The Rudin-Shapiro sequence and similar sequences are normal along squares

Clemens Müllner

Tuesday, October 2nd, 2018

Sum of digits

Let $q \geq 2$ be a base.

$$n = \sum_{j=0}^{r} \varepsilon_j^{(q)}(n) q^j,$$

where $\varepsilon_j^{(q)}(n) \in \{0, \ldots, q-1\}$ and $r = \lfloor \log_q(n) \rfloor$.

Definition

We define the sum of digits function $s_q(n)$

$$s_q(n) := \sum_{j=0}^{r} \varepsilon_j^{(q)}(n).$$

Sum of digits

Let $q \geq 2$ be a base.

$$n = \sum_{j=0}^{r} \varepsilon_j^{(q)}(n) q^j,$$

where $\varepsilon_j^{(q)}(n) \in \{0, \ldots, q-1\}$ and $r = \lfloor \log_q(n) \rfloor$.

Definition

We define the sum of digits function $s_q(n)$

$$s_q(n) := \sum_{j=0}^{r} \varepsilon_j^{(q)}(n).$$

Sum of digits

Let $q \geq 2$ be a base.

$$n = \sum_{j=0}^{r} \varepsilon_j^{(q)}(n) q^j,$$

where $\varepsilon_j^{(q)}(n) \in \{0, \ldots, q-1\}$ and $r = \lfloor \log_q(n) \rfloor$.

Definition

We define the sum of digits function $s_q(n)$

$$s_q(n) := \sum_{j=0}^{r} \varepsilon_j^{(q)}(n).$$

Gelfond

Let $q \geq 2$ and m such that $\gcd(q-1, m) = 1$.

Theorem (Gelfond 1967)

$(s_q(an+b) \bmod m)_{n\in\mathbb{N}}$ is simply normal.

2. Gelfond Problem

$(s_q(p) \bmod m)_{p\in\mathcal{P}}$ is simply normal.
Solved by Mauduit and Rivat in 2010.

3. Gelfond Problem

Let $P(x)$ be a polynomial with integer coefficients.
Then $(s_q(P(n)) \bmod m)_{n\in\mathbb{N}}$ is simply normal.
Solved by Mauduit and Rivat in 2009 for $P(n) = n^2$.
Drmota, Mauduit and Rivat (2018): $(s_2(n^2) \bmod 2)_{n\in\mathbb{N}}$ is normal!

Gelfond

Let $q \geq 2$ and m such that $\gcd(q-1, m) = 1$.

Theorem (Gelfond 1967)

$(s_q(an+b) \bmod m)_{n\in\mathbb{N}}$ is simply normal.

2. Gelfond Problem

$(s_q(p) \bmod m)_{p\in\mathcal{P}}$ is simply normal.

Solved by Mauduit and Rivat in 2010.

3. Gelfond Problem

Let $P(x)$ be a polynomial with integer coefficients.
Then $(s_q(P(n)) \bmod m)_{n\in\mathbb{N}}$ is simply normal.

Solved by Mauduit and Rivat in 2009 for $P(n) = n^2$.

Drmota, Mauduit and Rivat (2018): $(s_2(n^2) \bmod 2)_{n\in\mathbb{N}}$ is normal!

Gelfond

Let $q \geq 2$ and m such that $\gcd(q-1, m) = 1$.

Theorem (Gelfond 1967)

$(s_q(an+b) \bmod m)_{n\in\mathbb{N}}$ is simply normal.

2. Gelfond Problem

$(s_q(p) \bmod m)_{p\in\mathcal{P}}$ is simply normal.
Solved by Mauduit and Rivat in 2010.

3. Gelfond Problem

Let $P(x)$ be a polynomial with integer coefficients.
Then $(s_q(P(n)) \bmod m)_{n\in\mathbb{N}}$ is simply normal.
Solved by Mauduit and Rivat in 2009 for $P(n) = n^2$.
Drmota, Mauduit and Rivat (2018): $(s_2(n^2) \bmod 2)_{n\in\mathbb{N}}$ *is normal!*

Gelfond

Let $q \geq 2$ and m such that $\gcd(q-1, m) = 1$.

Theorem (Gelfond 1967)

$(s_q(an+b) \bmod m)_{n \in \mathbb{N}}$ is simply normal.

2. Gelfond Problem

$(s_q(p) \bmod m)_{p \in \mathcal{P}}$ is simply normal.
Solved by Mauduit and Rivat in 2010.

3. Gelfond Problem

Let $P(x)$ be a polynomial with integer coefficients.
Then $(s_q(P(n)) \bmod m)_{n \in \mathbb{N}}$ is simply normal.
Solved by Mauduit and Rivat in 2009 for $P(n) = n^2$.
Drmota, Mauduit and Rivat (2018): $(s_2(n^2) \bmod 2)_{n \in \mathbb{N}}$ is normal!

Gelfond

Let $q \geq 2$ and m such that $\gcd(q-1, m) = 1$.

Theorem (Gelfond 1967)

$(s_q(an+b) \bmod m)_{n\in\mathbb{N}}$ is simply normal.

2. Gelfond Problem

$(s_q(p) \bmod m)_{p\in\mathcal{P}}$ is simply normal.
Solved by Mauduit and Rivat in 2010.

3. Gelfond Problem

Let $P(x)$ be a polynomial with integer coefficients.
Then $(s_q(P(n)) \bmod m)_{n\in\mathbb{N}}$ is simply normal.
Solved by Mauduit and Rivat in 2009 for $P(n) = n^2$.
Drmota, Mauduit and Rivat (2018): $(s_2(n^2) \bmod 2)_{n\in\mathbb{N}}$ is normal!

Gelfond

Let $q \geq 2$ and m such that $\gcd(q-1, m) = 1$.

Theorem (Gelfond 1967)

$(s_q(an+b) \bmod m)_{n \in \mathbb{N}}$ is simply normal.

2. Gelfond Problem

$(s_q(p) \bmod m)_{p \in \mathcal{P}}$ is simply normal.
Solved by Mauduit and Rivat in 2010.

3. Gelfond Problem

Let $P(x)$ be a polynomial with integer coefficients.
Then $(s_q(P(n)) \bmod m)_{n \in \mathbb{N}}$ is simply normal.
Solved by Mauduit and Rivat in 2009 for $P(n) = n^2$.
Drmota, Mauduit and Rivat (2018): $(s_2(n^2) \bmod 2)_{n \in \mathbb{N}}$ is normal!

Pattern-counting function

Definition (Pattern-counting function)

Fix $\ell \geq 1$ and a pattern
$P = (p_0, \dots, p_{\ell-1}) \in \{0, \dots, q-1\}^{\ell}$, $P \neq (0, \dots, 0)$.
Then we define the *pattern-counting function*

$$f_P(n) = \sum_{j=0}^{r-\ell+1} \mathbf{1}_{[(\varepsilon_{j+\ell-1}^{(q)}(n), \dots, \varepsilon_j^{(q)}(n)) = P]}.$$

Rudin-Shapiro: $(f_{11}(n) \bmod 2)_{n \in \mathbb{N}}$.

Pattern-counting function

Definition (Pattern-counting function)

Fix $\ell \geq 1$ and a pattern
$P = (p_0, \ldots, p_{\ell-1}) \in \{0, \ldots, q-1\}^{\ell}, P \neq (0, \ldots, 0)$.
Then we define the *pattern-counting function*

$$f_P(n) = \sum_{j=0}^{r-\ell+1} \mathbf{1}_{[(\varepsilon_{j+\ell-1}^{(q)}(n), \ldots, \varepsilon_j^{(q)}(n)) = P]}.$$

Rudin-Shapiro: $(f_{11}(n) \bmod 2)_{n \in \mathbb{N}}$.

Pattern-counting function

Definition (Pattern-counting function)

Fix $\ell \geq 1$ and a pattern
$P = (p_0, \ldots, p_{\ell-1}) \in \{0, \ldots, q-1\}^\ell, P \neq (0, \ldots, 0)$.
Then we define the *pattern-counting function*

$$f_P(n) = \sum_{j=0}^{r-\ell+1} \mathbf{1}_{[(\varepsilon_{j+\ell-1}^{(q)}(n), \ldots, \varepsilon_j^{(q)}(n))=P]}.$$

Rudin-Shapiro: $(f_{11}(n) \bmod 2)_{n \in \mathbb{N}}$.

Block-additive function

Definition (Block-additive function)

We say that $b : \mathbb{N} \to \mathbb{Z}$ is *block-additive / digital* if there exists $\ell \geq 1$ and $F : \{0, \ldots, q-1\}^\ell \to \mathbb{Z}$ such that $F(0, \ldots, 0) = 0$ and

$$b(n) = \sum_{j \in \mathbb{Z}} F(\varepsilon_{j+\ell-1}^{(q)}(n), \ldots, \varepsilon_j^{(q)}(n)),$$

where $\varepsilon_j(n) = 0$ for $j \notin \{0, \ldots, r\}$.

A block-additive function is (almost) a linear combination of pattern-counting functions.

Proposition

Block-additive functions $\bmod m$ give *automatic sequences*.

Block-additive function

Definition (Block-additive function)

We say that $b : \mathbb{N} \to \mathbb{Z}$ is *block-additive* / *digital* if there exists $\ell \geq 1$ and $F : \{0, \dots, q-1\}^\ell \to \mathbb{Z}$ such that $F(0, \dots, 0) = 0$ and

$$b(n) = \sum_{j \in \mathbb{Z}} F(\varepsilon_{j+\ell-1}^{(q)}(n), \dots, \varepsilon_j^{(q)}(n)),$$

where $\varepsilon_j(n) = 0$ for $j \notin \{0, \dots, r\}$.

A block-additive function is (almost) a linear combination of pattern-counting functions.

Proposition

Block-additive functions $\bmod m$ give *automatic sequences*.

Block-additive function

Definition (Block-additive function)

We say that $b : \mathbb{N} \to \mathbb{Z}$ is *block-additive / digital* if there exists $\ell \geq 1$ and $F : \{0, \ldots, q-1\}^\ell \to \mathbb{Z}$ such that $F(0, \ldots, 0) = 0$ and

$$b(n) = \sum_{j \in \mathbb{Z}} F(\varepsilon_{j+\ell-1}^{(q)}(n), \ldots, \varepsilon_j^{(q)}(n)),$$

where $\varepsilon_j(n) = 0$ for $j \notin \{0, \ldots, r\}$.

A block-additive function is (almost) a linear combination of pattern-counting functions.

Proposition

Block-additive functions $\bmod m$ give *automatic sequences*.

Extensions for the 2nd Gelfond Problem

Theorem (Mauduit and Rivat, 2015)

The Rudin-Shapiro sequence is simply normal along primes.

Theorem (Hanna, 2017)

Pattern-counting functions $\bmod m$ along primes are simply normal.

Theorem (M., 2017)

All automatic sequences are orthogonal to the Mobius function.
The densities along primes can be described.

Extensions for the 2nd Gelfond Problem

Theorem (Mauduit and Rivat, 2015)

The Rudin-Shapiro sequence is simply normal along primes.

Theorem (Hanna, 2017)

Pattern-counting functions $\bmod m$ along primes are simply normal.

Theorem (M., 2017)

All automatic sequences are orthogonal to the Mobius function.
The densities along primes can be described.

Extensions for the 2nd Gelfond Problem

Theorem (Mauduit and Rivat, 2015)

The Rudin-Shapiro sequence is simply normal along primes.

Theorem (Hanna, 2017)

Pattern-counting functions $\bmod m$ along primes are simply normal.

Theorem (M., 2017)

All automatic sequences are orthogonal to the Mobius function.
The densities along primes can be described.

Main Result

Theorem (M., 2017)

Let b be a block-additive function and $m \in \mathbb{N}$ with $\gcd(q-1, m) = 1$ and $\gcd(m, \{b(n), n \in \mathbb{N}\}) = 1$. Then $(b(n^2) \bmod m)_{n \in \mathbb{N}}$ is normal in base m'.

This covers all pattern-counting functions mod m, where $\gcd(q-1, m) = 1$, including the Thue-Morse sequence and the Rudin-Shapiro sequence.

Main Result

Theorem (M., 2017)

Let b be a block-additive function and $m \in \mathbb{N}$ with $\gcd(q-1, m) = 1$ and $\gcd(m, \{b(n), n \in \mathbb{N}\}) = 1$. Then $(b(n^2) \bmod m)_{n \in \mathbb{N}}$ is normal in base m'.

This covers all pattern-counting functions $\bmod m$, where $\gcd(q-1, m) = 1$, including the Thue-Morse sequence and the Rudin-Shapiro sequence.

Conditions

1. $\gcd(m, \{b(n), n \in \mathbb{N}\}) = 1$: necessary for simple normality.
2. $\gcd(q-1, m) = 1$: $s_q(n) \equiv n \pmod{q-1}$ is periodic.
3. $F(0, \dots, 0) = 0 : f_{(0,\dots,0)}(n) = \lfloor \log_q(n) \rfloor - \sum_{P \neq (0,\dots,0)} f_P(n)$.
4. Index-range $\mathbb{Z}$ instead of $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)} \bmod 2$.

The technical conditions (3) and (4) are necessary to get very natural restrictions (1) and (2).

Conditions

1. $\gcd(m, \{b(n), n \in \mathbb{N}\}) = 1$: necessary for simple normality.
2. $\gcd(q-1, m) = 1$: $s_q(n) \equiv n \pmod{q-1}$ is periodic.
3. $F(0, \ldots, 0) = 0$: $f_{(0,\ldots,0)}(n) = \lfloor \log_q(n) \rfloor - \sum_{P \neq (0,\ldots,0)} f_P(n)$.
4. Index-range $\mathbb{Z}$ instead of $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)} \bmod 2$.

The technical conditions (3) and (4) are necessary to get very natural restrictions (1) and (2).

Conditions

1. $\gcd(m, \{b(n), n \in \mathbb{N}\}) = 1$: necessary for simple normality.
2. $\gcd(q-1, m) = 1$: $s_q(n) \equiv n (\bmod\, q-1)$ is periodic.
3. $F(0, \ldots, 0) = 0$: $f_{(0,\ldots,0)}(n) = \lfloor \log_q(n) \rfloor - \sum_{P \neq (0,\ldots,0)} f_P(n)$.
4. Index-range $\mathbb{Z}$ instead of $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)} \bmod 2$.

The technical conditions (3) and (4) are necessary to get very natural restrictions (1) and (2).

Conditions

1. $\gcd(m, \{b(n), n \in \mathbb{N}\}) = 1$: necessary for simple normality.
2. $\gcd(q-1, m) = 1$: $s_q(n) \equiv n \pmod{q-1}$ is periodic.
3. $F(0, \dots, 0) = 0 : f_{(0,\dots,0)}(n) = \lfloor \log_q(n) \rfloor - \sum_{P \neq (0,\dots,0)} f_P(n)$.
4. Index-range $\mathbb{Z}$ instead of $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)} \bmod 2$.

The technical conditions (3) and (4) are necessary to get very natural restrictions (1) and (2).

Conditions

1. $\gcd(m, \{b(n), n \in \mathbb{N}\}) = 1$: necessary for simple normality.
2. $\gcd(q-1, m) = 1$: $s_q(n) \equiv n (\bmod\, q-1)$ is periodic.
3. $F(0, \ldots, 0) = 0$: $f_{(0,\ldots,0)}(n) = \lfloor \log_q(n) \rfloor - \sum_{P \neq (0,\ldots,0)} f_P(n)$.
4. Index-range $\mathbb{Z}$ instead of $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)} \bmod 2$.

The technical conditions (3) and (4) are necessary to get very natural restrictions (1) and (2).

Conditions

1. $\gcd(m, \{b(n), n \in \mathbb{N}\}) = 1$: necessary for simple normality.
2. $\gcd(q-1, m) = 1$: $s_q(n) \equiv n (\bmod q-1)$ is periodic.
3. $F(0, \ldots, 0) = 0 : f_{(0,\ldots,0)}(n) = \lfloor \log_q(n) \rfloor - \sum_{P \neq (0,\ldots,0)} f_P(n)$.
4. Index-range $\mathbb{Z}$ instead of $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)}$ mod 2.

The technical conditions (3) and (4) are necessary to get very natural restrictions (1) and (2).

Conditions

1. $\gcd(m, \{b(n), n \in \mathbb{N}\}) = 1$: necessary for simple normality.
2. $\gcd(q-1, m) = 1$: $s_q(n) \equiv n (\bmod q-1)$ is periodic.
3. $F(0, \ldots, 0) = 0 : f_{(0,\ldots,0)}(n) = \lfloor \log_q(n) \rfloor - \sum_{P \neq (0,\ldots,0)} f_P(n)$.
4. Index-range $\mathbb{Z}$ instead of $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)} \bmod 2$.

The technical conditions (3) and (4) are necessary to get very natural restrictions (1) and (2).

Conditions

1. $\gcd(m, \{b(n), n \in \mathbb{N}\}) = 1$: necessary for simple normality.
2. $\gcd(q-1, m) = 1$: $s_q(n) \equiv n (\bmod q-1)$ is periodic.
3. $F(0, \ldots, 0) = 0$: $f_{(0,\ldots,0)}(n) = \lfloor \log_q(n) \rfloor - \sum_{P \neq (0,\ldots,0)} f_P(n)$.
4. Index-range $\mathbb{Z}$ instead of $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)}$ mod 2.

The technical conditions (3) and (4) are necessary to get very natural restrictions (1) and (2).

Conditions

1. $\gcd(m, \{b(n), n \in \mathbb{N}\}) = 1$: necessary for simple normality.
2. $\gcd(q-1, m) = 1$: $s_q(n) \equiv n (\bmod q-1)$ is periodic.
3. $F(0, \ldots, 0) = 0 : f_{(0,\ldots,0)}(n) = \lfloor \log_q(n) \rfloor - \sum_{P \neq (0,\ldots,0)} f_P(n)$.
4. Index-range $\mathbb{Z}$ instead of $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)} \bmod 2$.

The technical conditions (3) and (4) are necessary to get very natural restrictions (1) and (2).

General Strategy

- Rewrite the statement in terms of exponential sums. Every block of length k appears with density m^{-k} if

$$\left|\sum_{n\leq N} \mathrm{e}\left(\sum_{j=0}^{k-1} \alpha_j b((n+j)^2\right)\right| = o(N),$$

for all $(\alpha_0, \ldots, \alpha_{k-1}) \neq (0, \ldots, 0)$, where $\mathrm{e}(x) = exp(2\pi ix)$.

- Use a variation of the Van-der-Corput inequality,

$$\left|\sum_{0<n<N} z_n\right|^2 \leq \frac{N+QR-Q}{R} \sum_{|r|<R} \left(1-\frac{|r|}{R}\right) \sum_{0<n,n+Qr<N} z_{n+Qr}\overline{z_n}.$$

- This cuts off “high“ and “low“ digits.

General Strategy

- Rewrite the statement in terms of exponential sums.
  Every block of length k appears with density m^{-k} if

$$\left| \sum_{n \leq N} \mathrm{e}\left(\sum_{j=0}^{k-1} \alpha_j b((n+j)^2) \right) \right| = o(N),$$

  for all $(\alpha_0, \ldots, \alpha_{k-1}) \neq (0, \ldots, 0)$, where $\mathrm{e}(x) = exp(2\pi i x)$.
- Use a variation of the Van-der-Corput inequality,

$$\left| \sum_{0<n<N} z_n \right|^2 \leq \frac{N + QR - Q}{R} \sum_{|r|<R} \left(1 - \frac{|r|}{R} \right) \sum_{0<n, n+Qr<N} z_{n+Qr} \overline{z_n}.$$

- This cuts off “high“ and “low“ digits.

General Strategy

- Rewrite the statement in terms of exponential sums. Every block of length k appears with density m^{-k} if

$$\left| \sum_{n \leq N} \mathrm{e}\left(\sum_{j=0}^{k-1} \alpha_j b((n+j)^2) \right) \right| = o(N),$$

for all $(\alpha_0, \ldots, \alpha_{k-1}) \neq (0, \ldots, 0)$, where $\mathrm{e}(x) = exp(2\pi i x)$.

- Use a variation of the Van-der-Corput inequality,

$$\left| \sum_{0<n<N} z_n \right|^2 \leq \frac{N + QR - Q}{R} \sum_{|r|<R} \left(1 - \frac{|r|}{R} \right) \sum_{0<n, n+Qr<N} z_{n+Qr} \overline{z_n}.$$

- This cuts off “high“ and “low“ digits.

General Strategy

- Use Vaaler's method to approximate the characteristic function of $[0, \alpha)$ mod 1.
- Find appropriate estimates for the new Fourier-terms,

$$H^I_\lambda(h,d) = \sum_{u<q^\lambda} \mathrm{e}\left(\sum_j \alpha_j b(u+jd+i_j) - huq^{-\lambda}\right).$$

General Strategy

- Use Vaaler's method to approximate the characteristic function of $[0, \alpha)$ mod 1.
- Find appropriate estimates for the new Fourier-terms,

$$H^I_\lambda(h, d) = \sum_{u < q^\lambda} \mathrm{e}\left(\sum_j \alpha_j b(u + jd + i_j) - huq^{-\lambda}\right).$$