mathcal{S})$ is the special modulus corresponding to $\mathcal{S}$. There exist absolute constants $A, B > 0$ such that if $\min\{p \in \mathcal{S}\} \geqslant B$ and $v \nmid \gcd(s,t)$, then the following bound holds for $L \geqslant 3$ and $z \geqslant \max\{p \in \mathcal{S}\}$:

$$\big|S_L(\mathcal{A}; s, t, v)\big| \leqslant \#\mathcal{N}_L(\mathcal{A}) \cdot \exp\left(-\frac{A\,L}{\log z (\log\log z)^5}\right).$$

P r o o f. As in the proof of Lemma 2.2, we have

$$S_L(\mathcal{A}; s, t, v) = \sum_{\substack{a_0, a_1, \dots, a_{L-1} \in \mathcal{D} \\ a_0 \in \mathcal{A},\ a_{L-1} \neq 0}} \prod_{k=0}^{L-1} e(a_k(sg^k + tg^{L-1-k})/v),$$

and therefore

$$\left|S_L(\mathcal{A};s,t,v)\right| \leqslant \#\mathcal{A}\,(g-1)\prod_{k=1}^{L-2}\left|\sum_{a=0}^{g-1} e(a(sg^k+tg^{L-1-k})/v)\right|.$$

Now let us write $L-2 = m\Theta_v+\ell$, where $m=\lfloor (L-2)/\Theta_v\rfloor$ and $0\leqslant \ell<\Theta_v$. Using the arithmetic-geometric mean inequality, we derive that

$$\begin{aligned}\left|S_L(\mathcal{A};s,t,v)\right|^2 &\leqslant (\#\mathcal{A})^2(g-1)^2g^{2\ell}\prod_{k=1}^{m\Theta_v}\left|\sum_{a=0}^{g-1} e(a(sg^k+tg^{L-1-k})/v)\right|^2\\ &\leqslant (\#\mathcal{A})^2(g-1)^2g^{2\ell}\left(\frac{1}{m\Theta_v}\sum_{k=1}^{m\Theta_v}\left|\sum_{a=0}^{g-1} e(a(sg^k+tg^{L-1-k})/v)\right|^2\right)^{m\Theta_v}\\ &= (\#\mathcal{A})^2(g-1)^2g^{2\ell}\left(\frac{T}{m\Theta_v}\right)^{m\Theta_v}, \end{aligned} \tag{8}$$

where

$$\begin{aligned} T &= \sum_{k=1}^{m\Theta_v}\sum_{a,b=0}^{g-1} e((a-b)(sg^k+tg^{L-1-k})/v)\\ &= gm\Theta_v + m\sum_{\substack{a,b=0\\ a\neq b}}^{g-1}\sum_{k=1}^{\Theta_v} e((a-b)(sg^k+tg^{L-1-k})/v)\\ &= gm\Theta_v + m\sum_{\substack{a,b=0\\ a\neq b}}^{g-1} K_v((a-b)s,(a-b)tg^{L-1}).\end{aligned}$$

To estimate the last sum, we apply Lemma 2.3, assuming that $B>g$. Since $p\nmid \gcd(s,t)$, there exists a prime $p\in\mathcal{S}$ such that $\gcd(s,t,p)=1$; thus,

$$\left|K_v((a-b)s,(a-b)tg^{L-1})\right| \leqslant \left(1-\frac{A}{\log z(\log\log z)^5}\right)$$

holds for all a,b in the sum. Consequently,

$$|T| \leqslant gm\Theta_v + g(g-1)m\Theta_v\left(1-\frac{A}{\log z(\log\log z)^5}\right) \leqslant g^2m\Theta_v - \frac{Ag(g-1)m\Theta_v}{\log z(\log\log z)^5},$$

and by (8) we have

$$\left|S_L(\mathcal{A};s,t,v)\right|^2 \leqslant (\#\mathcal{A})^2(g-1)^2g^{2(L-2)}\left(1-\frac{A(1-1/g)}{\log z(\log\log z)^5}\right)^{m\Theta_v}.$$

Using (4), the estimates $1-1/g \geqslant 1/2$ and $m\Theta_v \geqslant (L-2)/2 \geqslant L/6$ (for $L \geqslant 3$), and replacing A by $24A$, the result follows. $\square$

3. Distributional properties of reversals

Lemma 3.1. *For all integers s, t, v, w, L with $v, w, L \geqslant 1$ and an arbitrary subset $\mathcal{A} \subseteq \{0, 1, \dots, g-1\}$, let*

$$\mathcal{N}_L(\mathcal{A}; s, t, v, w) = \big\{n \in \mathcal{N}_L(\mathcal{A}) : n \equiv s \pmod v \text{ and } R(n) \equiv t \pmod w\big\}.$$

If $\gcd(vw, g(g^2-1)) = 1$ and $L \geqslant 6$, then the following estimate holds:

$$\left|\#\mathcal{N}_L(\mathcal{A}; s, t, v, w) - \frac{\#\mathcal{N}_L(\mathcal{A})}{vw}\right| < \#\mathcal{N}_L(\mathcal{A}) \cdot \exp(-L/(vw)^2).$$

P r o o f. Using the elementary relation

$$\frac{1}{q}\sum_{h=0}^{q-1} e(hm/q) = \begin{cases} 1 & \text{if } m \equiv 0 \pmod q, \\ 0 & \text{otherwise,} \end{cases}$$

it follows that

$$\begin{aligned}\mathcal{N}_L(\mathcal{A}; s, t, v, w) &= \sum_{n \in \mathcal{N}_L(\mathcal{A})} \frac{1}{v}\sum_{a=0}^{v-1} e\left(\frac{a(n-s)}{v}\right) \cdot \frac{1}{w}\sum_{b=0}^{w-1} e\left(\frac{b(R(n)-t)}{w}\right) \\ &= \frac{1}{vw}\sum_{a=0}^{v-1}\sum_{b=0}^{w-1} e\left(-\frac{as}{v} - \frac{bt}{w}\right) \sum_{n \in \mathcal{N}_L(\mathcal{A})} e\left(\frac{an}{v} + \frac{bR(n)}{w}\right) \\ &= \frac{\#\mathcal{N}_L(\mathcal{A})}{vw} + \frac{1}{vw}\sum_{\substack{a=0 \\ (a,b)\neq(0,0)}}^{v-1}\sum_{b=0}^{w-1} e\left(-\frac{as}{v} - \frac{bt}{w}\right) \cdot S_L(\mathcal{A}; a, b, v, w),\end{aligned}$$

where $S_L(\mathcal{A}; a, b, v, w)$ is the exponential sum considered in Lemma 2.2. For all pairs $(a, b) \neq (0, 0)$ in the last double summation above, either $v \nmid a$ or $b \nmid t$; hence, by Lemma 2.2, we have

$$\left|\#\mathcal{N}_L(\mathcal{A}; s, t, v, w) - \frac{\#\mathcal{N}_L(\mathcal{A})}{vw}\right| \leqslant \frac{1}{vw}\sum_{\substack{a=0 \\ (a,b)\neq(0,0)}}^{v-1}\sum_{b=0}^{w-1} \big|S_L(\mathcal{A}; a, b, v, w)\big|$$

$$\leqslant \frac{1}{vw}\sum_{\substack{a=0 \\ (a,b)\neq(0,0)}}^{v-1}\sum_{b=0}^{w-1} \#\mathcal{N}_L(\mathcal{A}) \cdot \exp(-L/(vw)^2) < \#\mathcal{N}_L(\mathcal{A}) \cdot \exp(-L/(vw)^2).$$

This completes the proof. □

Similarly, using Lemma 2.5 instead of Lemma 2.2, we obtain the following result:

Lemma 3.2. *For all integers s,t,v,L with $v,L \geqslant 1$ and an arbitrary subset $\mathcal{A} \subseteq \{0,1,\dots,g-1\}$, let*

$$\mathcal{N}_L(\mathcal{A};s,t,v) = \big\{n \in \mathcal{N}_L(\mathcal{A}) : n \equiv s \pmod v \text{ and } R(n) \equiv t \pmod v\big\}.$$

Suppose that $\mathcal{S}$ is a good set of primes, and $v = v(\mathcal{S})$ is the special modulus corresponding to $\mathcal{S}$. There exist absolute constants $A, B > 0$ such that if $\min\{p \in \mathcal{S}\} \geqslant B$ and $v \nmid \gcd(s,t)$, then for $L \geqslant 3$ and $z \geqslant \max\{p \in \mathcal{S}\}$ we have:

$$\left|\#\mathcal{N}_L(\mathcal{A};s,t,v) - \frac{\#\mathcal{N}_L(\mathcal{A})}{v^2}\right| < \#\mathcal{N}_L(\mathcal{A}) \cdot \exp\left(-\frac{A\,L}{\log z(\log\log z)^5}\right).$$

The following two theorems, which extend Lemmas 3.1 and 3.2, respectively, describe the distribution of the pairs $\{(n,R(n)) : n \leqslant x\}$ over congruence classes:

Theorem 3.3. *For a real number $x \geqslant 1$, integers s,t,v,w with $v,w \geqslant 1$, and an arbitrary subset $\mathcal{A} \subseteq \{0,1,\dots,g-1\}$, let*

$$\mathcal{N}(\mathcal{A};s,t,v,w;x) = \big\{n \leqslant x : n \in \mathcal{N}(\mathcal{A}),\ n \equiv s \,(\mathrm{mod}\ v) \text{ and } R(n) \equiv t \,(\mathrm{mod}\ w)\big\},$$

where

$$\mathcal{N}(\mathcal{A}) = \bigcup_{L \geqslant 1} \mathcal{N}_L(\mathcal{A}) = \{n : n \equiv a \pmod g \text{ for some } a \in \mathcal{A}\}.$$

If $\gcd(vw, g(g^2-1)) = 1$, then the following estimate holds:

$$\left|\#\mathcal{N}(\mathcal{A};s,t,v,w;x) - \frac{\#\mathcal{A}}{gvw}\,x\right| \ll x \exp\left(-\frac{\log x}{2(vw)^2 \log g}\right).$$

Proof. We assume that $vw \geqslant 2$, since the case $v = w = 1$ is trivial. Let s,t,v,w and $\mathcal{A}$ be fixed, and write $\mathcal{N}(x) = \mathcal{N}(\mathcal{A};s,t,v,w;x)$ for all $x \geqslant 1$, and let

$$\mathcal{N}(y,x) = \big\{y \leqslant n \leqslant x : n \in \mathcal{N}(\mathcal{A}),\ n \equiv s \pmod v \text{ and } R(n) \equiv t \pmod w\big\}$$

for all $x \geqslant y \geqslant 1$. Let $L \geqslant 6$ be an integer parameter to be chosen later, and put $n_0 = \lfloor x/g^L \rfloor$. We begin with the following estimate:

$$\#\mathcal{N}(x) = \sum_{k=1}^{n_0} \#\mathcal{N}(kg^L+1, kg^L+g^L-1) + O(g^L + x/g^L).$$

For fixed k with $1 \leqslant k \leqslant n_0$, every integer $n \in \mathcal{N}(kg^L+1, kg^L+g^L-1)$ can be uniquely represented in the form $n = kg^L + m$, where $m \in \mathcal{N}(\mathcal{A})$, and the

integer $\beta = \ell(m)$ (which is determined by n) satisfies $1 \leqslant \beta \leqslant L$. The reversals $R(n)$ and $R(m)$ are related as follows:

$$R(n) = R(m)g^{L-\beta+\ell(k)} + R(k).$$

Since n satisfies the congruences

$$\begin{aligned} n &\equiv s \pmod{v}, \\ R(n) &\equiv t \pmod{w}, \end{aligned} \tag{9}$$

it follows that m satisfies

$$\begin{aligned} m &\equiv s - kg^L \pmod{v}, \\ R(m) &\equiv (t - R(k))g^{-L+\beta-\ell(k)} \pmod{w}. \end{aligned} \tag{10}$$

That is, m lies in the set

$$\widetilde{\mathcal{N}}(k,\beta) = \mathcal{N}_\beta\left(\mathcal{A}; s - kg^L, (t - R(k))g^{-L+\beta-\ell(k)}, v, w\right)$$

considered in Lemma 3.1. Conversely, if $1 \leqslant \beta \leqslant L$, and $m \in \widetilde{\mathcal{N}}(k,\beta)$, then m satisfies the congruences (10), hence the integer $n = kg^L + m$ satisfies (9); consequently, $n \in \mathcal{N}(kg^L + 1, kg^L + g^L - 1)$. We therefore have

$$\#\mathcal{N}(x) = \sum_{k=1}^{n_0}\sum_{\beta=1}^{L} \#\widetilde{\mathcal{N}}(k,\beta) + O(g^L + x/g^L). \tag{11}$$

Replacing the 4-tuple (s,t,v,w) by $(0,0,1,1)$ in the arguments above, we get

$$\frac{\#A}{g}\, x + O(1) = \sum_{k=1}^{n_0}\sum_{\beta=1}^{L} \#\mathcal{N}_\beta(\mathcal{A}) + O(g^L + x/g^L). \tag{12}$$

We now express the double sum in (11) as a sum of

$$T_1 = \sum_{k=1}^{n_0}\sum_{\beta=1}^{5} \#\widetilde{\mathcal{N}}(k,\beta) \qquad \text{and} \qquad T_2 = \sum_{k=1}^{n_0}\sum_{\beta=6}^{L} \#\widetilde{\mathcal{N}}(k,\beta).$$

For each term in T_1, we use the trivial estimate $\#\widetilde{\mathcal{N}}(k,\beta) \leqslant \#\mathcal{N}_\beta(\mathcal{A}) = O(1)$, and we obtain $T_1 = O(x/g^L)$. For each term in T_2, from Lemma 3.1 we get

$$\left|\widetilde{\mathcal{N}}(k,\beta) - \frac{\#\mathcal{N}_\beta(\mathcal{A})}{vw}\right| < \#\mathcal{N}_\beta(\mathcal{A}) \exp(-\beta/(vw)^2).$$

Taking into account (12), we derive that

$$T_2 = \sum_{k=1}^{n_0}\sum_{\beta=6}^{L} \frac{\#\mathcal{N}_\beta(\mathcal{A})}{vw} + O(T_3) = \frac{\#\mathcal{A}}{gvw}\, x + O\big(T_3 + x/g^L\big),$$

where

$$T_3 = \sum_{k=1}^{n_0} \sum_{\beta=6}^{L} \#\mathcal{N}_\beta(\mathcal{A}) \exp(-\beta/(vw)^2).$$

Noting that

$$\#\mathcal{N}_\beta(\mathcal{A}) \exp(-\beta/(vw)^2) \ll h^\beta,$$

where $h = g\exp(-1/(vw)^2) > 3/2$ (since $g \geqslant 2$ and $vw \geqslant 2$), it follows that

$$T_3 \ll \sum_{k=1}^{n_0} \sum_{\beta=0}^{L} h^\beta \ll n_0 h^L \ll x \exp(-L/(vw)^2).$$

Putting everything together, we obtain that

$$\#\mathcal{N}(x) = \frac{\#\mathcal{A}}{gvw}\, x + O\big(g^L + x\exp(-L/(vw)^2)\big).$$

We now choose

$$L = \left\lceil \frac{\log x}{(vw)^{-2} + \log g} \right\rceil$$

(to balance the two expressions in the error term), and the result follows. □

Similarly, using Lemma 3.2 instead of Lemma 3.1, we obtain the following result (the proof is omitted):

Theorem 3.4. *For a real number $x \geqslant 1$, integers s, t, v, w with $v, w \geqslant 1$, and an arbitrary subset $\mathcal{A} \subseteq \{0, 1, \dots, g-1\}$, let*

$$\mathcal{N}(\mathcal{A}; s, t, v; x) = \big\{n \leqslant x : n \in \mathcal{N}(\mathcal{A}),\ n \equiv s \pmod v \text{ and } R(n) \equiv t \pmod v\big\}.$$

Suppose further that $\mathcal{S}$ is a good set of primes, and $v = v(\mathcal{S})$ is the special modulus corresponding to $\mathcal{S}$. There exist absolute constants $A, B > 0$ such that if $\min\{p \in \mathcal{S}\} \geqslant B$, then the following bound holds for $L \geqslant 3$ and $z \geqslant \max\{p \in \mathcal{S}\}$:

$$\left|\#\mathcal{N}(\mathcal{A}; s, t, v; x) - \frac{\#\mathcal{A}}{gv^2}\, x\right| \ll x \exp\left(-\frac{A\log x}{\log g \log z (\log\log z)^5}\right).$$

To conclude this paper, we prove the following fundamental estimate:

Theorem 3.5. *For a real number $x \geqslant 1$ and integers t, w with $w \geqslant 1$, let*

$$\mathcal{N}(t, w; x) = \big\{n \leqslant x : R(n) \equiv t \pmod w\big\}.$$

Then

$$\left|\#\mathcal{N}(t, w; x) - \frac{x}{w}\right| \ll \sqrt{x}\log x.$$

P r o o f. For every $L \geqslant 1$, let $\mathcal{N}_L = \mathcal{N}_L(\{1, \dots, g-1\}) = \{n : \ell(n) = L \text{ and } g \nmid n\}$. The reversal map $R : N_L \to N_L$ is a bijection; therefore, defining $N_L(a, v) = \{n \in N_L : R(n) \equiv a \pmod v\}$ for all integers a, v with $v \geqslant 1$, and taking $m = R(n)$, we obtain

$$\begin{aligned} \#N_L(a, v) &= \#\{n \in N_L : R(n) \equiv a \pmod v\} \\ &= \#\{m \in N_L : m \equiv a \pmod v\} = \frac{\#N_L}{v} + O(1). \end{aligned} \tag{13}$$

For fixed t, w, write $\mathcal{N}(x) = \mathcal{N}(t, w; x)$ for all $x \geqslant 1$, and let $\mathcal{N}(y, x) = \big\{y \leqslant n \leqslant x : R(n) \equiv t \pmod w\big\}$ for all $x \geqslant y \geqslant 1$. Let $L \geqslant 1$ be an integer parameter to be chosen later, and put $n_0 = \lfloor x/g^L \rfloor$. As in the proof of Theorem 3.3,

$$\#\mathcal{N}(b, w; x) = \sum_{k=1}^{n_0} \#\mathcal{N}(kg^L + 1, kg^L + g^L - 1) + O(g^L + x/g^L).$$

For fixed k with $1 \leqslant k \leqslant n_0$, every integer $n \in \mathcal{N}(kg^L + 1, kg^L + g^L - 1)$ can be uniquely represented in the form $n = kg^L + mg^\alpha$, where $0 \leqslant \alpha < L$ and $g \nmid m$. Note that the integers α and $\beta = \ell(m)$ are uniquely determined by n, and $1 \leqslant \beta \leqslant L - \alpha$. The reversals $R(n)$ and $R(m)$ are related as follows:

$$R(n) = R(m)g^{L-\alpha-\beta+\ell(k)} + R(k).$$

Since n satisfies the congruence

$$R(n) \equiv b \pmod w, \tag{14}$$

it follows that m satisfies

$$R(m) \equiv (b - R(k))g^{-L+\alpha+\beta-\ell(k)} \pmod w. \tag{15}$$

That is, m lies in the set

$$\widetilde{\mathcal{N}}(k, \alpha, \beta) = \mathcal{N}_\beta\left((b - R(k))g^{-L+\alpha+\beta-\ell(k)}, w\right).$$

Conversely, if $0 \leqslant \alpha < L$, $1 \leqslant \beta \leqslant L - \alpha$, and $m \in \widetilde{\mathcal{N}}(k, \alpha, \beta)$, then m satisfies the congruence (15), hence the integer $n = kg^L + mg^\alpha$ satisfies (14); consequently, $n \in \mathcal{N}(kg^L + 1, kg^L + g^L - 1)$. Therefore,

$$\#\mathcal{N}(b, w; x) = \sum_{k=1}^{n_0} \sum_{\alpha=0}^{L-1} \sum_{\beta=1}^{L-\alpha} \#\widetilde{\mathcal{N}}(k, \alpha, \beta) + O(g^L + x/g^L).$$

Replacing the 2-tuple (t, w) by $(0, 1)$ in the arguments above, we also obtain

$$\lfloor x \rfloor = \sum_{n \leqslant x} 1 = \sum_{k=1}^{n_0} \sum_{\alpha=0}^{L-1} \sum_{\beta=1}^{L-\alpha} \#\mathcal{N}_\beta + O(g^L + x/g^L). \tag{16}$$

Using (13) together with (16), it follows that

$$\#\mathcal{N}(b,w;x) = \frac{x}{w} + O(g^L + L^2 x/g^L).$$

We now choose

$$L = \left\lceil \frac{\log x + 2\log\log x}{2\log g} \right\rceil,$$

and the result follows. □

REFERENCES

[1] BANKS, W. – HART, D. – SAKATA, M.: *Almost all palindromes are composite*, Math. Res. Lett. **11** (2004), no. 5-6, 853–868.

[2] BANKS, W. – HEATH-BROWN, D.R. – SHPARLINSKI, I.: *On the average value of divisor sums in arithmetic progressions*, Internal Math. Res. Notices **2005**, no. 1, 1–25.

[3] BANKS, W. – SHPARLINSKI, I.: *Prime divisors of palindromes*, Period. Math. Hungar. **51** (2005), no. 1, 1–10.

[4] BÉJIAN, R. – FAURE, H.: *Discrépance de la suite de Van der Corput*, Séminaire Delange-Pisot-Poitou, 19e année: 1977/78, Théorie des nombres, Fasc. **1**, Exp. No. 13, 14 pp., Secrtariat Math., Paris, 1978.

[5] CAFLISCH, R.E.: *Monte Carlo and quasi-Monte Carlo methods*, Acta numerica **7**, Cambridge Univ. Press, Cambridge, 1998, pp. 1–49.

[6] COCHRANE, T. – PINNER, C. – ROSENHOUSE, J.: *Bounds on exponential sums and the polynomial Waring problem mod p*, J. London Math. Soc. (2) **67** (2003), no. 2, 319–336.

[7] COL, S.: *Palindromes dans les progressions arithmétiques*, Acta Arith. (to appear).

[8] VAN DER CORPUT, J.G.: *Verteilungsfunktionen. I. Mitt*, Proc. Ned. Wet. Amsterdam **38** (1935), 813–821.

[9] DRMOTA, M.– TICHY, R.F.: *Sequences, Discrepancies and Applications*, Lecture Notes in Math. **1651**, Springer-Verlag, Berlin, 1997.

[10] ERDŐS, P. – TURÁN, P.: *On a problem in the theory of uniform distribution. II*, Indag. Math. **10** (1948), 406–413.

[11] FAURE, H.: *Discrépances de suites associées à un système de numération*, Bull. Soc. Math. France **109** (1981), no. 2, 143–182.

[12] HABER, S.: *On a sequence of points of interest for numerical quadrature*, J. Res. Nat. Bur. Standards Sect. B **70B** (1966), 127–136.

[13] HEATH-BROWN, D.R.: *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38.

[14] HLAWKA, E.: *Funktionen von beschränkter Variation in der Theorie der Gleichverteilung*, Ann. Mat. Pura Appl. (4) **54** (1961), 325–333.

[15] HLAWKA, E.: *Zur angenäherten Berechnung mehrfacher Integrale*, Monatsh. Math. **66** (1962), 140–151.

[16] KOKSMA, J.F.: *A general theorem from the theory of uniform distribution modulo 1* (Dutch), Mathematica, Zutphen. B. **11** (1942), 7–11.

[17] KOKSMA, J.F.: *Some theorems on Diophantine inequalities*, Scriptum no. **5**, Math. Centrum Amsterdam, 1950, 51 pp.
[18] KOROBOV, N. M.: *Approximate calculation of repeated integrals by number-theoretical methods* (Russian), Dokl. Akad. Nauk SSSR (N.S.) **115** (1957), 1062–1065.
[19] KUIPERS, L.– NIEDERREITER, H.: *Uniform Distribution of Sequences*, Pure and Applied Mathematics, Wiley-Interscience, New York, 1974.
[20] LAMBERT, J.P.: *Quasi-random sequences in numerical practice*, Numerical Mathematics (Singapore 1988), Internat. Schriftenreihe Numer. Math. **86**, Birkhäuser, Basel, 1988, pp. 273–284.
[21] LEVEQUE, W.J.: *An inequality connected with Weyl's criterion for uniform distribution*, Proc. Sympos. Pure Math. Vol. **VIII**, Amer. Math. Soc., Providence, R.I., 1965, pp. 22–30.
[22] NIEDERREITER, H.: *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, PA, 1992.
[23] NIEDERREITER, H. – PHILIPP, W.: *Berry-Esseen bounds and a theorem of Erdős and Turán on uniform distribution* mod 1, Duke Math. J. **40** (1973), 633–649.
[24] ROTH, K.F.: *On irregularities of distribution*, Mathematika **1** (1954), 73–79.
[25] SCHMIDT, W.M.: *Diophantine Approximation*, Lecture Notes in Math. No. **785**, Springer-Verlag, 1980.
[26] STRAUCH, O. – PAŠTÉKA, M. – GREKOS, G.: *Kloosterman's uniformly distributed sequence*, J. Number Theory **103** (2003), no. 1, 1–15.

Received April 27, 2006
Revised March 20, 2007
Accepted

William Banks
Department of Mathematics
University of Missouri
Columbia, MO 65211
USA
E-mail: bbanks@math.missouri.edu

Filip Saidak
Department of Mathematics
University of North Carolina
Greensboro, NC 27403
USA
E-mail: f_saidak@uncg.edu

Mayumi Sakata
Department of Mathematics
William Jewell College
Liberty, MO 64068
USA
E-mail: sakatam@william.jewell.edu