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

Clemens Müllner

Tuesday, October 2nd, 2018

Pattern-counting function

Fix $q \geq 2$ a base. We denote the base q expansion of n as follows,

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

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

Definition (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*

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

Pattern-counting function

Fix $q \geq 2$ a base. We denote the base q expansion of n as follows,

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

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

Definition (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*

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

Pattern-counting function

Fix $q \geq 2$ a base. We denote the base q expansion of n as follows,

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

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

Definition (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*

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

Pattern-counting function

Fix $q \geq 2$ a base. We denote the base q expansion of n as follows,

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

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

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*

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

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

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

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

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

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.

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.

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.

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 $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)} \bmod 2$.

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 $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)} \bmod 2$.

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 $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)}$ 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 $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)}$ 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. $\gcd(q-1, m) = 1$: $s_q(n) \equiv n \pmod{q-1}$ 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 $\mathbb{N}$: $f_{(0,1)} + f_{(1,0)}$ 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).

Automatic Sequences

Definition (Automaton - DFA)

$$A = (Q, \Sigma = \{0, \ldots, k-1\}, \delta, q_0, \tau)$$

Example (Thue-Morse sequence)

$$n = 22 = (10110)_2, \qquad t_{22} = 1$$

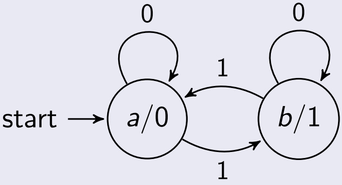
$$\mathbf{t} = (t_n)_{n \geq 0} = 0110100110010110100101100110100 1 \ldots$$

Automatic Sequences

Definition (Automaton - DFA)

$$A = (Q, \Sigma = \{0, \dots, k-1\}, \delta, q_0, \tau)$$

Example (Thue-Morse sequence)



$$n = 22 = (10110)_2, \qquad t_{22} = 1$$

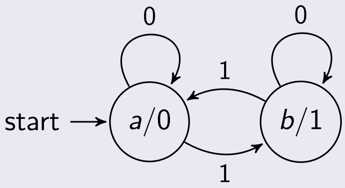
$$\mathbf{t} = (t_n)_{n\geq 0} = 0110100110010110100101100110 1001\dots$$

Automatic Sequences

Definition (Automaton - DFA)

$$A = (Q, \Sigma = \{0, \dots, k-1\}, \delta, q_0, \tau)$$

Example (Thue-Morse sequence)



$$n = 22 = (10110)_2, \qquad t_{22} = 1$$

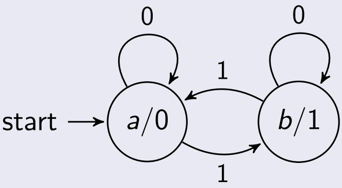
$$\mathbf{t} = (t_n)_{n\geq 0} = 01101001100101101001011001101001\dots$$

Automatic Sequences

Definition (Automaton - DFA)

$$A = (Q, \Sigma = \{0, \ldots, k-1\}, \delta, q_0, \tau)$$

Example (Thue-Morse sequence)



$$n = 22 = (10110)_2, \qquad t_{22} = 1$$

$$\mathbf{t} = (t_n)_{n \geq 0} = 0110100110010110100101100110100 1 \ldots$$

Automatic Sequences

- Blockadditive functions modulo m are automatic sequences.
- The subword complexity p_k of an automatic sequence is (at most) linear in k.
- Every subsequence $(u_{an+b})_{n\geq 0}$ along an arithmetic progression of an automatic sequence $(u_n)_{n\geq 0}$ is again automatic.

Automatic Sequences

- Blockadditive functions modulo m are automatic sequences.
- The subword complexity p_k of an automatic sequence is (at most) linear in k.
- Every subsequence $(u_{an+b})_{n\geq 0}$ along an arithmetic progression of an automatic sequence $(u_n)_{n\geq 0}$ is again automatic.

Automatic Sequences

- Blockadditive functions modulo m are automatic sequences.
- The subword complexity p_k of an automatic sequence is (at most) linear in k.
- Every subsequence $(u_{an+b})_{n\geq 0}$ along an arithmetic progression of an automatic sequence $(u_n)_{n\geq 0}$ is again automatic.

Thue-Morse sequence along squares

Theorem (Moshe, 2007)

The subword-complexity of $(t_{n^2})_{n\in\mathbb{N}}$ is maximal.

Theorem (Mauduit and Rivat, 2009)

$(t_{n^2})_{n\in\mathbb{N}}$ is simply normal in base 2

Theorem (Drmota, Mauduit and Rivat, 2017)

The sequence (t_{n^2}) is normal in base 2.

Thue-Morse sequence along squares

Theorem (Moshe, 2007)

The subword-complexity of $(t_{n^2})_{n\in\mathbb{N}}$ is maximal.

Theorem (Mauduit and Rivat, 2009)

$(t_{n^2})_{n\in\mathbb{N}}$ is simply normal in base 2

Theorem (Drmota, Mauduit and Rivat, 2017)

The sequence (t_{n^2}) is normal in base 2.

Thue-Morse sequence along squares

Theorem (Moshe, 2007)

The subword-complexity of $(t_{n^2})_{n\in\mathbb{N}}$ is maximal.

Theorem (Mauduit and Rivat, 2009)

$(t_{n^2})_{n\in\mathbb{N}}$ is simply normal in base 2

Theorem (Drmota, Mauduit and Rivat, 2017)

The sequence (t_{n^2}) is normal in base 2.

General Strategy

- Rewrite the statement in terms of exponential sums.
  E.g. $dens(t_{n^2}, 0) = 1/2$ holds if

$$\left| \sum_{n \leq N} \mathrm{e}\left(\frac{s_2(n^2)}{2} \right) \right| = o(N),$$

  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 "highänd "low" digits.

General Strategy

- Rewrite the statement in terms of exponential sums. E.g. $dens(t_{n^2}, 0) = 1/2$ holds if

$$\left| \sum_{n \leq N} \mathrm{e}\left(\frac{s_2(n^2)}{2} \right) \right| = o(N),$$

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 "highänd "low"digits.

General Strategy

- Rewrite the statement in terms of exponential sums.
  E.g. $dens(t_{n^2}, 0) = 1/2$ holds if

$$\left|\sum_{n\leq N} \mathrm{e}\left(\frac{s_2(n^2)}{2}\right)\right| = o(N),$$

  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 "highänd "low" digits.

General Strategy

- We end up with somithing like

$$\sum_{r,s} \sum_{n<N} \mathrm{e}\Bigg(\sum_{j} \alpha_j \Big(b_{\lambda,\mu}((n+j)^2) - b_{\lambda,\mu}((n+j+r)^2) - b_{\lambda,\mu}((n+j+sq^{\mu})^2) + b_{\lambda,\mu}((n+j+sq^{\mu}+r)^2) \Big) \Bigg).$$

- Treat all of these independently, where they have the common form

$$H_{\lambda}(h,d) = \sum_{u<q^{\lambda}} \mathrm{e}\left(\sum_{j} \alpha_j b_{\lambda}(u+jd) - huq^{-\lambda} \right).$$

General Strategy

- We end up with somithing like

$$\sum_{r,s}\sum_{n<N} \mathrm{e}\Bigg(\sum_j \alpha_j \bigg(b_{\lambda,\mu}((n+j)^2) - b_{\lambda,\mu}((n+j+r)^2)$$
$$- b_{\lambda,\mu}((n+j+sq^{\mu})^2) + b_{\lambda,\mu}((n+j+sq^{\mu}+r)^2)\bigg)\Bigg).$$

- Treat all of these independently, where they have the common form

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