#A47 INTEGERS 12 (2012)

A REVERSE ORDER PROPERTY OF CORRELATION MEASURES OF THE SUM-OF-DIGITS FUNCTION

Johannes F. Morgenbesser[1]
Universität Wien, Fakultät für Mathematik, Wien, Austria
johannes.morgenbesser@univie.ac.at

Lukas Spiegelhofer[2]
Institut für Diskrete Mathematik und Geometrie, Technische Universität Wien, Wien, Austria
lukas.spiegelhofer@tuwien.ac.at

Received: 1/9/12, Accepted: 7/7/12, Published: 9/3/12

Abstract

Let s_q be the sum-of-digits function in base q, $q \geqslant 2$. If t is a positive integer, we denote by t^R the unique integer that is obtained from t by reversing the order of the digits of the proper representation of t in base q. In this work we prove that for all $\alpha \in \mathbb{R}$ and all positive integers t the correlation measure

$$\gamma(\alpha, t) = \lim_{x \to \infty} \frac{1}{x} \sum_{n<x} e^{2\pi i \alpha (s_q(n+t) - s_q(n))}$$

satisfies $\gamma(\alpha, t) = \gamma(\alpha, t^R)$. From this we deduce that for all integers d the sets $\{n \in \mathbb{N} : s_q(n+t) - s_q(n) = d\}$ and $\{n \in \mathbb{N} : s_q(n+t^R) - s_q(n) = d\}$ have the same asymptotic density. The proof involves methods coming from the study of q-additive functions, linear algebra, and analytic number theory.

1. Introduction and Main Results

Throughout this work, q is a fixed positive integer $\geqslant 2$. For a real number x, the expression $\mathrm{e}(x)$ denotes $e^{2\pi i x}$. Every integer $n > 0$ has a unique representation in base q of the form

$$n = \sum_{j=0}^{\nu} \varepsilon_j(n) q^j, \qquad \varepsilon_j(n) \in \{0, \ldots, q-1\},$$

with $\varepsilon_\nu(n) \neq 0$. We set $\varepsilon_j(n) = 0$ for $j > \nu$. The sum-of-digits function $s_q(n)$ in base q is defined by $s_q(n) = \sum_{j \geqslant 0} \varepsilon_j(n)$. If $\ell \geqslant \nu$, we write $n = (\varepsilon_\ell(n)\varepsilon_{\ell-1}(n) \ldots \varepsilon_0(n))_q$.

[1]The author was supported by the Austrian Science Foundation FWF, grant P21209.

[2]The author was supported by the Austrian Science Foundation FWF, grant S9604, which is part of the National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

In the case that $\ell = \nu$ (that is, $\varepsilon_\ell(n) \neq 0$), this is called the proper representation of n. If $t = (\varepsilon_\nu(t)\varepsilon_{\nu-1}(t)\dots\varepsilon_0(t))_q$ with $\varepsilon_\nu(t) \neq 0$, we set

$$t^R = (\varepsilon_0(t)\dots\varepsilon_\nu(t))_q,$$

that is, t^R is obtained from t by reversing the order of the digits in base q. Moreover, we set $0^R = 0$. Note that palindromes (in base q) are exactly those integers that satisfy $t = t^R$. Note furthermore that the function $t \mapsto t^R$ restricted to positive integers not congruent to 0 modulo q is bijective. In particular, if $t = q^k \cdot \hat{t}$ with $(\hat{t}, q) = 1$ and $k \geqslant 0$, then we have $t^{RR} = \hat{t}$. For $t \geqslant 0$ we set

$$\gamma(\alpha, t) = \lim_{x\to\infty} \frac{1}{x} \sum_{n<x} \mathrm{e}(\alpha(s_q(n+t) - s_q(n))).$$

In the case that $\alpha = 1/2$ and $q = 2$ it was proven by Mahler [7] that the limits actually exist and that $\gamma(1/2, t) \neq 0$ for infinitely many t. For general α and $q \geqslant 2$ it follows from [1] that the limits exist for all $t \geqslant 0$. Interestingly, $\gamma(1/2, t)$ is equal to the t-th Fourier coefficient of the correlation measure associated to the Thue-Morse dynamical system (see [6]). Our main result deals with these correlation measures for an integer t and its associated integer t^R. Even though there seems to be no simple relation between $s_q(n+t)$ and $s_q(n+t^R)$, we have the following result:

Theorem 1. *Let $q \geqslant 2$, $\alpha \in \mathbb{R}$ and $t \geqslant 0$. Then we have $\gamma(\alpha, t) = \gamma(\alpha, t^R)$.*

This theorem implies that the set of positive integers n such that $s_q(n+t) - s_q(n)$ is a fixed integer d satisfies a similar property. For $d \in \mathbb{Z}$ and $t \geqslant 0$ let $\delta(d, t)$ be the asymptotic density of the set $\{n \in \mathbb{N} : s_q(n+t) - s_q(n) = d\}$, that is,

$$\delta(d, t) = \lim_{x\to\infty} \frac{1}{x} \#\{n < x : s_q(n+t) - s_q(n) = d\}.$$

(The existence of the limit follows from [1, Lemma 1], which tells us that the set $\{n \in \mathbb{N} : s_q(n+t) - s_q(n) = d\}$ is a union of arithmetic progressions.)

Corollary 2. *Let $q \geqslant 2$, $d \in \mathbb{Z}$ and $t \geqslant 0$. Then we have $\delta(d, t) = \delta(d, t^R)$.*

Our research was motivated by a question of Thomas W. Cusick [2]: Let c_t be defined for $t \geqslant 0$ by

$$c_t = \lim_{x\to\infty} \frac{1}{x} \#\{n < x : s_q(n+t) \geqslant s_q(n)\}.$$

He asked whether it is true that $c_t > 1/2$ for all integers $t \geqslant 0$. This question arose while he was working on a combinatorial problem proposed by Tu and Deng [8] that is strongly related to Boolean functions with optimal cryptographic properties. In [3] some cases of this conjecture have been proved, and there are several other recent papers dealing with this subject, see for example [5, 4]). Although we could not answer Cusick's original question, Theorem 1 implies the following interesting result:

Corollary 3. *Let $q \geqslant 2$ and $t \geqslant 0$. Then we have $c_t = c_{t^R}$.*

2. Proof of Theorem 1

Bésineau [1, Section II.6] showed that the quantities $\gamma(\alpha, t)$ satisfy the following recurrence relation: We have $\gamma(\alpha, 0) = 1$ and

$$\gamma(\alpha, qt + k) = \frac{q-k}{q}\,\mathrm{e}(\alpha k)\gamma(\alpha, t) + \frac{k}{q}\,\mathrm{e}(-\alpha(q-k))\gamma(\alpha, t+1)$$

for $t \geqslant 0$ and $0 \leqslant k < q$. In particular, we have $\gamma(\alpha, qt) = \gamma(\alpha, t)$ and $u := \gamma(\alpha, 1) = (q-1)/(q\,\mathrm{e}(-\alpha) - \mathrm{e}(-\alpha q))$. It is not difficult to see that $\gamma(\alpha, t)$ can be explicitly computed with the help of transition matrices. Set

$$A(k) = \begin{pmatrix} \frac{q-k}{q}\,\mathrm{e}(\alpha k) & \frac{k}{q}\,\mathrm{e}(-\alpha(q-k)) \\ \frac{q-k-1}{q}\,\mathrm{e}(\alpha(k+1)) & \frac{k+1}{q}\,\mathrm{e}(-\alpha(q-k-1)) \end{pmatrix}.$$

Then we have

$$\gamma(\alpha, t) = (1\,,0)\,A(\varepsilon_0(t)) \cdots A(\varepsilon_\nu(t)) \begin{pmatrix} 1 \\ u \end{pmatrix}. \tag{1}$$

Note that it is not important whether the proper representation of t is used in order to calculate $\gamma(\alpha, t)$. Indeed, this follows from the fact that $(1\,, u)^T$ is a right eigenvector of $A(0)$ to the eigenvalue 1. Note furthermore that $\gamma(\alpha, qt) = \gamma(\alpha, t)$ corresponds to the fact that $(1\,,0)$ is a left eigenvector of $A(0)$ to the eigenvalue 1. Set

$$S = \begin{pmatrix} 1 & \bar{u} \\ 0 & 1 \end{pmatrix}.$$

Proposition 4. *Let $\ell \geqslant 0$ and $(\varepsilon_0, \ldots, \varepsilon_\ell) \in \{0, \ldots, q-1\}^{\ell+1}$. Then we have*

$$(1\,,0)\,S^{-1}A(\varepsilon_0) \cdots A(\varepsilon_\ell) \begin{pmatrix} 1 \\ u \end{pmatrix} = (1\,,0)\,A(\varepsilon_\ell) \cdots A(\varepsilon_0) S \begin{pmatrix} 1-|u|^2 \\ 0 \end{pmatrix} \tag{2}$$

and

$$(0\,,\bar{u})\,S^{-1}A(\varepsilon_0) \cdots A(\varepsilon_\ell) \begin{pmatrix} 1 \\ u \end{pmatrix} = (1\,,0)\,A(\varepsilon_\ell) \cdots A(\varepsilon_0) S \begin{pmatrix} 0 \\ u \end{pmatrix}. \tag{3}$$

This proposition immediately implies Theorem 1. Indeed, if we sum up (2) and (3) we obtain

$$(1\,,\bar{u})\,S^{-1}A(\varepsilon_0) \cdots A(\varepsilon_\ell) \begin{pmatrix} 1 \\ u \end{pmatrix} = (1\,,0)\,A(\varepsilon_\ell) \cdots A(\varepsilon_0) S \begin{pmatrix} 1-|u|^2 \\ u \end{pmatrix}.$$

Since $(1\,,\bar{u})S^{-1} = (1\,,0)$ and $S(1-|u|^2\,, u)^T = (1\,,u)^T$, relation (1) implies that $\gamma(\alpha, t) = \gamma(\alpha, t^R)$.

Proof of Proposition 4. We will show this result by induction on ℓ. For notational convenience we set

$$A(\varepsilon) = \begin{pmatrix} a_1(\varepsilon) & a_2(\varepsilon) \\ a_3(\varepsilon) & a_4(\varepsilon) \end{pmatrix} \qquad \text{and} \qquad S^{-1}A(\varepsilon)S = \begin{pmatrix} s_1(\varepsilon) & s_2(\varepsilon) \\ s_3(\varepsilon) & s_4(\varepsilon) \end{pmatrix}.$$

Throughout the proof, we will use (at several places) the relation

$$a_1(\varepsilon)|u|^2 + a_2(\varepsilon)u = a_3(\varepsilon)\bar{u} + a_4(\varepsilon)|u|^2 \tag{4}$$

which holds for $0 \leqslant \varepsilon < q$. The validity of (4) is easily seen by multiplying both sides by $|u|^{-2}$ and evaluating them: This gives

$$\frac{\mathrm{e}(\alpha\varepsilon)}{q-1}\left(q - \varepsilon - 1 + \varepsilon\,\mathrm{e}(-\alpha(q-1))\right)$$

on the left hand side as well as on the right hand side. If $\ell = 0$ we have to show that

$$(1\,,0)\,S^{-1}A(\varepsilon_0)\begin{pmatrix} 1 \\ u \end{pmatrix} = (1\,,0)\,A(\varepsilon_0)S\begin{pmatrix} 1-|u|^2 \\ 0 \end{pmatrix} \tag{5}$$

and

$$(0\,,\bar{u})\,S^{-1}A(\varepsilon_0)\begin{pmatrix} 1 \\ u \end{pmatrix} = (1\,,0)\,A(\varepsilon_0)S\begin{pmatrix} 0 \\ u \end{pmatrix}. \tag{6}$$

Equation (5) is satisfied if $a_1(\varepsilon_0)+a_2(\varepsilon_0)u-a_3(\varepsilon_0)\bar{u}-a_4(\varepsilon_0)|u|^2 = a_1(\varepsilon_0)(1-|u|^2)$. Using (4), we see that this holds true indeed. Equation (6) is also equivalent to (4) and we are done. Assume now that $\ell \geqslant 1$. Set

$$\begin{pmatrix} \mathfrak{a} \\ \mathfrak{b} \end{pmatrix} = S^{-1}A(\varepsilon_1)\ldots A(\varepsilon_\ell)\begin{pmatrix} 1 \\ u \end{pmatrix} \qquad \text{and} \qquad (\mathfrak{a}'\,,\mathfrak{b}') = (1\,,0)A(\varepsilon_\ell)\cdots A(\varepsilon_1)S.$$

The induction hypothesis implies that

$$\mathfrak{a} = \mathfrak{a}'(1-|u|^2) \qquad \text{and} \qquad \mathfrak{b}\bar{u} = \mathfrak{b}'u. \tag{7}$$

In order to prove (2), we have to show that

$$(1,\,0)S^{-1}A(\varepsilon_0)S\begin{pmatrix} \mathfrak{a} \\ \mathfrak{b} \end{pmatrix} = (\mathfrak{a}'\,,\mathfrak{b}')S^{-1}A(\varepsilon_0)S\begin{pmatrix} 1-|u|^2 \\ 0 \end{pmatrix}. \tag{8}$$

This is equivalent to $s_1(\varepsilon_0)\mathfrak{a} + s_2(\varepsilon_0)\mathfrak{b} = s_1(\varepsilon_0)(1-|u|^2)\mathfrak{a}' + s_3(\varepsilon_0)(1-|u|^2)\mathfrak{b}'$. Using (7), we see that this holds true if $s_2(\varepsilon_0)u/\bar{u} = s_3(\varepsilon_0)(1-|u|^2)$. Note that $s_2(\varepsilon_0)$ and $s_3(\varepsilon_0)$ are given by $s_2(\varepsilon_0) = a_1(\varepsilon_0)\bar{u} + a_2(\varepsilon_0) - \bar{u}^2a_3(\varepsilon_0) - \bar{u}a_4(\varepsilon_0)$ and $s_3(\varepsilon_0) = a_3(\varepsilon_0)$. Using these relations and (4), we see that (8) holds true. The validity of (3) can be shown the same way. This finally proves Proposition 4. □

3. Proof of Corollary 2 and Corollary 3

Proof of Corollary 2. Using the dominated convergence theorem, we see that

$$\begin{aligned}\delta(d,t) &= \lim_{x\to\infty}\frac{1}{x}\#\{n<x : s_q(n+t)-s_q(n)=d\}\\ &= \lim_{x\to\infty}\frac{1}{x}\sum_{n<x}\int_0^1 \mathrm{e}(\alpha(s_q(n+t)-s_q(n)-d))\mathrm{d}\alpha\\ &= \int_0^1 \lim_{x\to\infty}\sum_{n<x}\frac{1}{x}\,\mathrm{e}(\alpha(s_q(n+t)-s_q(n)-d))\mathrm{d}\alpha.\end{aligned}$$

Thus we have $\delta(d,t) = \int_0^1 \gamma(\alpha,t)\,\mathrm{e}(-\alpha d)\mathrm{d}\alpha$. By Theorem 1 we have $\gamma(\alpha,t) = \gamma(\alpha,t^R)$ and we get $\delta(d,t)=\delta(d,t^R)$. □

Proof of Corollary 3. The sub-additivity of $s_q(n)$ implies $s_q(n+t)-s_q(n)\leqslant s_q(t)$. Therefore we have $c_t=\sum_{k=0}^{s_q(t)}\delta(k,t)$. Since $s_q(t)=s_q(t^R)$, we are done. □

References

[1] J. Bésineau, Indépendance statistique d'ensembles liés à la fonction "somme des chiffres", *Acta Arith.* **20** (1972), 401–416.

[2] T. W. Cusick, private communication (2012).

[3] T. W. Cusick, Y. Li, and P. Stănică, On a combinatorial conjecture, *Integers* **11** A17 (2011), 185–203.

[4] J.-P. Flori, H. Randriam, On the Number of Carries Occuring in an Addition mod 2^k-1, *Integers* **12** A10 (2012), 42pp.

[5] J.-P. Flori, H. Randriambololona, G. Cohen, and S. Mesnager, On a Conjecture about Binary Strings Distribution, *Sequences and Their Applications - SETA 2010 Springer Berlin/Heidelberg (Ed.)*, (2010), 346–358.

[6] M. Keane, Generalized Morse sequences, *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **10** (1968), 335–353.

[7] K. Mahler, The spectrum of an array and its application to the study of the translation properties of a simple class of arithmetical functions II. On the translation properties of a simple class of arithmetical functions, *J. Math. and Physics* **6** (1927), 158–163.

[8] Z. Tu and Y. Deng, A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity, *Des. Codes Cryptogr.* **60** no. 1, 1–14.