On the Digits of Squares and the Distribution of Quadratic Subsequences of Digital Sequences[1]

Heidrun Zellinger[2]

Institute for Financial Mathematics, University of Linz, Austria

June 25, 2012

UDT2012, Smolenice, Slovakia

[1]joint work with R. Hofer and G. Larcher

[2]Recipient of a DOC-fFORTE-fellowship of the Austrian Academy of Science

Contents

Basic definitions

Definition

Let $m = m_0 + m_1 q + \cdots + m_r q^r$ be the q-adic representation of an integer m and let $\gamma = (\gamma_0, \gamma_1, \dots) \in \mathbb{Z}_q^{\mathbb{N}_0}$ with $\gamma_i \in \{0, 1, \dots, q-1\}$ be a weight sequence, then the *weighted sum-of-digits function of m* is given by

$$s_{q,\gamma}(m) := \gamma_0 m_0 + \gamma_1 m_1 + \cdots + \gamma_r m_r.$$

We have analyzed distribution properties of $s_{q,\gamma}(n^2)$ in prime bases q for finite weight sequences.

Basic definitions

Definition

For prime bases q, digits $d \in \{0, 1, \ldots, q-1\}$ and nonnegative integers n and N we define

$$T_{\gamma,d,q} := \lim_{N\to\infty} T_{\gamma,d,q}(N), \text{ where}$$
$$T_{\gamma,d,q}(N) := \frac{1}{N} \cdot \# \left\{0 \leq n < N | s_{q,\gamma}(n^2) \equiv d \pmod{q}\right\}$$

for finite weight sequences $\gamma = (\gamma_0, \gamma_1, \ldots, \gamma_{l-1}, 0, 0, \ldots)$ with $\gamma_i \in \{0, 1, \ldots, q-1\}$ and $\gamma_{l-1} \neq 0$. ($l \in \mathbb{N}$ is the minimal index such that $\gamma_i = 0$ for all $i \geq l$.)

Question: For which γ, d and q is the distribution of $T_{\gamma,d,q}$ fair in the sense that $T_{\gamma,d,q} = 1/q$?

Formulas for $T_{\gamma,d,q}$ - Basic tools

Basic tools: Quadratic residues a and the number of solutions of $x^2 \equiv a \pmod{2^l}$ and $x^2 \equiv a \pmod{q^l}$ for odd primes q.

Lemma

Let L be the number of solutions of $x^2 \equiv a \pmod{2^l}$ with $x \in \{0, 1, \dots, 2^l - 1\}$.

(1) *If l is even, then*

$$\begin{aligned} L &= 2^{\frac{l}{2}} && \text{for } a = 0, \\ L &= 2^{\frac{l}{2}} && \text{for } a = 2^{l-2}, \\ L &= 2^{v+2} && \text{for } a = 2^{2v} \cdot b \text{ with} \\ & && b \equiv 1 \pmod 8 \text{ and} \\ & && v \in \{0, \dots, (l-4)/2\}, \\ L &= 0 && \text{otherwise.} \end{aligned}$$

(2) *If l is odd, then*

$$\begin{aligned} L &= 2^{\frac{l-1}{2}} && \text{for } a = 0, \\ L &= 2^{\frac{l-1}{2}} && \text{for } a = 2^{l-1}, \\ L &= 2^{v+2} && \text{for } a = 2^{2v} \cdot b \text{ with} \\ & && b \equiv 1 \pmod 8 \text{ and} \\ & && v \in \{0, \dots, (l-3)/2\}, \\ L &= 0 && \text{otherwise.} \end{aligned}$$

Formulas for $T_{\gamma,d,q}$ - Basic tools

Lemma

Let q be an odd prime and let $C := \left\{c_1, \ldots, c_{(q-1)/2}\right\}$ be the set of the c_k with $0 < c_k < q$ and $c_k^{(q-1)/2} \equiv 1 \pmod q$.
Let L be the number of solutions of $x^2 \equiv a \pmod{q^l}$ with $x \in \{0, 1, \ldots, q^l - 1\}$. Then

$$
\begin{aligned}
L &= q^{\lfloor \frac{l}{2} \rfloor} && \text{for } a = 0,\\
L &= 2q^i && \text{for } a = q^{2i}(c + qw),\\
& && \text{with } c \in C,\\
& && i \in \{0, 1, \ldots, \lfloor (l+1)/2 \rfloor - 1\},\\
& && \text{and } w \in \mathbb{N}_0 \text{ such that } a < q^l,\\
L &= 0 && \text{otherwise.}
\end{aligned}
$$

Formulas for $T_{\gamma,d,q}$ - Idea of the proof

With the two lemmas we can derive formulas for

$$T_{\gamma,d,q} := \lim_{N\to\infty} \underbrace{\frac{1}{N} \cdot \#\left\{0 \le n < N | s_{q,\gamma}(n^2) \equiv d \pmod q\right\}}_{T_{\gamma,d,q}(N)}$$

Idea of the proof:

- For $n \equiv m \pmod{q^l}$ we have $s_{q,\gamma}(n^2) = s_{q,\gamma}(m^2)$, and

  $$\left\lfloor \frac{N}{q^l} \right\rfloor \cdot q^l \cdot T_{\gamma,d,q}(q^l) \le N \cdot T_{\gamma,d,q}(N) \le \left(\left\lfloor \frac{N}{q^l} \right\rfloor + 1 \right) \cdot q^l \cdot T_{\gamma,d,q}(q^l).$$

  Therefore $T_{\gamma,d,q} = T_{\gamma,d,q}(q^l)$.

- Compute $T_{\gamma,d,q}(q^l)$ by identifying those quadratic residues a of the congruences from the lemmas, which are elements of the set

  $$A_{\gamma,d,q,l} := \{0 \le a < q^l | s_{q,\gamma}(a) \equiv d \pmod q\}.$$

Formulas for $T_{\gamma,d,q}$

Theorem

If $q = 2$, *then*

for l *even*
$$T_{\gamma,0,2} = \begin{cases} \frac{1}{2} & \text{if } \gamma_{l-2} = 1, \\ \frac{1}{2} + 2^{-\frac{l}{2}} & \text{if } \gamma_{l-2} = 0, \end{cases}$$

for l *odd*
$$T_{\gamma,0,2} = \begin{cases} \frac{1}{2} & \text{if } l = 1, \\ \frac{1}{2} - 2^{-\frac{l+1}{2}} & \text{if } l \geq 3 \text{ and } \gamma_{l-3} = 1, \\ \frac{1}{2} + 2^{-\frac{l+1}{2}} & \text{if } l \geq 3 \text{ and } \gamma_{l-3} = 0. \end{cases}$$

If $q \geq 3$ *prime, then*

for l *even*
$$T_{\gamma,d,q} = \frac{1}{q} - q^{-\frac{l}{2}-1} + \begin{cases} q^{-\frac{l}{2}} & \text{if } d = 0, \\ 0 & \text{else}, \end{cases}$$

for l *odd*
$$T_{\gamma,d,q} = \begin{cases} \frac{1}{q} & \text{if } d = 0, \\ \frac{1}{q} + q^{-\frac{1+l}{2}} & \text{if } d \in C, \\ \frac{1}{q} - q^{-\frac{1+l}{2}} & \text{else}. \end{cases}$$

Admissible weight sequences

Definition

We call a weight sequence $\gamma \in \mathbb{Z}_q^{\mathbb{N}_0}$ *admissible* for $\left(n^2\right)_{n\geq 0}$ if

$$T_{\gamma,d,q} = 1/q$$

for all $d \in \{0, 1, \dots, q-1\}$.

Corollary

The finite weight sequence $\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{l-1}, 0, 0, \dots)$ *with* $\gamma_{l-1} \neq 0$ *is admissible for* $(n^2)_{n\geq 0}$ *if and only if* $q = 2$*,* l *even and* $\gamma_{l-2} = \gamma_{l-1} = 1$ *or if* $q = 2$*,* $\gamma_0 = 1$ *and* $\gamma_i = 0$ *for* $i \geq 1$*.*

Example (Admissible finite weight sequences for $(n^2)_{n\geq 0}$ in base 2)

$$\gamma = (\mathbf{1}, 0, 0, \dots),\ \gamma = (\mathbf{1}, \mathbf{1}, 0, \dots),\ \gamma = (0, 0, \mathbf{1}, \mathbf{1}, 0, \dots),$$
$$\gamma = (1, 1, \mathbf{1}, \mathbf{1}, 0,),\ \gamma = (1, 0, 1, 0, \mathbf{1}, \mathbf{1}, 0, \dots)$$

Construction of digital $(\boldsymbol{T}, s)$-sequences $(\boldsymbol{x}_n)_{n\geq 0}$ over $\mathbb{Z}_q$ generated by matrices with finite rows

- Choose s $\mathbb{N}_0 \times \mathbb{N}_0$-matrices $C^{(1)}, \ldots, C^{(s)}$ over $\mathbb{Z}_q$, q prime, with finite rows exclusively.
- To generate the ith coordinate $x_n^{(i)}$ of $\boldsymbol{x}_n$, represent the integer n in base q

$$n = n_0 + n_1 q + \cdots + n_r q^r.$$

- Set

$$\boldsymbol{n} := (n_0, \ldots, n_r, 0, 0, \ldots)^T$$

and

$$C^{(i)} \cdot \boldsymbol{n} =: \boldsymbol{y}^{(i)} = (y_0^{(i)}, y_1^{(i)}, \ldots)^T.$$

- Then

$$x_n^{(i)} := \frac{y_0^{(i)}}{q} + \frac{y_1^{(i)}}{q^2} + \ldots .$$

Classification of u.d. subsequences $(\boldsymbol{x}_{n^2})_{n\geq 0}$

Theorem

Let $(\boldsymbol{x}_n)_{n\geq 0}$ be a digital $(\boldsymbol{T}, s)$-sequence over $\mathbb{Z}_q$, q prime, generated by the matrices $C^{(1)}, \ldots, C^{(s)}$. Then the sequence $(\boldsymbol{x}_{n^2})_{n\geq 0}$ is uniformly distributed if and only if every nontrivial linear combination of any finite set of rows of $C^{(1)}, \ldots, C^{(s)}$ over $\mathbb{Z}_q$ is admissible for $(n^2)_{n\geq 0}$.

Remark

Note that this result is valid for arbitrary $C^{(1)}, \ldots, C^{(s)}$ and not only for matrices with finite rows exclusively.

Examples of generating matrices

Example

The subsequence $(\boldsymbol{x}_{n^2})_{n\geq 0}$ of the digital $(0,1)$-sequence over $\mathbb{Z}_2$ generated by

$$C^{(1)} = \begin{pmatrix} 1&1&0&0&0&0&0&0&0&0&\dots \\ 0&1&1&1&0&0&0&0&0&0&\dots \\ 0&0&1&1&1&1&0&0&0&0&\dots \\ 0&0&0&1&1&1&1&1&0&0&\dots \\ &&&&&&\ddots&&&& \end{pmatrix}$$

is for example uniformly distributed.

Example

The subsequence $(\boldsymbol{x}_{n^2})_{n\geq 0}$ of the digital $(\boldsymbol{T},2)$-sequence over $\mathbb{Z}_2$ generated by

$$C^{(1)} = \begin{pmatrix} 1&1&0&0&0&0&0&0&0&0&\dots \\ 0&0&0&0&1&1&0&0&0&0&\dots \\ 0&0&0&0&0&0&0&0&1&1&\dots \\ &&&&&\ddots&&&&& \end{pmatrix} \text{ and } C^{(2)} = \begin{pmatrix} 0&0&1&1&0&0&0&0&0&0&0&0&\dots \\ 0&0&0&0&0&0&1&1&0&0&0&0&\dots \\ 0&0&0&0&0&0&0&0&0&0&1&1&\dots \\ &&&&&&\ddots&&&&&& \end{pmatrix}$$

is for example uniformly distributed.