Automatic sequences from the point of view of Higher order Fourier analysis

Jakub Konieczny

Camille Jordan Institute
Claude Bernard University Lyon 1

Nilpotent structures in topological dynamics,
ergodic theory and combinatorics
Będlewo, 04–10 June 2023

The Thue–Morse(–Prouhet) sequence

$$+1, -1, -1, +1, -1, +1, +1, -1, -1, +1, +1, -1, +1, -1, -1, +1, \ldots$$

The Thue–Morse sequence (discovered by Prouhet) $t\colon \mathbb{N} \to \{+1, -1\}$ is the paradigmatic example of an automatic sequence. It can be defined in several ways:

1. Explicit formula: $t(n) = \begin{cases} +1 & \text{if } n \text{ is } \textit{evil} \text{ (i.e., sum of binary digits is even),} \\ -1 & \text{if } n \text{ is } \textit{odious} \text{ (i.e., sum of binary digits is odd).} \end{cases}$
2. Recurrence: $t(0) = +1, \quad t(2n) = t(n), \quad t(2n+1) = -t(n).$
3. Fixed point of a substitution: $+1 \mapsto +1, -1; \quad -1 \mapsto -1, +1.$
4. Automatic sequence:

5. Strongly 2-multiplicative sequence: $t(1) = -1$, and if $m < 2^\alpha$ then

$$t(2^\alpha n + m) = t(n)t(m).$$

The Thue–Morse(–Prouhet) sequence

$$+1, -1, -1, +1, -1, +1, +1, -1, -1, +1, +1, -1, +1, -1, -1, +1, \ldots$$

The Thue–Morse sequence (discovered by Prouhet) $t\colon \mathbb{N} \to \{+1, -1\}$ is the paradigmatic example of an automatic sequence. It can be defined in several ways:

1. Explicit formula: $t(n) = \begin{cases} +1 & \text{if } n \text{ is } \textit{evil} \text{ (i.e., sum of binary digits is even),} \\ -1 & \text{if } n \text{ is } \textit{odious} \text{ (i.e., sum of binary digits is odd).} \end{cases}$
2. Recurrence: $t(0) = +1, \quad t(2n) = t(n), \quad t(2n+1) = -t(n).$
3. Fixed point of a substitution: $+1 \mapsto +1, -1; \quad -1 \mapsto -1, +1.$
4. Automatic sequence:

5. Strongly 2-multiplicative sequence: $t(1) = -1$, and if $m < 2^\alpha$ then

$$t(2^\alpha n + m) = t(n)t(m).$$

The Thue–Morse(–Prouhet) sequence

$$+1, -1, -1, +1, -1, +1, +1, -1, -1, +1, +1, -1, +1, -1, -1, +1, \ldots$$

The Thue–Morse sequence (discovered by Prouhet) $t\colon \mathbb{N} \to \{+1, -1\}$ is the paradigmatic example of an automatic sequence. It can be defined in several ways:

1. Explicit formula: $t(n) = \begin{cases} +1 & \text{if } n \text{ is } \textit{evil} \text{ (i.e., sum of binary digits is even)}, \\ -1 & \text{if } n \text{ is } \textit{odious} \text{ (i.e., sum of binary digits is odd)}. \end{cases}$
2. Recurrence: $t(0) = +1, \quad t(2n) = t(n), \quad t(2n+1) = -t(n).$
3. Fixed point of a substitution: $+1 \mapsto +1, -1; \quad -1 \mapsto -1, +1.$
4. Automatic sequence:

5. Strongly 2-multiplicative sequence: $t(1) = -1$, and if $m < 2^\alpha$ then

$$t(2^\alpha n + m) = t(n)t(m).$$

The Thue–Morse(–Prouhet) sequence

$$+1, -1, -1, +1, -1, +1, +1, -1, -1, +1, +1, -1, +1, -1, -1, +1, \ldots$$

The Thue–Morse sequence (discovered by Prouhet) $t\colon \mathbb{N} \to \{+1, -1\}$ is the paradigmatic example of an automatic sequence. It can be defined in several ways:

1. Explicit formula: $t(n) = \begin{cases} +1 & \text{if } n \text{ is } \textit{evil} \text{ (i.e., sum of binary digits is even)}, \\ -1 & \text{if } n \text{ is } \textit{odious} \text{ (i.e., sum of binary digits is odd)}. \end{cases}$
2. Recurrence: $t(0) = +1, \quad t(2n) = t(n), \quad t(2n+1) = -t(n)$.
3. Fixed point of a substitution: $+1 \mapsto +1, -1; \quad -1 \mapsto -1, +1$.
4. Automatic sequence:

5. Strongly 2-multiplicative sequence: $t(1) = -1$, and if $m < 2^\alpha$ then

$$t(2^\alpha n + m) = t(n)t(m).$$

The Thue–Morse(–Prouhet) sequence

$$+1, -1, -1, +1, -1, +1, +1, -1, -1, +1, +1, -1, +1, -1, -1, +1, \ldots$$

The Thue–Morse sequence (discovered by Prouhet) $t\colon \mathbb{N} \to \{+1, -1\}$ is the paradigmatic example of an automatic sequence. It can be defined in several ways:

1. Explicit formula: $t(n) = \begin{cases} +1 & \text{if } n \text{ is } \textit{evil} \text{ (i.e., sum of binary digits is even),} \\ -1 & \text{if } n \text{ is } \textit{odious} \text{ (i.e., sum of binary digits is odd).} \end{cases}$
2. Recurrence: $t(0) = +1, \quad t(2n) = t(n), \quad t(2n+1) = -t(n).$
3. Fixed point of a substitution: $+1 \mapsto +1, -1; \quad -1 \mapsto -1, +1.$
4. Automatic sequence:

5. Strongly 2-multiplicative sequence: $t(1) = -1$, and if $m < 2^\alpha$ then

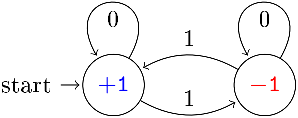
$$t(2^\alpha n + m) = t(n)t(m).$$

The Thue–Morse(–Prouhet) sequence

$$+1, -1, -1, +1, -1, +1, +1, -1, -1, +1, +1, -1, +1, -1, -1, +1, \ldots$$

The Thue–Morse sequence (discovered by Prouhet) $t\colon \mathbb{N} \to \{+1, -1\}$ is the paradigmatic example of an automatic sequence. It can be defined in several ways:

1. Explicit formula: $t(n) = \begin{cases} +1 & \text{if } n \text{ is } \textit{evil} \text{ (i.e., sum of binary digits is even),} \\ -1 & \text{if } n \text{ is } \textit{odious} \text{ (i.e., sum of binary digits is odd).} \end{cases}$
2. Recurrence: $t(0) = +1, \quad t(2n) = t(n), \quad t(2n+1) = -t(n).$
3. Fixed point of a substitution: $+1 \mapsto +1, -1; \quad -1 \mapsto -1, +1.$
4. Automatic sequence:



5. Strongly 2-multiplicative sequence: $t(1) = -1$, and if $m < 2^\alpha$ then

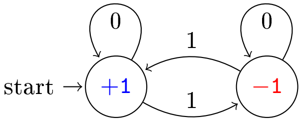
$$t(2^\alpha n + m) = t(n)t(m).$$

The Thue–Morse(–Prouhet) sequence

$$+1, -1, -1, +1, -1, +1, +1, -1, -1, +1, +1, -1, +1, -1, -1, +1, \dots$$

The Thue–Morse sequence (discovered by Prouhet) $t\colon \mathbb{N} \to \{+1, -1\}$ is the paradigmatic example of an automatic sequence. It can be defined in several ways:

1. Explicit formula: $t(n) = \begin{cases} +1 & \text{if } n \text{ is } \textit{evil} \text{ (i.e., sum of binary digits is even)}, \\ -1 & \text{if } n \text{ is } \textit{odious} \text{ (i.e., sum of binary digits is odd)}. \end{cases}$
2. Recurrence: $t(0) = +1, \quad t(2n) = t(n), \quad t(2n+1) = -t(n)$.
3. Fixed point of a substitution: $+1 \mapsto +1, -1; \quad -1 \mapsto -1, +1$.
4. Automatic sequence:



5. Strongly 2-multiplicative sequence: $t(1) = -1$, and if $m < 2^\alpha$ then

$$t(2^\alpha n + m) = t(n)t(m).$$

Automatic sequences via finite automata

Some notation: We let k denote the base in which we work. $\longrightarrow$ e.g. $k = 10$ or $k = 2$

- $\Sigma_k = \{0, 1, \ldots, k-1\}$, the set of digits in base k;
- Σ_k^* is the set of words over Σ_k, monoid with concatenation;
- for $n \in \mathbb{N}$, $(n)_k \in \Sigma_k^*$ is the base-k expansion of n; $\longrightarrow$ no leading zeros
- for $w \in \Sigma_k^*$, $[w]_k \in \mathbb{N}$ is the integer encoded by w.

A finite k-automaton consists of:

- a finite set of states S with a distinguished initial state s_0;
- a transition function $\delta \colon S \times \Sigma_k \to S$;
- an output function $\tau \colon S \to \Omega$.

Computing the sequence:

- Extend δ to a map $S \times \Sigma_k^*$ with $\delta(s, uv) = \delta(\delta(s, u), v)$ or $\delta(\delta(s, v), u)$;
- The sequence computed by the automaton is given by $a(n) = \tau\left(\delta(s_0, (n)_k)\right)$.
- The automaton above computes the Rudin–Shapiro sequence $(-1)^{\#\text{ of }11\text{ in }(n)_2}$.

Intuition: Automatic $\Longleftrightarrow$ Computable by a finite device.

Automatic sequences via finite automata

Some notation: We let k denote the base in which we work. $\longrightarrow$ e.g. $k = 10$ or $k = 2$

- $\Sigma_k = \{0, 1, \ldots, k-1\}$, the set of digits in base k;
- Σ_k^* is the set of words over Σ_k, monoid with concatenation;
- for $n \in \mathbb{N}$, $(n)_k \in \Sigma_k^*$ is the base-k expansion of n; $\longrightarrow$ no leading zeros
- for $w \in \Sigma_k^*$, $[w]_k \in \mathbb{N}$ is the integer encoded by w.

A finite k-automaton consists of:

- a finite set of states S with a distinguished initial state s_0;
- a transition function $\delta \colon S \times \Sigma_k \to S$;
- an output function $\tau \colon S \to \Omega$.

Computing the sequence:

- Extend δ to a map $S \times \Sigma_k^*$ with $\delta(s, uv) = \delta(\delta(s, u), v)$ or $\delta(\delta(s, v), u)$;
- The sequence computed by the automaton is given by $a(n) = \tau(\delta(s_0, (n)_k))$.
- The automaton above computes the Rudin–Shapiro sequence $(-1)^{\#\text{ of }11\text{ in }(n)_2}$.

Intuition: Automatic $\Longleftrightarrow$ Computable by a finite device.

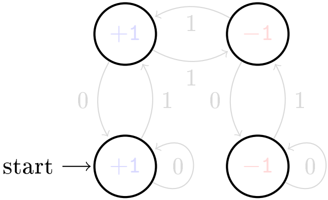
Automatic sequences via finite automata

Some notation: We let k denote the base in which we work. $\longrightarrow$ e.g. $k = 10$ or $k = 2$

- $\Sigma_k = \{0, 1, \ldots, k-1\}$, the set of digits in base k;
- Σ_k^* is the set of words over Σ_k, monoid with concatenation;
- for $n \in \mathbb{N}$, $(n)_k \in \Sigma_k^*$ is the base-k expansion of n; $\longrightarrow$ no leading zeros
- for $w \in \Sigma_k^*$, $[w]_k \in \mathbb{N}$ is the integer encoded by w.

A finite k-automaton consists of:

- a finite set of states S with a distinguished initial state s_0;
- a transition function $\delta \colon S \times \Sigma_k \to S$;
- an output function $\tau \colon S \to \Omega$.



Computing the sequence:

- Extend δ to a map $S \times \Sigma_k^*$ with $\delta(s, uv) = \delta(\delta(s, u), v)$ or $\delta(\delta(s, v), u)$;
- The sequence computed by the automaton is given by $a(n) = \tau(\delta(s_0, (n)_k))$.
- The automaton above computes the Rudin–Shapiro sequence $(-1)^{\#\text{ of } 11 \text{ in } (n)_2}$.

Intuition: Automatic $\Longleftrightarrow$ Computable by a finite device.

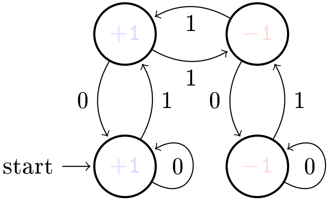
Automatic sequences via finite automata

Some notation: We let k denote the base in which we work. $\longrightarrow$ e.g. $k = 10$ or $k = 2$

- $\Sigma_k = \{0, 1, \ldots, k-1\}$, the set of digits in base k;
- Σ_k^* is the set of words over Σ_k, monoid with concatenation;
- for $n \in \mathbb{N}$, $(n)_k \in \Sigma_k^*$ is the base-k expansion of n; $\longrightarrow$ no leading zeros
- for $w \in \Sigma_k^*$, $[w]_k \in \mathbb{N}$ is the integer encoded by w.

A finite k-automaton consists of:

- a finite set of states S with a distinguished initial state s_0;
- a transition function $\delta \colon S \times \Sigma_k \to S$;
- an output function $\tau \colon S \to \Omega$.



Computing the sequence:

- Extend δ to a map $S \times \Sigma_k^*$ with $\delta(s, uv) = \delta(\delta(s, u), v)$ or $\delta(\delta(s, v), u)$;
- The sequence computed by the automaton is given by $a(n) = \tau\left(\delta(s_0, (n)_k)\right)$.
- The automaton above computes the Rudin–Shapiro sequence $(-1)^{\#\text{ of } 11 \text{ in } (n)_2}$.

Intuition: Automatic $\Longleftrightarrow$ Computable by a finite device.

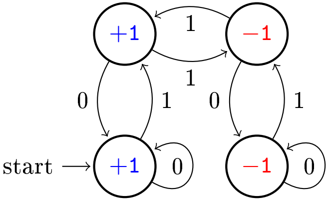
Automatic sequences via finite automata

Some notation: We let k denote the base in which we work. $\longrightarrow$ e.g. $k = 10$ or $k = 2$

- $\Sigma_k = \{0, 1, \ldots, k-1\}$, the set of digits in base k;
- Σ_k^* is the set of words over Σ_k, monoid with concatenation;
- for $n \in \mathbb{N}$, $(n)_k \in \Sigma_k^*$ is the base-k expansion of n; $\longrightarrow$ no leading zeros
- for $w \in \Sigma_k^*$, $[w]_k \in \mathbb{N}$ is the integer encoded by w.

A finite k-automaton consists of:

- a finite set of states S with a distinguished initial state s_0;
- a transition function $\delta \colon S \times \Sigma_k \to S$;
- an output function $\tau \colon S \to \Omega$.



Computing the sequence:

- Extend δ to a map $S \times \Sigma_k^*$ with $\delta(s, uv) = \delta(\delta(s,u), v)$ or $\delta(\delta(s,v), u)$;
- The sequence computed by the automaton is given by $a(n) = \tau(\delta(s_0, (n)_k))$.
- The automaton above computes the Rudin–Shapiro sequence $(-1)^{\#\text{ of } 11 \text{ in } (n)_2}$.

Intuition: Automatic $\Longleftrightarrow$ Computable by a finite device.

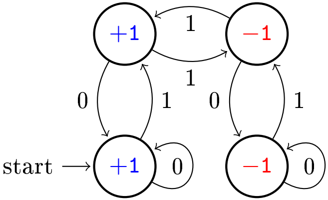
Automatic sequences via finite automata

Some notation: We let k denote the base in which we work. $\longrightarrow$ e.g. $k = 10$ or $k = 2$

- $\Sigma_k = \{0, 1, \ldots, k-1\}$, the set of digits in base k;
- Σ_k^* is the set of words over Σ_k, monoid with concatenation;
- for $n \in \mathbb{N}$, $(n)_k \in \Sigma_k^*$ is the base-k expansion of n; $\longrightarrow$ no leading zeros
- for $w \in \Sigma_k^*$, $[w]_k \in \mathbb{N}$ is the integer encoded by w.

A finite k-automaton consists of:

- a finite set of states S with a distinguished initial state s_0;
- a transition function $\delta \colon S \times \Sigma_k \to S$;
- an output function $\tau \colon S \to \Omega$.



Computing the sequence:

- Extend δ to a map $S \times \Sigma_k^*$ with $\delta(s, uv) = \delta(\delta(s, u), v)$ or $\delta(\delta(s, v), u)$;
- The sequence computed by the automaton is given by $a(n) = \tau\left(\delta(s_0, (n)_k)\right)$.
- The automaton above computes the Rudin–Shapiro sequence $(-1)^{\#\text{ of } 11 \text{ in } (n)_2}$.

Intuition: Automatic $\Longleftrightarrow$ Computable by a finite device.

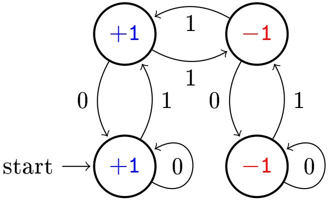
Automatic sequences via finite automata

Some notation: We let k denote the base in which we work. $\longrightarrow$ e.g. $k = 10$ or $k = 2$

- $\Sigma_k = \{0, 1, \ldots, k-1\}$, the set of digits in base k;
- Σ_k^* is the set of words over Σ_k, monoid with concatenation;
- for $n \in \mathbb{N}$, $(n)_k \in \Sigma_k^*$ is the base-k expansion of n; $\longrightarrow$ no leading zeros
- for $w \in \Sigma_k^*$, $[w]_k \in \mathbb{N}$ is the integer encoded by w.

A finite k-automaton consists of:

- a finite set of states S with a distinguished initial state s_0;
- a transition function $\delta \colon S \times \Sigma_k \to S$;
- an output function $\tau \colon S \to \Omega$.



Computing the sequence:

- Extend δ to a map $S \times \Sigma_k^*$ with $\delta(s, uv) = \delta(\delta(s,u), v)$ or $\delta(\delta(s,v), u)$;
- The sequence computed by the automaton is given by $a(n) = \tau\left(\delta(s_0, (n)_k)\right)$.
- The automaton above computes the Rudin–Shapiro sequence $(-1)^{\#\text{ of }11\text{ in }(n)_2}$.

Intuition: Automatic $\Longleftrightarrow$ Computable by a finite device.

Uniformity of Thue–Morse

Question (Mauduit & Sarközy (1998)/folklore)

Is which ways is the Thue–Morse sequence *uniform*/*pseudorandom*?

Structure:

1. Linear *subword complexity*: $\#\left\{w \in \{+1,-1\}^l : w \text{ appears in } t\right\} = O(l)$.
2. $\#\{n < N : t(n) = t(n+1)\} \simeq N/3 \neq N/2$. $\longrightarrow$ $t(n) = t(n+1)$ iff $2 \nmid \nu_2(n+1)$
3. $\#\{n < N : t(n) = t(n+1) = t(n+2)\} = 0$. $\longrightarrow$ in general: t is cube-free

Uniformity:

1. Maximal *arithmetical subword complexity*: For each $l \in \mathbb{N}$ and $w \in \{+1,-1\}^l$ there exist $n, m \in \mathbb{N}_0$ such that $w = t(n), t(n+m), \ldots, t(n+(l-1)m)$.
2. $\sum_{n<N} t(n) = O(1)$ (not very hard).
3. $\sum_{n<N} t(an+b) = O(N^{1-c})$ with $c > 0$. $\longrightarrow$ Gelfond (1968)
4. *Level of distribution* equal to 1: For each $\varepsilon > 0$ there exists $\delta > 0$ such that
$$\sum_{d<N^{1-\varepsilon}} \max_{a \bmod d} \left| \sum_{\substack{n<N \\ n \equiv a \bmod d}} t(n) \right| = O(N^{1-\delta}).$$
$\longrightarrow$ Spiegelhofer (2020)

Uniformity of Thue–Morse

Question (Mauduit & Sarközy (1998)/folklore)

Is which ways is the Thue–Morse sequence *uniform*/*pseudorandom*?

Structure:

1. Linear *subword complexity*: $\#\left\{w \in \{+1,-1\}^l \,:\, w \text{ appears in } t\right\} = O(l)$.
2. $\#\{n < N \,:\, t(n) = t(n+1)\} \simeq N/3 \neq N/2$. $\longrightarrow$ $t(n) = t(n+1)$ iff $2 \nmid \nu_2(n+1)$
3. $\#\{n < N \,:\, t(n) = t(n+1) = t(n+2)\} = 0$. $\longrightarrow$ in general: t is cube-free

Uniformity:

1. Maximal *arithmetical subword complexity*: For each $l \in \mathbb{N}$ and $w \in \{+1,-1\}^l$ there exist $n, m \in \mathbb{N}_0$ such that $w = t(n), t(n+m), \ldots, t(n+(l-1)m)$.
2. $\sum_{n<N} t(n) = O(1)$ (not very hard).
3. $\sum_{n<N} t(an+b) = O(N^{1-c})$ with $c > 0$. $\longrightarrow$ Gelfond (1968)
4. *Level of distribution* equal to 1: For each $\varepsilon > 0$ there exists $\delta > 0$ such that
$$\sum_{d < N^{1-\varepsilon}} \max_{a \bmod d} \left| \sum_{\substack{n<N \\ n \equiv a \bmod d}} t(n) \right| = O(N^{1-\delta}).$$
$\longrightarrow$ Spiegelhofer (2020)

Uniformity of Thue–Morse

Question (Mauduit & Sarközy (1998)/folklore)

Is which ways is the Thue–Morse sequence *uniform*/*pseudorandom*?

Structure:

1. Linear *subword complexity*: $\#\left\{w \in \{+1,-1\}^l : w \text{ appears in } t\right\} = O(l)$.
2. $\#\{n < N : t(n) = t(n+1)\} \simeq N/3 \neq N/2$. $\longrightarrow$ $t(n) = t(n+1)$ iff $2 \nmid \nu_2(n+1)$
3. $\#\{n < N : t(n) = t(n+1) = t(n+2)\} = 0$. $\longrightarrow$ in general: t is cube-free

Uniformity:

1. Maximal *arithmetical subword complexity*: For each $l \in \mathbb{N}$ and $w \in \{+1,-1\}^l$ there exist $n, m \in \mathbb{N}_0$ such that $w = t(n), t(n+m), \ldots, t(n+(l-1)m)$.
2. $\sum_{n<N} t(n) = O(1)$ (not very hard).
3. $\sum_{n<N} t(an+b) = O(N^{1-c})$ with $c > 0$. $\longrightarrow$ Gelfond (1968)
4. *Level of distribution* equal to 1: For each $\varepsilon > 0$ there exists $\delta > 0$ such that

$$\sum_{d<N^{1-\varepsilon}} \max_{a \bmod d} \left| \sum_{\substack{n<N \\ n \equiv a \bmod d}} t(n) \right| = O(N^{1-\delta}).$$

$\longrightarrow$ Spiegelhofer (2020)

Uniformity of Thue–Morse

Question (Mauduit & Sarközy (1998)/folklore)

Is which ways is the Thue–Morse sequence *uniform/pseudorandom*?

Structure:

1. Linear *subword complexity*: $\#\left\{w \in \{+1,-1\}^l \,:\, w \text{ appears in } t\right\} = O(l)$.
2. $\#\{n < N \,:\, t(n) = t(n+1)\} \simeq N/3 \neq N/2$. $\longrightarrow$ $t(n) = t(n+1)$ iff $2 \nmid \nu_2(n+1)$
3. $\#\{n < N \,:\, t(n) = t(n+1) = t(n+2)\} = 0$. $\longrightarrow$ in general: t is cube-free

Uniformity:

1. Maximal *arithmetical subword complexity*: For each $l \in \mathbb{N}$ and $w \in \{+1,-1\}^l$ there exist $n, m \in \mathbb{N}_0$ such that $w = t(n), t(n+m), \ldots, t(n+(l-1)m)$.
2. $\sum_{n<N} t(n) = O(1)$ (not very hard).
3. $\sum_{n<N} t(an+b) = O(N^{1-c})$ with $c > 0$. $\longrightarrow$ Gelfond (1968)
4. *Level of distribution* equal to 1: For each $\varepsilon > 0$ there exists $\delta > 0$ such that

$$\sum_{d<N^{1-\varepsilon}} \max_{a \bmod d} \left| \sum_{\substack{n<N \\ n \equiv a \bmod d}} t(n) \right| = O(N^{1-\delta}).$$

$\longrightarrow$ Spiegelhofer (2020)

Uniformity of Thue–Morse

Question (Mauduit & Sarközy (1998)/folklore)

Is which ways is the Thue–Morse sequence *uniform*/*pseudorandom*?

Structure:

1. Linear *subword complexity*: $\#\left\{w \in \{+1,-1\}^l \,:\, w \text{ appears in } t\right\} = O(l)$.
2. $\#\{n < N \,:\, t(n) = t(n+1)\} \simeq N/3 \neq N/2$. $\longrightarrow$ $t(n) = t(n+1)$ iff $2 \nmid \nu_2(n+1)$
3. $\#\{n < N \,:\, t(n) = t(n+1) = t(n+2)\} = 0$. $\longrightarrow$ in general: t is cube-free

Uniformity:

1. Maximal *arithmetical subword complexity*: For each $l \in \mathbb{N}$ and $w \in \{+1,-1\}^l$ there exist $n, m \in \mathbb{N}_0$ such that $w = t(n), t(n+m), \ldots, t(n+(l-1)m)$.
2. $\sum_{n<N} t(n) = O(1)$ (not very hard).
3. $\sum_{n<N} t(an+b) = O(N^{1-c})$ with $c > 0$. $\longrightarrow$ Gelfond (1968)
4. *Level of distribution* equal to 1: For each $\varepsilon > 0$ there exists $\delta > 0$ such that
$$\sum_{d<N^{1-\varepsilon}} \max_{a \bmod d} \left| \sum_{\substack{n<N \\ n \equiv a \bmod d}} t(n) \right| = O(N^{1-\delta}).$$
$\longrightarrow$ Spiegelhofer (2020)

Uniformity of Thue–Morse

Question (Mauduit & Sarközy (1998)/folklore)

Is which ways is the Thue–Morse sequence *uniform*/*pseudorandom*?

Structure:

1. Linear *subword complexity*: $\#\left\{w \in \{+1,-1\}^l : w \text{ appears in } t\right\} = O(l)$.
2. $\#\{n < N : t(n) = t(n+1)\} \simeq N/3 \neq N/2$. $\longrightarrow$ $t(n) = t(n+1)$ iff $2 \nmid \nu_2(n+1)$
3. $\#\{n < N : t(n) = t(n+1) = t(n+2)\} = 0$. $\longrightarrow$ in general: t is cube-free

Uniformity:

1. Maximal *arithmetical subword complexity*: For each $l \in \mathbb{N}$ and $w \in \{+1,-1\}^l$ there exist $n, m \in \mathbb{N}_0$ such that $w = t(n), t(n+m), \ldots, t(n+(l-1)m)$.
2. $\sum_{n<N} t(n) = O(1)$ (not very hard).
3. $\sum_{n<N} t(an+b) = O(N^{1-c})$ with $c > 0$. $\longrightarrow$ Gelfond (1968)
4. *Level of distribution* equal to 1: For each $\varepsilon > 0$ there exists $\delta > 0$ such that
$$\sum_{d<N^{1-\varepsilon}} \max_{a \bmod d} \left| \sum_{\substack{n<N \\ n\equiv a \bmod d}} t(n) \right| = O(N^{1-\delta}).$$
$\longrightarrow$ Spiegelhofer (2020)

Gelfond problems

1. Thue-Morse does not correlate with the primes: ⟶ Mauduit & Rivat (2010)

$$\#\{p < N \,:\, p \text{ is prime},\ t(p) = +1\} = \frac{1}{2}\pi(N) + O(N^{1-c}).$$

2. Thue-Morse does not correlate with polynomials $p(x) \in \mathbb{Q}[x]$ such that $p(\mathbb{N}) \subseteq \mathbb{N}$:

$$\#\{n < N \,:\, t(p(n)) = +1\} = \frac{1}{2}N + O(N^{1-c}).$$

Known for $p(n) = n^2$; open for $\deg p \geq 3$. ⟶ Mauduit & Rivat (2009)

3. Thue-Morse does not correlate with Piatetski-Shapiro sequences:

$$\#\{n < N \,:\, t(\lfloor n^\alpha \rfloor) = +1\} = \frac{1}{2}N + O(N^{1-c}).$$

Known for $\alpha < 2$; open for $\alpha > 2$. ⟶ Spiegelhofer (2018)

Gelfond problems

1. Thue-Morse does not correlate with the primes: ⟶ Mauduit & Rivat (2010)

$$\#\{p < N \,:\, p \text{ is prime},\ t(p) = +1\} = \frac{1}{2}\pi(N) + O(N^{1-c}).$$

2. Thue-Morse does not correlate with polynomials $p(x) \in \mathbb{Q}[x]$ such that $p(\mathbb{N}) \subseteq \mathbb{N}$:

$$\#\{n < N \,:\, t(p(n)) = +1\} = \frac{1}{2}N + O(N^{1-c}).$$

Known for $p(n) = n^2$; open for $\deg p \geq 3$. ⟶ Mauduit & Rivat (2009)

3. Thue-Morse does not correlate with Piatetski-Shapiro sequences:

$$\#\{n < N \,:\, t(\lfloor n^{\alpha} \rfloor) = +1\} = \frac{1}{2}N + O(N^{1-c}).$$

Known for $\alpha < 2$; open for $\alpha > 2$. ⟶ Spiegelhofer (2018)

Gelfond problems

1. Thue-Morse does not correlate with the primes: $\longrightarrow$ Mauduit & Rivat (2010)

$$\#\{p < N \,:\, p \text{ is prime},\ t(p) = +1\} = \frac{1}{2}\pi(N) + O(N^{1-c}).$$

2. Thue-Morse does not correlate with polynomials $p(x) \in \mathbb{Q}[x]$ such that $p(\mathbb{N}) \subseteq \mathbb{N}$:

$$\#\{n < N \,:\, t(p(n)) = +1\} = \frac{1}{2}N + O(N^{1-c}).$$

Known for $p(n) = n^2$; open for $\deg p \geq 3$. $\longrightarrow$ Mauduit & Rivat (2009)

3. Thue-Morse does not correlate with Piatetski-Shapiro sequences:

$$\#\{n < N \,:\, t(\lfloor n^\alpha \rfloor) = +1\} = \frac{1}{2}N + O(N^{1-c}).$$

Known for $\alpha < 2$; open for $\alpha > 2$. $\longrightarrow$ Spiegelhofer (2018)

Higher order Fourier analysis: first glance

Definition (Gowers norm)

Fix $k \geq 2$. Let $f\colon [N] \to \mathbb{R}$. Then $\|f\|_{U^k[N]} \geq 0$ is defined by:

$$\|f\|_{U^k[N]}^{2^k} = \mathop{\mathbb{E}}_{\mathbf{n}} \prod_{\omega \in \{0,1\}^k} \mathsf{C}^{|\omega|} f\left(n_0 + \omega_1 n_1 + \ldots \omega_k n_k\right),$$

where the average is taken over all parallelepipeds in $[N]$, i.e., over all $\mathbf{n} = (n_0, \ldots, n_k) \in \mathbb{Z}^{k+1}$ such that $n_0 + \omega_1 n_1 + \ldots \omega_k n_k \in [N]$ for all $\omega \in \{0,1\}^k$.

Theorem (Generalised von Neumann Theorem)

Fix $s \geq 1$ and let $f_0, f_1, \ldots, f_{s+1}\colon [N] \to \mathbb{C}$ be 1-bounded. Then

$$\left| \mathop{\mathbb{E}}_{n,m} f_0(n) f_1(n+m) f_2(n+2m) \ldots f_{s+1}(n+(s+1)m) \right| \ll \min_i \|f_i\|_{U^{s+1}[N]}.$$

Corollary: If $A \subset [N]$, $\#A = \alpha N$ and $\left\|1_A - \alpha 1_{[N]}\right\|_{U^{s+1}[N]} \leq \varepsilon$ then then A contains almost as many $(s+2)$-term APs as a random set of the same size,

$$\#\{(n,m) \in [N]^2 \ : \ n, n+m, \ldots, n+(s+1)m \in A\} = \alpha^{s+2} N^2/2(s+1) + O(\varepsilon N^2).$$

Higher order Fourier analysis: first glance

Definition (Gowers norm)

Fix $k \geq 2$. Let $f\colon [N] \to \mathbb{R}$. Then $\|f\|_{U^k[N]} \geq 0$ is defined by:

$$\|f\|_{U^k[N]}^{2^k} = \mathop{\mathbb{E}}_{\mathbf{n}} \prod_{\omega \in \{0,1\}^k} \mathsf{C}^{|\omega|} f\left(n_0 + \omega_1 n_1 + \ldots \omega_k n_k\right),$$

where the average is taken over all parallelepipeds in $[N]$, i.e., over all $\mathbf{n} = (n_0, \ldots, n_k) \in \mathbb{Z}^{k+1}$ such that $n_0 + \omega_1 n_1 + \ldots \omega_k n_k \in [N]$ for all $\omega \in \{0,1\}^k$.

Theorem (Generalised von Neumann Theorem)

Fix $s \geq 1$ and let $f_0, f_1, \ldots, f_{s+1}\colon [N] \to \mathbb{C}$ be 1-bounded. Then

$$\left| \mathop{\mathbb{E}}_{n,m} f_0(n) f_1(n+m) f_2(n+2m) \ldots f_{s+1}(n+(s+1)m) \right| \ll \min_i \|f_i\|_{U^{s+1}[N]}.$$

Corollary: If $A \subset [N]$, $\#A = \alpha N$ and $\left\|1_A - \alpha 1_{[N]}\right\|_{U^{s+1}[N]} \leq \varepsilon$ then then A contains almost as many $(s+2)$-term APs as a random set of the same size,

$$\#\{(n,m) \in [N]^2 \ : \ n, n+m, \ldots, n+(s+1)m \in A\} = \alpha^{s+2} N^2 / 2(s+1) + O(\varepsilon N^2).$$

Higher order Fourier analysis meets Thue–Morse

Recall: $\|f\|_{U^2} \simeq \|\hat{f}\|_{\ell^4} \simeq \|\hat{f}\|_\infty$. Hence, the result of Gelfond (1968) implies that the Thue–Morse sequence is U^2-uniform, $\|t\|_{U^2[N]} \ll N^{-c}$.

Corollary: The number of 3-term APs in $\{n \in [N] : t(n) = +1\}$ is $\sim N^2/32$.

Theorem (K.)

The Thue–Morse sequence is Gowers uniform of all orders. More precisely, for each $s \geq 1$ there exists $c = c_s > 0$ such that $\|t\|_{U^{s+1}[N]} \ll N^{-c}$.

Corollary: The number of $(s+2)$-term APs in $\{n \in [N] : t(n) = +1\}$ is $\sim N^2/2^{s+3}(s+1)$.

Higher order Fourier analysis meets Thue–Morse

Recall: $\|f\|_{U^2} \simeq \|\hat{f}\|_{\ell^4} \simeq \|\hat{f}\|_\infty$. Hence, the result of Gelfond (1968) implies that the Thue–Morse sequence is U^2-uniform, $\|t\|_{U^2[N]} \ll N^{-c}$.
Corollary: The number of 3-term APs in $\{n \in [N] : t(n) = +1\}$ is $\sim N^2/32$.

Theorem (K.)

The Thue–Morse sequence is Gowers uniform of all orders. More precisely, for each $s \geq 1$ there exists $c = c_s > 0$ such that $\|t\|_{U^{s+1}[N]} \ll N^{-c}$.

Corollary: The number of $(s+2)$-term APs in $\{n \in [N] : t(n) = +1\}$ is $\sim N^2/2^{s+3}(s+1)$.

Uniform "digital" sequences

A sequence $f\colon \mathbb{N} \to \mathbb{C}$ is k-**multiplicative** if

$$f(n+m) = f(n)f(m) \qquad \text{for all } n, m \geq 0 \text{ such that } m < k^i,\ k^i | n.$$

Theorem (Fan & K.) If f is bounded and k-multiplicative, and $s \geq 1$ then

$$\|f\|_{U^{s+1}[N]} \to 0 \text{ as } N \to \infty \text{ if and only if } \|f\|_{U^2[N]} \to 0 \text{ as } N \to \infty.$$

Nota bene: The same equivalence holds for multiplicative sequences, i.e., $f\colon \mathbb{N} \to \mathbb{C}$ such that $f(nm) = f(n)f(m)$ if $\gcd(n,m) = 1$. $\longrightarrow$ Frantzikinakis & Host (2017)

Rudin–Shapiro sequence: $r\colon \mathbb{N} \to \{-1, +1\}$.

- Explicit formula:

$$r(n) = \begin{cases} +1 & \text{if 11 appears an even number of times in the binary expansion of } n, \\ -1 & \text{if 11 appears an odd number of times in the binary expansion of } n. \end{cases}$$

- Recurrence: $r(0) = +1$, $r(2n) = r(n)$, $r(2n+1) = (-1)^n r(n)$.

Theorem (K.) For each $s \geq 1$ there exists $c > 0$ such that $\|r\|_{U^{s+1}[N]} \ll N^{-c}$.
Remark: The same applies to other sequences defined by "counting patterns".

Uniform "digital" sequences

A sequence $f\colon \mathbb{N} \to \mathbb{C}$ is k-**multiplicative** if

$$f(n+m) = f(n)f(m) \qquad \text{for all } n, m \geq 0 \text{ such that } m < k^i,\ k^i | n.$$

Theorem (Fan & K.) If f is bounded and k-multiplicative, and $s \geq 1$ then

$$\|f\|_{U^{s+1}[N]} \to 0 \text{ as } N \to \infty \text{ if and only if } \|f\|_{U^2[N]} \to 0 \text{ as } N \to \infty.$$

Nota bene: The same equivalence holds for multiplicative sequences, i.e., $f\colon \mathbb{N} \to \mathbb{C}$ such that $f(nm) = f(n)f(m)$ if $\gcd(n, m) = 1$. $\longrightarrow$ Frantzikinakis & Host (2017)

Rudin–Shapiro sequence: $r\colon \mathbb{N} \to \{-1, +1\}$.

- Explicit formula:

$$r(n) = \begin{cases} +1 & \text{if 11 appears an even number of times in the binary expansion of } n, \\ -1 & \text{if 11 appears an odd number of times in the binary expansion of } n. \end{cases}$$

- Recurrence: $r(0) = +1$, $r(2n) = r(n)$, $r(2n+1) = (-1)^n r(n)$.

Theorem (K.) For each $s \geq 1$ there exists $c > 0$ such that $\|r\|_{U^{s+1}[N]} \ll N^{-c}$.
Remark: The same applies to other sequences defined by "counting patterns".

Higher order Fourier analysis meets automatic sequences

Question

Which among k-automatic sequences are Gowers uniform?

Basic classes of non-uniform sequences:

1. *periodic*, such as $n \mapsto n \bmod 3$;
2. *forward synchronising*, such as $n \mapsto \nu_2(n) \bmod 2$; $\longrightarrow 2^{\nu_2(n)} \parallel n$
3. *backwards synchronising*, such as $n \mapsto \lfloor \log_2(n) \rfloor \bmod 2$.

Theorem (Byszewski, K. & Müllner)

Each automatic sequence $a \colon \mathbb{N}_0 \to \mathbb{C}$ has a decomposition $a = a_{\mathrm{str}} + a_{\mathrm{uni}}$, where

1. *a_{uni} is uniform in the sense that for each $s \geq 1$ there exists $c_s > 0$ such that*

$$\|a_{\mathrm{uni}}\|_{U^{s+1}[N]} \ll N^{-c_s}.$$

2. *a_{str} is structured in the sense that there exist $a_{\mathrm{per}}, a_{\mathrm{fs}}, a_{\mathrm{bs}} \colon \mathbb{N}_0 \to \Omega_{\mathrm{per}}, \Omega_{\mathrm{fs}}, \Omega_{\mathrm{bs}}$ which are periodic, forward synchronising and backward synchronising respectively and a map $F \colon \Omega_{\mathrm{per}} \times \Omega_{\mathrm{fs}} \times \Omega_{\mathrm{bs}} \to \mathbb{C}$ such that*

$$a_{\mathrm{str}}(n) = F\left(a_{\mathrm{per}}(n), a_{\mathrm{fs}}(n), a_{\mathrm{bs}}(n)\right).$$

Higher order Fourier analysis meets automatic sequences

Question

Which among k-automatic sequences are Gowers uniform?

Basic classes of non-uniform sequences:

1. *periodic*, such as $n \mapsto n \bmod 3$;
2. *forward synchronising*, such as $n \mapsto \nu_2(n) \bmod 2$; $\longrightarrow 2^{\nu_2(n)} \parallel n$
3. *backwards synchronising*, such as $n \mapsto \lfloor \log_2(n) \rfloor \bmod 2$.

Theorem (Byszewski, K. & Müllner)

Each automatic sequence $a \colon \mathbb{N}_0 \to \mathbb{C}$ has a decomposition $a = a_{\text{str}} + a_{\text{uni}}$, where

1. *a_{uni} is uniform in the sense that for each $s \geq 1$ there exists $c_s > 0$ such that*
$$\|a_{\text{uni}}\|_{U^{s+1}[N]} \ll N^{-c_s}.$$
2. *a_{str} is structured in the sense that there exist $a_{\text{per}}, a_{\text{fs}}, a_{\text{bs}} \colon \mathbb{N}_0 \to \Omega_{\text{per}}, \Omega_{\text{fs}}, \Omega_{\text{bs}}$ which are periodic, forward synchronising and backward synchronising respectively and a map $F \colon \Omega_{\text{per}} \times \Omega_{\text{fs}} \times \Omega_{\text{bs}} \to \mathbb{C}$ such that*
$$a_{\text{str}}(n) = F\left(a_{\text{per}}(n), a_{\text{fs}}(n), a_{\text{bs}}(n)\right).$$

Higher order Fourier analysis meets automatic sequences

Question

Which among k-automatic sequences are Gowers uniform?

Basic classes of non-uniform sequences:

1. *periodic*, such as $n \mapsto n \bmod 3$;
2. *forward synchronising*, such as $n \mapsto \nu_2(n) \bmod 2$; $\longrightarrow 2^{\nu_2(n)} \parallel n$
3. *backwards synchronising*, such as $n \mapsto \lfloor \log_2(n) \rfloor \bmod 2$.

Theorem (Byszewski, K. & Müllner)

Each automatic sequence $a \colon \mathbb{N}_0 \to \mathbb{C}$ has a decomposition $a = a_{\text{str}} + a_{\text{uni}}$, where

1. a_{uni} *is uniform in the sense that for each $s \geq 1$ there exists $c_s > 0$ such that*
$$\|a_{\text{uni}}\|_{U^{s+1}[N]} \ll N^{-c_s}.$$
2. a_{str} *is structured in the sense that there exist $a_{\text{per}}, a_{\text{fs}}, a_{\text{bs}} \colon \mathbb{N}_0 \to \Omega_{\text{per}}, \Omega_{\text{fs}}, \Omega_{\text{bs}}$ which are periodic, forward synchronising and backward synchronising respectively and a map $F \colon \Omega_{\text{per}} \times \Omega_{\text{fs}} \times \Omega_{\text{bs}} \to \mathbb{C}$ such that*
$$a_{\text{str}}(n) = F\left(a_{\text{per}}(n), a_{\text{fs}}(n), a_{\text{bs}}(n)\right).$$

Arithmetic regularity lemma

Theorem (Green & Tao (2010))

Fix $s \geq 1$, $\varepsilon > 0$ and a growth function $\mathcal{F} \colon \mathbb{R}_+ \to \mathbb{R}_+$. Each sequence $a \colon [N] \to [0,1]$ has a decomposition $a = a_{\text{nil}} + a_{\text{sml}} + a_{\text{uni}}$, where $M = O(1)$ and

1. a_{uni} *is uniform in the sense that* $\|a_{\text{uni}}\|_{U^{s+1}[N]} \leq 1/\mathcal{F}(M)$.
2. a_{sml} *is small in the sense that* $\|a_{\text{sml}}\|_{L^2[N]} \leq \varepsilon$.
3. a_{nil} *is a* $(\mathcal{F}(M), N)$*-irrational virtual degree* s *nilsequence of complexity* $\leq M$.

Recall: If a is automatic, then $a_{\text{str}}(n) = F\left(a_{\text{per}}(n), a_{\text{fs}}(n), a_{\text{bs}}(n)\right)$, where

- a_{per} is periodic;
- a_{fs} is essentially periodic; $\longrightarrow a_{\text{fs}} = [k^i\text{-periodic}] + O(1/k^{i\eta})$ in $L^2[N]$
- a_{bs} is constant on long intervals.

Hence, $a_{\text{str}} = [\text{1-step nilsequence}] + [\text{small error}]$.

Key differences:

- For automatic sequences, 1-step nilsequences are enough.
- Quantitative bounds in the decomposition are reasonable.

Arithmetic regularity lemma

Theorem (Green & Tao (2010))

Fix $s \geq 1$, $\varepsilon > 0$ and a growth function $\mathcal{F} \colon \mathbb{R}_+ \to \mathbb{R}_+$. Each sequence $a \colon [N] \to [0,1]$ has a decomposition $a = a_{\mathrm{nil}} + a_{\mathrm{sml}} + a_{\mathrm{uni}}$, where $M = O(1)$ and

1. *a_{uni} is uniform in the sense that $\|a_{\mathrm{uni}}\|_{U^{s+1}[N]} \leq 1/\mathcal{F}(M)$.*
2. *a_{sml} is small in the sense that $\|a_{\mathrm{sml}}\|_{L^2[N]} \leq \varepsilon$.*
3. *a_{nil} is a $(\mathcal{F}(M), N)$-irrational virtual degree s nilsequence of complexity $\leq M$.*

Recall: If a is automatic, then $a_{\mathrm{str}}(n) = F\left(a_{\mathrm{per}}(n), a_{\mathrm{fs}}(n), a_{\mathrm{bs}}(n)\right)$, where

- a_{per} is periodic;
- a_{fs} is essentially periodic; $\longrightarrow a_{\mathrm{fs}} = [k^i\text{-periodic}] + O(1/k^{i\eta})$ in $L^2[N]$
- a_{bs} is constant on long intervals.

Hence, $a_{\mathrm{str}} = [\text{1-step nilsequence}] + [\text{small error}]$.

Key differences:

- For automatic sequences, 1-step nilsequences are enough.
- Quantitative bounds in the decomposition are reasonable.

Arithmetic regularity lemma

Theorem (Green & Tao (2010))

Fix $s \geq 1$, $\varepsilon > 0$ *and a growth function* $\mathcal{F}\colon \mathbb{R}_+ \to \mathbb{R}_+$. *Each sequence* $a\colon [N] \to [0,1]$ *has a decomposition* $a = a_{\mathrm{nil}} + a_{\mathrm{sml}} + a_{\mathrm{uni}}$, *where* $M = O(1)$ *and*

1. a_{uni} *is uniform in the sense that* $\|a_{\mathrm{uni}}\|_{U^{s+1}[N]} \leq 1/\mathcal{F}(M)$.
2. a_{sml} *is small in the sense that* $\|a_{\mathrm{sml}}\|_{L^2[N]} \leq \varepsilon$.
3. a_{nil} *is a* $(\mathcal{F}(M), N)$*-irrational virtual degree* s *nilsequence of complexity* $\leq M$.

Recall: If a is automatic, then $a_{\mathrm{str}}(n) = F\left(a_{\mathrm{per}}(n), a_{\mathrm{fs}}(n), a_{\mathrm{bs}}(n)\right)$, where

- a_{per} is periodic;
- a_{fs} is essentially periodic; $\longrightarrow a_{\mathrm{fs}} = [k^i\text{-periodic}] + O(1/k^{i\eta})$ in $L^2[N]$
- a_{bs} is constant on long intervals.

Hence, $a_{\mathrm{str}} = [\text{1-step nilsequence}] + [\text{small error}]$.

Key differences:

- For automatic sequences, 1-step nilsequences are enough.
- Quantitative bounds in the decomposition are reasonable.

Application: Popular differences

Fix $l \in \mathbb{N}$, $\alpha > 0$ and $\varepsilon > 0$. Let $A \subset [N]$ be a set with $\#A \geq \alpha N$. We will call an integer $m \in [N]$ a *popular difference* if A contains at least $(\alpha^l - \varepsilon)N$ length-l arithmetic progressions with difference m.

Theorem (Bergelson, Host & Kra (2005); Green & Tao (2010))

If $l \leq 4$ then there are $\gg N$ popular differences. This is no longer true for $l \geq 5$.

Corollary: Suppose that $A = \tilde{A} \cap [N]$ for some automatic set $\tilde{A}$ (with complexity bounded as $N \to \infty$). Then for each $l \in \mathbb{N}$, there are $\gg N$ popular differences.

Proof ideas:

- Let $M \in \mathbb{N}$ be large, let $d \in \mathbb{N}$ multiplicatively rich. Suppose that $N = k^L$.
- Put $P = \left\{m \in \mathbb{N} : m \equiv 0 \bmod d,\ m \equiv 0 \bmod k^M,\ m < k^{L-M}\right\}$.
- Hope: Many $m \in P$ are popular differences, $\mathop{\mathbb{E}}_{m \in P} \mathop{\mathbb{E}}_{n \in [N]} \prod_{i=0}^{l-1} 1_A(n + im) \gtrsim \alpha^l$.
- By generalised von Neumann, we only need $\mathop{\mathbb{E}}_{m \in P} \mathop{\mathbb{E}}_{n \in [N]} \prod_{i=0}^{l-1} 1_{A,\mathrm{str}}(n + im) \gtrsim \alpha^l$.
- Because $1_{A,\mathrm{str}}$ is structured, we almost always have $1_{A,\mathrm{str}}(n + im) = 1_{A,\mathrm{str}}(n)$.

Application: Popular differences

Fix $l \in \mathbb{N}$, $\alpha > 0$ and $\varepsilon > 0$. Let $A \subset [N]$ be a set with $\#A \geq \alpha N$. We will call an integer $m \in [N]$ a *popular difference* if A contains at least $(\alpha^l - \varepsilon)N$ length-l arithmetic progressions with difference m.

Theorem (Bergelson, Host & Kra (2005); Green & Tao (2010))

If $l \leq 4$ then there are $\gg N$ popular differences. This is no longer true for $l \geq 5$.

Corollary: Suppose that $A = \tilde{A} \cap [N]$ for some automatic set $\tilde{A}$ (with complexity bounded as $N \to \infty$). Then for each $l \in \mathbb{N}$, there are $\gg N$ popular differences.

Proof ideas:

- Let $M \in \mathbb{N}$ be large, let $d \in \mathbb{N}$ multiplicatively rich. Suppose that $N = k^L$.
- Put $P = \left\{ m \in \mathbb{N} : m \equiv 0 \bmod d,\ m \equiv 0 \bmod k^M,\ m < k^{L-M} \right\}$.
- Hope: Many $m \in P$ are popular differences, $\mathop{\mathbb{E}}_{m \in P} \mathop{\mathbb{E}}_{n \in [N]} \prod_{i=0}^{l-1} 1_A(n + im) \gtrsim \alpha^l$.
- By generalised von Neumann, we only need $\mathop{\mathbb{E}}_{m \in P} \mathop{\mathbb{E}}_{n \in [N]} \prod_{i=0}^{l-1} 1_{A,\mathrm{str}}(n + im) \gtrsim \alpha^l$.
- Because $1_{A,\mathrm{str}}$ is structured, we almost always have $1_{A,\mathrm{str}}(n + im) = 1_{A,\mathrm{str}}(n)$.

Application: Popular differences

Fix $l \in \mathbb{N}$, $\alpha > 0$ and $\varepsilon > 0$. Let $A \subset [N]$ be a set with $\#A \geq \alpha N$. We will call an integer $m \in [N]$ a *popular difference* if A contains at least $(\alpha^l - \varepsilon)N$ length-l arithmetic progressions with difference m.

Theorem (Bergelson, Host & Kra (2005); Green & Tao (2010))

If $l \leq 4$ then there are $\gg N$ popular differences. This is no longer true for $l \geq 5$.

Corollary: Suppose that $A = \tilde{A} \cap [N]$ for some automatic set $\tilde{A}$ (with complexity bounded as $N \to \infty$). Then for each $l \in \mathbb{N}$, there are $\gg N$ popular differences.

Proof ideas:

- Let $M \in \mathbb{N}$ be large, let $d \in \mathbb{N}$ multiplicatively rich. Suppose that $N = k^L$.
- Put $P = \left\{ m \in \mathbb{N} \,:\, m \equiv 0 \bmod d,\ m \equiv 0 \bmod k^M,\ m < k^{L-M} \right\}$.
- Hope: Many $m \in P$ are popular differences, $\mathbb{E}_{m \in P} \mathbb{E}_{n \in [N]} \prod_{i=0}^{l-1} 1_A(n + im) \gtrsim \alpha^l$.
- By generalised von Neumann, we only need $\mathbb{E}_{m \in P} \mathbb{E}_{n \in [N]} \prod_{i=0}^{l-1} 1_{A,\mathrm{str}}(n + im) \gtrsim \alpha^l$.
- Because $1_{A,\mathrm{str}}$ is structured, we almost always have $1_{A,\mathrm{str}}(n + im) = 1_{A,\mathrm{str}}(n)$.

Application: Popular differences

Fix $l \in \mathbb{N}$, $\alpha > 0$ and $\varepsilon > 0$. Let $A \subset [N]$ be a set with $\#A \geq \alpha N$. We will call an integer $m \in [N]$ a *popular difference* if A contains at least $(\alpha^l - \varepsilon)N$ length-l arithmetic progressions with difference m.

Theorem (Bergelson, Host & Kra (2005); Green & Tao (2010))

If $l \leq 4$ then there are $\gg N$ popular differences. This is no longer true for $l \geq 5$.

Corollary: Suppose that $A = \tilde{A} \cap [N]$ for some automatic set $\tilde{A}$ (with complexity bounded as $N \to \infty$). Then for each $l \in \mathbb{N}$, there are $\gg N$ popular differences.

Proof ideas:

- Let $M \in \mathbb{N}$ be large, let $d \in \mathbb{N}$ multiplicatively rich. Suppose that $N = k^L$.
- Put $P = \left\{ m \in \mathbb{N} \,:\, m \equiv 0 \bmod d,\ m \equiv 0 \bmod k^M,\ m < k^{L-M} \right\}$.
- Hope: Many $m \in P$ are popular differences, $\mathop{\mathbb{E}}_{m \in P} \mathop{\mathbb{E}}_{n \in [N]} \prod_{i=0}^{l-1} 1_A(n + im) \gtrsim \alpha^l$.
- By generalised von Neumann, we only need $\mathop{\mathbb{E}}_{m \in P} \mathop{\mathbb{E}}_{n \in [N]} \prod_{i=0}^{l-1} 1_{A,\mathrm{str}}(n + im) \gtrsim \alpha^l$.
- Because $1_{A,\mathrm{str}}$ is structured, we almost always have $1_{A,\mathrm{str}}(n + im) = 1_{A,\mathrm{str}}(n)$.

Application: Quantitative Cobham's theorem

Theorem (Cobham (1969))

Let $k, \ell \geq 2$ and let $a\colon \mathbb{N} \to \Omega$ be a sequence that is both k- and ℓ-automatic. Then

- *k and ℓ are multiplicatively dependent, i.e., $\log_k(\ell) \in \mathbb{Q}$; or*
- *a is eventually periodic (and hence automatic in every base).*

Question: How similar can a k-automatic sequence be to an ℓ-automatic sequence?

- We already know that they cannot be equal, or even asymptotically equal.
- We need to account for possible correlations with periodic sequences.

Theorem (Adamczewski, K., Müllner)

Let $k, \ell \geq 2$ be multiplicatively independent integers and let $a, b\colon \mathbb{N} \to \mathbb{C}$ be k- and ℓ-automatic, respectively. Then

$$\sum_{n<N} a(n)b(n) = \sum_{n<N} a_{\mathrm{str}}(n)b_{\mathrm{str}}(n) + O(N^{1-c}).$$

Corollary: Each Gowers uniform k-automatic sequence a is a orthogonal to each ℓ-automatic sequence b,

$$\sum_{n<N} a(n)b(n) = O(N^{1-c}).$$

Application: Quantitative Cobham's theorem

Theorem (Cobham (1969))

Let $k, \ell \geq 2$ and let $a\colon \mathbb{N} \to \Omega$ be a sequence that is both k- and ℓ-automatic. Then

- *k and ℓ are multiplicatively dependent, i.e., $\log_k(\ell) \in \mathbb{Q}$; or*
- *a is eventually periodic (and hence automatic in every base).*

Question: How similar can a k-automatic sequence be to an ℓ-automatic sequence?

- We already know that they cannot be equal, or even asymptotically equal.
- We need to account for possible correlations with periodic sequences.

Theorem (Adamczewski, K., Müllner)

Let $k, \ell \geq 2$ be multiplicatively independent integers and let $a, b\colon \mathbb{N} \to \mathbb{C}$ be k- and ℓ-automatic, respectively. Then

$$\sum_{n<N} a(n)b(n) = \sum_{n<N} a_{\mathrm{str}}(n)b_{\mathrm{str}}(n) + O(N^{1-c}).$$

Corollary: Each Gowers uniform k-automatic sequence a is a orthogonal to each ℓ-automatic sequence b,

$$\sum_{n<N} a(n)b(n) = O(N^{1-c}).$$

Application: Quantitative Cobham's theorem

Theorem (Cobham (1969))

Let $k, \ell \geq 2$ and let $a\colon \mathbb{N} \to \Omega$ be a sequence that is both k- and ℓ-automatic. Then

- *k and ℓ are multiplicatively dependent, i.e., $\log_k(\ell) \in \mathbb{Q}$; or*
- *a is eventually periodic (and hence automatic in every base).*

Question: How similar can a k-automatic sequence be to an ℓ-automatic sequence?

- We already know that they cannot be equal, or even asymptotically equal.
- We need to account for possible correlations with periodic sequences.

Theorem (Adamczewski, K., Müllner)

Let $k, \ell \geq 2$ be multiplicatively independent integers and let $a, b\colon \mathbb{N} \to \mathbb{C}$ be k- and ℓ-automatic, respectively. Then

$$\sum_{n<N} a(n)b(n) = \sum_{n<N} a_{\mathrm{str}}(n)b_{\mathrm{str}}(n) + O(N^{1-c}).$$

Corollary: Each Gowers uniform k-automatic sequence a is a orthogonal to each ℓ-automatic sequence b,

$$\sum_{n<N} a(n)b(n) = O(N^{1-c}).$$

Application: Quantitative Cobham's theorem

Theorem (Cobham (1969))

Let $k, \ell \geq 2$ and let $a \colon \mathbb{N} \to \Omega$ be a sequence that is both k- and ℓ-automatic. Then

- *k and ℓ are multiplicatively dependent, i.e., $\log_k(\ell) \in \mathbb{Q}$; or*
- *a is eventually periodic (and hence automatic in every base).*

Question: How similar can a k-automatic sequence be to an ℓ-automatic sequence?

- We already know that they cannot be equal, or even asymptotically equal.
- We need to account for possible correlations with periodic sequences.

Theorem (Adamczewski, K., Müllner)

Let $k, \ell \geq 2$ be multiplicatively independent integers and let $a, b \colon \mathbb{N} \to \mathbb{C}$ be k- and ℓ-automatic, respectively. Then

$$\sum_{n<N} a(n)b(n) = \sum_{n<N} a_{\text{str}}(n)b_{\text{str}}(n) + O(N^{1-c}).$$

Corollary: Each Gowers uniform k-automatic sequence a is a orthogonal to each ℓ-automatic sequence b,

$$\sum_{n<N} a(n)b(n) = O(N^{1-c}).$$

Group extensions of automata

Two "extreme" classes of k-automatic sequences:

1. *Synchronising (forwards):* There exists a *synchronising word* $w \in \Sigma_k^*$ such that

$$a(uwv) = a(wv) \text{ for all words } u, v \in \Sigma_k^*.$$

   In particular, a is *almost periodic.*

2. *Invertible:* There is a group G, $\lambda\colon \Sigma_k \to G$, $\lambda(0) = \mathrm{id}_G$, and a map $\chi\colon G \to \mathbb{C}$ such that

$$a(n) = \chi\left(\lambda\left(u_l\right) \cdot \lambda\left(u_{l-1}\right) \cdot \dots \cdot \lambda\left(u_0\right)\right) \text{ for } u_l u_{l-1} \dots u_0 = (n)_k \in \Sigma_k^*. \qquad (\dagger)$$

Idea: $\left\{\begin{matrix}\text{Arbitrary}\\ \text{automaton}\end{matrix}\right\} \longrightarrow \left\{\begin{matrix}\text{Synchronising}\\ \text{automaton}\end{matrix}\right\} \oplus \left\{\begin{matrix}\text{Group}\\ \text{labels}\end{matrix}\right\}.$

Simplifying assumptions:

1. The sequence a is invertible and given by $(\dagger)$. $\longrightarrow$ significantly simpler case
2. The map $\chi\colon G \to \mathbb{S}^1 \subset \mathbb{C}$ is a group homomorphism. $\longrightarrow$ Peter–Weyl, $\dim = 1$

Goal: The sequence a is either highly Gowers uniform of all orders or periodic.

Group extensions of automata

Two "extreme" classes of k-automatic sequences:

1. *Synchronising (forwards):* There exists a *synchronising word* $w \in \Sigma_k^*$ such that

$$a(uwv) = a(wv) \text{ for all words } u, v \in \Sigma_k^*.$$

   In particular, a is *almost periodic.*

2. *Invertible:* There is a group G, $\lambda\colon \Sigma_k \to G$, $\lambda(0) = \mathrm{id}_G$, and a map $\chi\colon G \to \mathbb{C}$ such that

$$a(n) = \chi\left(\lambda\left(u_l\right) \cdot \lambda\left(u_{l-1}\right) \cdot \cdots \cdot \lambda\left(u_0\right)\right) \text{ for } u_l u_{l-1} \ldots u_0 = (n)_k \in \Sigma_k^*. \qquad (\dagger)$$

Idea:
$$\left\{\begin{matrix}\text{Arbitrary}\\ \text{automaton}\end{matrix}\right\} \longrightarrow \left\{\begin{matrix}\text{Synchronising}\\ \text{automaton}\end{matrix}\right\} \oplus \left\{\begin{matrix}\text{Group}\\ \text{labels}\end{matrix}\right\}.$$

Simplifying assumptions:

1. The sequence a is invertible and given by $(\dagger)$. $\longrightarrow$ significantly simpler case
2. The map $\chi\colon G \to \mathbb{S}^1 \subset \mathbb{C}$ is a group homomorphism. $\longrightarrow$ Peter–Weyl, $\dim = 1$

Goal: The sequence a is either highly Gowers uniform of all orders or periodic.

Group extensions of automata

Two "extreme" classes of k-automatic sequences:

1. *Synchronising (forwards):* There exists a *synchronising word* $w \in \Sigma_k^*$ such that
$$a(uwv) = a(wv) \text{ for all words } u, v \in \Sigma_k^*.$$
In particular, a is *almost periodic.*
2. *Invertible:* There is a group G, $\lambda\colon \Sigma_k \to G$, $\lambda(0) = \mathrm{id}_G$, and a map $\chi\colon G \to \mathbb{C}$ such that
$$a(n) = \chi\left(\lambda\left(u_l\right) \cdot \lambda\left(u_{l-1}\right) \cdot \cdots \cdot \lambda\left(u_0\right)\right) \text{ for } u_l u_{l-1} \dots u_0 = (n)_k \in \Sigma_k^*. \qquad (\dagger)$$

Idea: $$\begin{Bmatrix}\text{Arbitrary}\\ \text{automaton}\end{Bmatrix} \longrightarrow \begin{Bmatrix}\text{Synchronising}\\ \text{automaton}\end{Bmatrix} \oplus \begin{Bmatrix}\text{Group}\\ \text{labels}\end{Bmatrix}.$$

Simplifying assumptions:

1. The sequence a is invertible and given by ($\dagger$). $\longrightarrow$ significantly simpler case
2. The map $\chi\colon G \to \mathbb{S}^1 \subset \mathbb{C}$ is a group homomorphism. $\longrightarrow$ Peter–Weyl, $\dim = 1$

Goal: The sequence a is either highly Gowers uniform of all orders or periodic.

Group extensions of automata

Two "extreme" classes of k-automatic sequences:

1. *Synchronising (forwards):* There exists a *synchronising word* $w \in \Sigma_k^*$ such that
$$a(uwv) = a(wv) \text{ for all words } u, v \in \Sigma_k^*.$$
In particular, a is *almost periodic.*
2. *Invertible:* There is a group G, $\lambda\colon \Sigma_k \to G$, $\lambda(0) = \mathrm{id}_G$, and a map $\chi\colon G \to \mathbb{C}$ such that
$$a(n) = \chi\left(\lambda\left(u_l\right) \cdot \lambda\left(u_{l-1}\right) \cdot \dots \cdot \lambda\left(u_0\right)\right) \text{ for } u_l u_{l-1} \dots u_0 = (n)_k \in \Sigma_k^*. \qquad (\dagger)$$

Idea: $$\begin{Bmatrix}\text{Arbitrary}\\ \text{automaton}\end{Bmatrix} \longrightarrow \begin{Bmatrix}\text{Synchronising}\\ \text{automaton}\end{Bmatrix} \oplus \begin{Bmatrix}\text{Group}\\ \text{labels}\end{Bmatrix}.$$

Simplifying assumptions:

1. The sequence a is invertible and given by $(\dagger)$. $\longrightarrow$ significantly simpler case
2. The map $\chi\colon G \to \mathbb{S}^1 \subset \mathbb{C}$ is a group homomorphism. $\longrightarrow$ Peter–Weyl, $\dim = 1$

Goal: The sequence a is either highly Gowers uniform of all orders or periodic.

Group extensions of automata

Definition: A *group extension* $\mathcal{T}$ of an automaton $\mathcal{A} = (S, s_0, \delta)$ (without output) by a group G consists of $\mathcal{A}$ and

- a label function $\lambda \colon S \times \Sigma_k \to G$.

In order to compute a sequence using $\mathcal{T}$:

- extend λ to $S \times \Sigma_k^*$ by $\lambda(s, uv) = \lambda(s, u)\lambda(\delta(s, u), v)$ for $u, v \in \Sigma_k^*$;
- pick an output function τ on $S \times G$ and put $a(n) = \tau\left(\delta(s_0, (n)_k), \lambda(s_0, (n)_k)\right)$.

Example: Rudin-Shapiro sequence

Figure: Automaton

Figure: Group extension

- $G = \{+1, -1\}$
- $\tau(s, g) = g$

Theorem (Müllner (2017)) Each primitive automatic sequence is produced by a group extension of a synchronising automaton.

Group extensions of automata

Definition: A *group extension* $\mathcal{T}$ of an automaton $\mathcal{A} = (S, s_0, \delta)$ (without output) by a group G consists of $\mathcal{A}$ and

- a label function $\lambda \colon S \times \Sigma_k \to G$.

In order to compute a sequence using $\mathcal{T}$:

- extend λ to $S \times \Sigma_k^*$ by $\lambda(s, uv) = \lambda(s,u)\lambda(\delta(s,u), v)$ for $u, v \in \Sigma_k^*$;
- pick an output function τ on $S \times G$ and put $a(n) = \tau\left(\delta(s_0, (n)_k), \lambda(s_0, (n)_k)\right)$.

Example: Rudin-Shapiro sequence

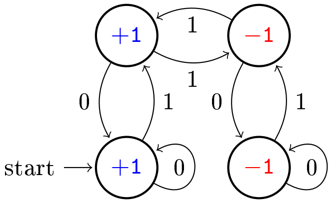


Figure: Automaton

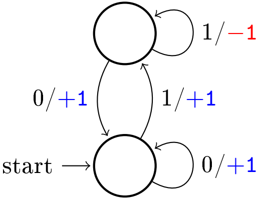


Figure: Group extension

- $G = \{+1, -1\}$
- $\tau(s, g) = g$

Theorem (Müllner (2017)) Each primitive automatic sequence is produced by a group extension of a synchronising automaton.

Group extensions of automata

Definition: A *group extension* $\mathcal{T}$ of an automaton $\mathcal{A} = (S, s_0, \delta)$ (without output) by a group G consists of $\mathcal{A}$ and

- a label function $\lambda\colon S \times \Sigma_k \to G$.

In order to compute a sequence using $\mathcal{T}$:

- extend λ to $S \times \Sigma_k^*$ by $\lambda(s, uv) = \lambda(s,u)\lambda(\delta(s,u), v)$ for $u, v \in \Sigma_k^*$;
- pick an output function τ on $S \times G$ and put $a(n) = \tau\left(\delta(s_0, (n)_k), \lambda(s_0, (n)_k)\right)$.

Example: Rudin-Shapiro sequence

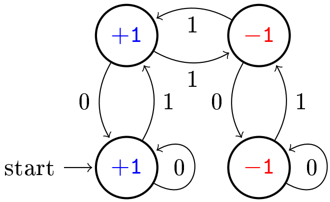


Figure: Automaton

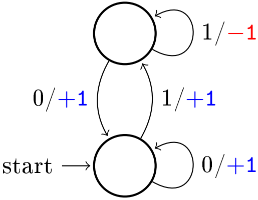


Figure: Group extension

- $G = \{+1, -1\}$
- $\tau(s, g) = g$

Theorem (Müllner (2017)) Each primitive automatic sequence is produced by a group extension of a synchronising automaton.

Recurrence (1/4)

Let us consider the U^2-norm of the Thue–Morse sequence t. Recall that

$$\|f\|_{U^2[N]}^4 = \langle f, f, f, f \rangle_{U^2[N]},$$

where $\langle \cdot \rangle_{U^2[N]}$ is the Gowers product given by

$$\langle f_{00}, f_{10}, f_{01}, f_{11} \rangle_{U^2[N]} = \mathop{\mathbb{E}}_{\mathbf{n} \sim N} f_{00}(n_0) \bar{f}_{10}(n_0 + n_1) \bar{f}_{10}(n_0 + n_2) f_{11}(n_0 + n_1 + n_2).$$

and the average is taken over all $\mathbf{n} = (n_0, n_1, n_2) \in \mathbb{Z}^3$ such that $n_0, n_0 + n_1, n_0 + n_2, n_0 + n_1 + n_2 \in [N] = \{0, 1, \ldots, N-1\}$.

Idea: Write $\mathbf{n} = 2\mathbf{n}' + \mathbf{e}$ with $\mathbf{e} \in \{0,1\}^3$ and replace $\mathop{\mathbb{E}}_{\mathbf{n} \sim N}$ with $\mathop{\mathbb{E}}_{\mathbf{n}' \sim N/2} \mathop{\mathbb{E}}_{\mathbf{e} \in \{0,1\}^3}$.

Basic computation yields:

$$t(n_0 + \omega_1 n_1 + \omega_2 n_2) = t(n_0' + \omega_1 n_1' + \omega_2 n_2' + r_\omega) t(e_0 + \omega_1 e_1 + \omega_2 e_2 \bmod 2),$$

where $r_\omega = r_\omega(e_0, e_1, e_2) = \lfloor (e_0 + \omega_1 e_1 + \omega_2 e_2) / 2 \rfloor$.

Recurrence (1/4)

Let us consider the U^2-norm of the Thue–Morse sequence t. Recall that

$$\|f\|_{U^2[N]}^4 = \langle f, f, f, f \rangle_{U^2[N]},$$

where $\langle \cdot \rangle_{U^2[N]}$ is the Gowers product given by

$$\langle f_{00}, f_{10}, f_{01}, f_{11} \rangle_{U^2[N]} = \mathop{\mathbb{E}}_{\mathbf{n}\sim N} f_{00}(n_0)\bar{f}_{10}(n_0+n_1)\bar{f}_{10}(n_0+n_2)f_{11}(n_0+n_1+n_2).$$

and the average is taken over all $\mathbf{n} = (n_0, n_1, n_2) \in \mathbb{Z}^3$ such that $n_0, n_0+n_1, n_0+n_2, n_0+n_1+n_2 \in [N] = \{0, 1, \ldots, N-1\}$.

Idea: Write $\mathbf{n} = 2\mathbf{n}' + \mathbf{e}$ with $\mathbf{e} \in \{0,1\}^3$ and replace $\mathop{\mathbb{E}}_{\mathbf{n}\sim N}$ with $\mathop{\mathbb{E}}_{\mathbf{n}'\sim N/2} \mathop{\mathbb{E}}_{\mathbf{e}\in\{0,1\}^3}$.

Basic computation yields:

$$t(n_0 + \omega_1 n_1 + \omega_2 n_2) = t(n_0' + \omega_1 n_1' + \omega_2 n_2' + r_\omega)t(e_0 + \omega_1 e_1 + \omega_2 e_2 \bmod 2),$$

where $r_\omega = r_\omega(e_0, e_1, e_2) = \lfloor (e_0 + \omega_1 e_1 + \omega_2 e_2)/2 \rfloor$.

Recurrence (2/4)

We are now ready to compute that:

$$\begin{aligned}\|t\|_{U^2[N]}^4 &= \mathop{\mathbb{E}}_{\mathbf{n}\sim N} t(n_0)t(n_0+n_1)t(n_0+n_2)t(n_0+n_1+n_2) \\ &\simeq \mathop{\mathbb{E}}_{\mathbf{e}\in\{0,1\}^3} t(e_0 \bmod 2)t(e_0+e_1 \bmod 2)t(e_0+e_2 \bmod 2)t(e_0+e_1+e_2 \bmod 2) \\ &\times \mathop{\mathbb{E}}_{\mathbf{n}'\sim N/2} t(n_0'+r_{00})t(n_0'+n_1'+r_{10})t(n_0'+n_2'+r_{01})t(n_0'+n_1'+n_2'+r_{11}) \\ &= \mathop{\mathbb{E}}_{\mathbf{e}\in\{0,1\}^3} \mu(\mathbf{e})\,\langle t_{00}^{\mathbf{e}}, t_{10}^{\mathbf{e}}, t_{01}^{\mathbf{e}}, t_{11}^{\mathbf{e}}\rangle_{U^2[N/2]}\,,\end{aligned}$$

where the last line can be taken as the definition of $\mu(\mathbf{e})$ and $t_\omega^{\mathbf{e}}$ for $\omega\in\{0,1\}^2$.

Iterate ($l \geq 0$ times) and collect:

$$\begin{aligned}\|t\|_{U^2[N]}^4 &\simeq \mathop{\mathbb{E}}_{\mathbf{e}\in[0,2^l)^3} \mu(\mathbf{e})\,\langle t_{00}^{\mathbf{e}}, t_{10}^{\mathbf{e}}, t_{01}^{\mathbf{e}}, t_{11}^{\mathbf{e}}\rangle_{U^2[N/2^l]} \\ &= \sum_{\mathbf{t}} w_l(\mathbf{t})\,\langle t_{00}, t_{10}, t_{01}, t_{11}\rangle_{U^2[N/2^l]}\,,\end{aligned}$$

where $\mathbf{t}=(t_{00},t_{10},t_{01},t_{11})$ and each t_ω, $\omega\in\{0,1\}^2$, is a shift of t.

Recurrence (2/4)

We are now ready to compute that:

$$\begin{aligned}\|t\|_{U^2[N]}^4 &= \mathop{\mathbb{E}}_{\mathbf{n}\sim N} t(n_0)t(n_0+n_1)t(n_0+n_2)t(n_0+n_1+n_2)\\ &\simeq \mathop{\mathbb{E}}_{\mathbf{e}\in\{0,1\}^3} t(e_0 \bmod 2)t(e_0+e_1 \bmod 2)t(e_0+e_2 \bmod 2)t(e_0+e_1+e_2 \bmod 2)\\ &\times \mathop{\mathbb{E}}_{\mathbf{n}'\sim N/2} t(n_0'+r_{00})t(n_0'+n_1'+r_{10})t(n_0'+n_2'+r_{01})t(n_0'+n_1'+n_2'+r_{11})\\ &= \mathop{\mathbb{E}}_{\mathbf{e}\in\{0,1\}^3} \mu(\mathbf{e})\,\langle t_{00}^{\mathbf{e}}, t_{10}^{\mathbf{e}}, t_{01}^{\mathbf{e}}, t_{11}^{\mathbf{e}}\rangle_{U^2[N/2]}\,,\end{aligned}$$

where the last line can be taken as the definition of $\mu(\mathbf{e})$ and $t_\omega^{\mathbf{e}}$ for $\omega \in \{0,1\}^2$.

Iterate ($l \geq 0$ times) and collect:

$$\begin{aligned}\|t\|_{U^2[N]}^4 &\simeq \mathop{\mathbb{E}}_{\mathbf{e}\in[0,2^l)^3} \mu(\mathbf{e})\,\langle t_{00}^{\mathbf{e}}, t_{10}^{\mathbf{e}}, t_{01}^{\mathbf{e}}, t_{11}^{\mathbf{e}}\rangle_{U^2[N/2^l]}\\ &= \sum_{\mathbf{t}} w_l\,(\mathbf{t})\,\langle t_{00}, t_{10}, t_{01}, t_{11}\rangle_{U^2[N/2^l]}\,,\end{aligned}$$

where $\mathbf{t} = (t_{00}, t_{10}, t_{01}, t_{11})$ and each t_ω, $\omega \in \{0,1\}^2$, is a shift of t.

Recurrence (3/4)

Recall: $\|t\|_{U^2[N]}^4 \simeq \sum_{\mathbf{t}} w_l(\mathbf{t}) \langle t_{00}, t_{10}, t_{01}, t_{11} \rangle_{U^2[N/2^l]}$.

Trivial bound: $\sum_{\mathbf{t}} |w_l(\mathbf{t})| \leq 1$. Need: any improvement.

If $\sum_{\mathbf{t}} |w_l(\mathbf{t})| \leq 1 - c$ then $\|t\|_{U^2[N]}^4 \ll (1-c)^{\log N / l \log 2} \ll N^{-c'}$, as claimed.

Non-trivial part of the argument: Find some $l \geq 0$ and $\mathbf{e}, \mathbf{e}' \in [0, 2^l)^3$ such that

- $\mu(\mathbf{e}) = +1$ and $\mu(\mathbf{e}') = -1$;
- $t_\omega^{\mathbf{e}} = t_\omega^{\mathbf{e}'} = t$ for all $\omega \in \{0,1\}^2$.

Recall that in this situation we have

$$\mu(\mathbf{e}) = t(e_0)t(e_0+e_1)t(e_0+e_2)t(e_0+e_1+e_2).$$

For Thue–Morse such $\mathbf{e}$ and $\mathbf{e}'$ can be constructed by an *ad hoc* argument. The key difficulty in generalising to other (invertible) sequences is to deal with this step.

Recurrence (3/4)

Recall: $\|t\|^4_{U^2[N]} \simeq \sum_{\mathbf{t}} w_l(\mathbf{t}) \langle t_{00}, t_{10}, t_{01}, t_{11} \rangle_{U^2[N/2^l]}$.

Trivial bound: $\sum_{\mathbf{t}} |w_l(\mathbf{t})| \leq 1$. Need: any improvement.

If $\sum_{\mathbf{t}} |w_l(\mathbf{t})| \leq 1 - c$ then $\|t\|^4_{U^2[N]} \ll (1-c)^{\log N / l \log 2} \ll N^{-c'}$, as claimed.

Non-trivial part of the argument: Find some $l \geq 0$ and $\mathbf{e}, \mathbf{e}' \in [0, 2^l)^3$ such that

- $\mu(\mathbf{e}) = +1$ and $\mu(\mathbf{e}') = -1$;
- $t^{\mathbf{e}}_\omega = t^{\mathbf{e}'}_\omega = t$ for all $\omega \in \{0,1\}^2$.

Recall that in this situation we have

$$\mu(\mathbf{e}) = t(e_0)t(e_0+e_1)t(e_0+e_2)t(e_0+e_1+e_2).$$

For Thue–Morse such $\mathbf{e}$ and $\mathbf{e}'$ can be constructed by an *ad hoc* argument. The key difficulty in generalising to other (invertible) sequences is to deal with this step.

Recurrence (3/4)

Recall: $\|t\|_{U^2[N]}^4 \simeq \sum_{\mathbf{t}} w_l(\mathbf{t}) \langle t_{00}, t_{10}, t_{01}, t_{11} \rangle_{U^2[N/2^l]}$.

Trivial bound: $\sum_{\mathbf{t}} |w_l(\mathbf{t})| \leq 1$. Need: any improvement.

If $\sum_{\mathbf{t}} |w_l(\mathbf{t})| \leq 1 - c$ then $\|t\|_{U^2[N]}^4 \ll (1-c)^{\log N / l \log 2} \ll N^{-c'}$, as claimed.

Non-trivial part of the argument: Find some $l \geq 0$ and $\mathbf{e}, \mathbf{e}' \in [0, 2^l)^3$ such that

- $\mu(\mathbf{e}) = +1$ and $\mu(\mathbf{e}') = -1$;
- $t_\omega^{\mathbf{e}} = t_\omega^{\mathbf{e}'} = t$ for all $\omega \in \{0,1\}^2$.

Recall that in this situation we have

$$\mu(\mathbf{e}) = t(e_0)t(e_0+e_1)t(e_0+e_2)t(e_0+e_1+e_2).$$

For Thue–Morse such $\mathbf{e}$ and $\mathbf{e}'$ can be constructed by an *ad hoc* argument. The key difficulty in generalising to other (invertible) sequences is to deal with this step.

Recurrence (4/4)

Back to general case: The sequence a is given by $a(n) = \chi(\lambda(n))$,

$$\lambda(n) = \lambda(u_l) \cdot \lambda(u_{l-1}) \cdot \dots \cdot \lambda(u_0) \text{ where } u_l u_{l-1} \dots u_0 = (n)_k \in \Sigma_k^*, \qquad (\dagger)$$

and $\chi \colon G \to \mathbb{C}$ is a homomorphism. Again, we have recurrence:

$$\|a\|_{U^2[N]}^4 \simeq \mathop{\mathbb{E}}_{\mathbf{e} \in [0,k^l)^3} \mu(\mathbf{e}) \langle a_{00}^{\mathbf{e}}, a_{10}^{\mathbf{e}}, a_{01}^{\mathbf{e}}, a_{11}^{\mathbf{e}} \rangle_{U^2[N/2^l]},$$

where $a_\omega^{\mathbf{e}}$ are shifts of a. If $\mathbf{e}$ is such that $a_\omega^{\mathbf{e}} = a$ for all $\omega \in \{0,1\}^2$ then

$$\mu(\mathbf{e}) = \prod_{\omega \in \{0,1\}^2} \chi(\lambda(e_0 + \omega_1 e_1 + \omega_2 e_2)).$$

We want to find $\mathbf{e}^{(0)}, \mathbf{e}^{(1)}, \dots, \mathbf{e}^{(m-1)} \in [0, k^l)^3$ such that $\sum_{j=0}^{m-1} \mu(\mathbf{e}^{(j)}) = 0$.

Key construction: the "cube group" $\mathcal{Q}^{[2]} \subset G^4$,

$$\mathcal{Q}^{[2]} = \mathcal{Q}^{[2]}(G, \lambda) := \left\{ \Big(\lambda(e_0 + \omega_1 e_1 + \omega_2 e_2) \Big)_{\omega \in \{0,1\}^2} \in G^4 \;:\; \mathbf{e} \in \mathbb{N}^3 \right\}.$$

Fact: $\mathcal{Q}^{[2]}$ is a group. The rest of the argument hinges on describing $\mathcal{Q}^{[2]}$.

Recurrence (4/4)

Back to general case: The sequence a is given by $a(n) = \chi(\lambda(n))$,

$$\lambda(n) = \lambda(u_l) \cdot \lambda(u_{l-1}) \cdot \dots \cdot \lambda(u_0) \text{ where } u_l u_{l-1} \dots u_0 = (n)_k \in \Sigma_k^*, \qquad (\dagger)$$

and $\chi\colon G \to \mathbb{C}$ is a homomorphism. Again, we have recurrence:

$$\|a\|_{U^2[N]}^4 \simeq \mathop{\mathbb{E}}_{\mathbf{e} \in [0,k^l)^3} \mu(\mathbf{e}) \left\langle a_{00}^{\mathbf{e}}, a_{10}^{\mathbf{e}}, a_{01}^{\mathbf{e}}, a_{11}^{\mathbf{e}} \right\rangle_{U^2[N/2^l]},$$

where $a_\omega^{\mathbf{e}}$ are shifts of a. If $\mathbf{e}$ is such that $a_\omega^{\mathbf{e}} = a$ for all $\omega \in \{0,1\}^2$ then

$$\mu(\mathbf{e}) = \prod_{\omega \in \{0,1\}^2} \chi(\lambda(e_0 + \omega_1 e_1 + \omega_2 e_2)).$$

We want to find $\mathbf{e}^{(0)}, \mathbf{e}^{(1)}, \dots, \mathbf{e}^{(m-1)} \in [0, k^l)^3$ such that $\sum_{j=0}^{m-1} \mu(\mathbf{e}^{(j)}) = 0$.

Key construction: the "cube group" $\mathcal{Q}^{[2]} \subset G^4$,

$$\mathcal{Q}^{[2]} = \mathcal{Q}^{[2]}(G, \lambda) := \left\{ \Big(\lambda(e_0 + \omega_1 e_1 + \omega_2 e_2) \Big)_{\omega \in \{0,1\}^2} \in G^4 \;:\; \mathbf{e} \in \mathbb{N}^3 \right\}.$$

Fact: $\mathcal{Q}^{[2]}$ is a group. The rest of the argument hinges on describing $\mathcal{Q}^{[2]}$.

Cube groups

Host–Kra cube groups: groups generated by “upper faces”:

$$\mathrm{HK}^{[2]}(G) = \langle (g,g,g,g), (\mathrm{id},\mathrm{id},g,g), (\mathrm{id},g,\mathrm{id},g) \ : \ g \in G \rangle < G^4.$$

We may freely assume that $\lambda(1), \ldots, \lambda(k-1)$ generate G. Then $\mathrm{HK}^{[2]}(G) \subset \mathcal{Q}^{[2]}$.

Example

Let $G = \mathbb{Z}/m\mathbb{Z}$ $m \mid k-1$ and $\lambda(i) = i$ for all $i \in \Sigma_k$. Then

$$\mathrm{HK}^{[2]}(G) = \mathcal{Q}^{[2]}(G,\lambda).$$

Definition: A pair (H,κ) (where H is a group and $\kappa\colon \Sigma_k \to H$, $\kappa(0) = \mathrm{id}_H$) is a *factor* of (G,λ) if there exists a *factor map* $\pi\colon H \to G$ such that

- π is a group epimorphism;
- $\kappa = \pi \circ \lambda$.

We always have the inclusion $\pi^{[2]}\left(Q^{[2]}(G,\lambda)\right) \subseteq \mathcal{Q}^{[2]}(H,\kappa)$.

We call (H,κ) *characteristic* if $Q^{[2]}(G,\lambda) = \left(\pi^{[2]}\right)^{-1}\left(\mathcal{Q}^{[2]}(H,\kappa)\right)$.

Goal: Find a characteristic factor of the form $(\mathbb{Z}/m\mathbb{Z}, \mathrm{id})$.

Cube groups

Host–Kra cube groups: groups generated by "upper faces":

$$\mathrm{HK}^{[2]}(G) = \langle (g,g,g,g), (\mathrm{id},\mathrm{id},g,g), (\mathrm{id},g,\mathrm{id},g) \ : \ g \in G \rangle < G^4.$$

We may freely assume that $\lambda(1), \ldots, \lambda(k-1)$ generate G. Then $\mathrm{HK}^{[2]}(G) \subset \mathcal{Q}^{[2]}$.

Example

Let $G = \mathbb{Z}/m\mathbb{Z}$ $m \mid k-1$ and $\lambda(i) = i$ for all $i \in \Sigma_k$. Then

$$\mathrm{HK}^{[2]}(G) = \mathcal{Q}^{[2]}(G, \lambda).$$

Definition: A pair (H, κ) (where H is a group and $\kappa \colon \Sigma_k \to H$, $\kappa(0) = \mathrm{id}_H$) is a *factor* of (G, λ) if there exists a *factor map* $\pi \colon H \to G$ such that

- π is a group epimorphism;
- $\kappa = \pi \circ \lambda$.

We always have the inclusion $\pi^{[2]}\left(Q^{[2]}(G,\lambda)\right) \subseteq \mathcal{Q}^{[2]}(H,\kappa)$.

We call (H,κ) *characteristic* if $Q^{[2]}(G,\lambda) = \left(\pi^{[2]}\right)^{-1}\left(\mathcal{Q}^{[2]}(H,\kappa)\right)$.

Goal: Find a characteristic factor of the form $(\mathbb{Z}/m\mathbb{Z}, \mathrm{id})$.

Cube groups

Host–Kra cube groups: groups generated by "upper faces":

$$\mathrm{HK}^{[2]}(G) = \langle (g,g,g,g), (\mathrm{id},\mathrm{id},g,g), (\mathrm{id},g,\mathrm{id},g) \ : \ g \in G \rangle < G^4.$$

We may freely assume that $\lambda(1), \ldots, \lambda(k-1)$ generate G. Then $\mathrm{HK}^{[2]}(G) \subset \mathcal{Q}^{[2]}$.

Example

Let $G = \mathbb{Z}/m\mathbb{Z}$ $m \mid k-1$ and $\lambda(i) = i$ for all $i \in \Sigma_k$. Then

$$\mathrm{HK}^{[2]}(G) = \mathcal{Q}^{[2]}(G, \lambda).$$

Definition: A pair (H, κ) (where H is a group and $\kappa \colon \Sigma_k \to H$, $\kappa(0) = \mathrm{id}_H$) is a *factor* of (G, λ) if there exists a *factor map* $\pi \colon H \to G$ such that

- π is a group epimorphism;
- $\kappa = \pi \circ \lambda$.

We always have the inclusion $\pi^{[2]}\left(Q^{[2]}(G,\lambda)\right) \subseteq \mathcal{Q}^{[2]}(H,\kappa)$.

We call (H, κ) *characteristic* if $Q^{[2]}(G,\lambda) = \left(\pi^{[2]}\right)^{-1}\left(\mathcal{Q}^{[2]}(H,\kappa)\right)$.

Goal: Find a characteristic factor of the form $(\mathbb{Z}/m\mathbb{Z}, \mathrm{id})$.

Characteristic factors

Lemma

There is a maximal normal subgroup $K < G$ such that the factor $(G/K, \bar{\lambda})$ is characteristic. It is the group generated by $h \in G$ such that $(h, \mathrm{id}_G, \mathrm{id}_G, \mathrm{id}_G) \in \mathcal{Q}^{[2]}$.

- Let $r = |G|$, and let $n \in \mathbb{N}$ be arbitrary. *For notational clarity, suppose $k = 10$.*
- Put $e_0 = 10^{2r}n + 1$, $e_1 = 10^{2r} - 10^r$, $e_2 = 10^r - 1$.
- We can compute the group labels:

$$\lambda(e_0) = \lambda((n)_{10}\underbrace{0\dots00}_{r}\underbrace{0\dots01}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0+e_1) = \lambda((n)_{10}\underbrace{9\dots99}_{r}\underbrace{0\dots01}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0+e_2) = \lambda((n)_{10}\underbrace{0\dots01}_{r}\underbrace{0\dots00}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0+e_1+e_2) = \lambda((n+1)_{10}\underbrace{0\dots00}_{r}\underbrace{0\dots00}_{r}) = \lambda(n+1).$$

- As a consequence, $\lambda(n+1)(\lambda(n)\lambda(1))^{-1} \in K$ and by induction: $\lambda(n)\lambda(1)^{-n} \in K$.
- This means that $G/K = \mathbb{Z}/m\mathbb{Z}$ and $\bar{\lambda}(n) = n \bmod m$, as needed.

Characteristic factors

Lemma

There is a maximal normal subgroup $K < G$ such that the factor $(G/K, \bar{\lambda})$ is characteristic. It is the group generated by $h \in G$ such that $(h, \mathrm{id}_G, \mathrm{id}_G, \mathrm{id}_G) \in \mathcal{Q}^{[2]}$.

- Let $r = |G|$, and let $n \in \mathbb{N}$ be arbitrary. *For notational clarity, suppose* $k = 10$.
- Put $e_0 = 10^{2r} n + 1$, $e_1 = 10^{2r} - 10^r$, $e_2 = 10^r - 1$.
- We can compute the group labels:

$$\lambda(e_0) = \lambda((n)_{10} \underbrace{0\dots00}_{r}\underbrace{0\dots01}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0 + e_1) = \lambda((n)_{10} \underbrace{9\dots99}_{r}\underbrace{0\dots01}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0 + e_2) = \lambda((n)_{10} \underbrace{0\dots01}_{r}\underbrace{0\dots00}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0 + e_1 + e_2) = \lambda((n+1)_{10} \underbrace{0\dots00}_{r}\underbrace{0\dots00}_{r}) = \lambda(n+1).$$

- As a consequence, $\lambda(n+1)(\lambda(n)\lambda(1))^{-1} \in K$ and by induction: $\lambda(n)\lambda(1)^{-n} \in K$.
- This means that $G/K = \mathbb{Z}/m\mathbb{Z}$ and $\bar{\lambda}(n) = n \bmod m$, as needed.

Characteristic factors

Lemma

There is a maximal normal subgroup $K < G$ such that the factor $(G/K, \bar{\lambda})$ is characteristic. It is the group generated by $h \in G$ such that $(h, \mathrm{id}_G, \mathrm{id}_G, \mathrm{id}_G) \in \mathcal{Q}^{[2]}$.

- Let $r = |G|$, and let $n \in \mathbb{N}$ be arbitrary. *For notational clarity, suppose $k = 10$.*
- Put $e_0 = 10^{2r} n + 1$, $e_1 = 10^{2r} - 10^r$, $e_2 = 10^r - 1$.
- We can compute the group labels:

$$\lambda(e_0) = \lambda((n)_{10}\underbrace{0\dots00}_{r}\underbrace{0\dots01}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0+e_1) = \lambda((n)_{10}\underbrace{9\dots99}_{r}\underbrace{0\dots01}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0+e_2) = \lambda((n)_{10}\underbrace{0\dots01}_{r}\underbrace{0\dots00}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0+e_1+e_2) = \lambda((n+1)_{10}\underbrace{0\dots00}_{r}\underbrace{0\dots00}_{r}) = \lambda(n+1).$$

- As a consequence, $\lambda(n+1)(\lambda(n)\lambda(1))^{-1} \in K$ and by induction: $\lambda(n)\lambda(1)^{-n} \in K$.
- This means that $G/K = \mathbb{Z}/m\mathbb{Z}$ and $\bar{\lambda}(n) = n \bmod m$, as needed.

Characteristic factors

Lemma

There is a maximal normal subgroup $K < G$ such that the factor $(G/K, \bar{\lambda})$ is characteristic. It is the group generated by $h \in G$ such that $(h, \mathrm{id}_G, \mathrm{id}_G, \mathrm{id}_G) \in \mathcal{Q}^{[2]}$.

- Let $r = |G|$, and let $n \in \mathbb{N}$ be arbitrary. *For notational clarity, suppose* $k = 10$.
- Put $e_0 = 10^{2r}n + 1$, $e_1 = 10^{2r} - 10^r$, $e_2 = 10^r - 1$.
- We can compute the group labels:

$$\lambda(e_0) = \lambda((n)_{10}\underbrace{0\ldots00}_{r}\underbrace{0\ldots01}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0 + e_1) = \lambda((n)_{10}\underbrace{9\ldots99}_{r}\underbrace{0\ldots01}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0 + e_2) = \lambda((n)_{10}\underbrace{0\ldots01}_{r}\underbrace{0\ldots00}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0 + e_1 + e_2) = \lambda((n+1)_{10}\underbrace{0\ldots00}_{r}\underbrace{0\ldots00}_{r}) = \lambda(n+1).$$

- As a consequence, $\lambda(n+1)(\lambda(n)\lambda(1))^{-1} \in K$ and by induction: $\lambda(n)\lambda(1)^{-n} \in K$.
- This means that $G/K = \mathbb{Z}/m\mathbb{Z}$ and $\bar{\lambda}(n) = n \bmod m$, as needed.

Characteristic factors

Lemma

There is a maximal normal subgroup $K < G$ such that the factor $(G/K, \bar{\lambda})$ is characteristic. It is the group generated by $h \in G$ such that $(h, \mathrm{id}_G, \mathrm{id}_G, \mathrm{id}_G) \in \mathcal{Q}^{[2]}$.

- Let $r = |G|$, and let $n \in \mathbb{N}$ be arbitrary. *For notational clarity, suppose* $k = 10$.
- Put $e_0 = 10^{2r}n + 1$, $e_1 = 10^{2r} - 10^r$, $e_2 = 10^r - 1$.
- We can compute the group labels:

$$\lambda(e_0) = \lambda((n)_{10}\underbrace{0\ldots00}_{r}\underbrace{0\ldots01}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0 + e_1) = \lambda((n)_{10}\underbrace{9\ldots99}_{r}\underbrace{0\ldots01}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0 + e_2) = \lambda((n)_{10}\underbrace{0\ldots01}_{r}\underbrace{0\ldots00}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0 + e_1 + e_2) = \lambda((n+1)_{10}\underbrace{0\ldots00}_{r}\underbrace{0\ldots00}_{r}) = \lambda(n+1).$$

- As a consequence, $\lambda(n+1)(\lambda(n)\lambda(1))^{-1} \in K$ and by induction: $\lambda(n)\lambda(1)^{-n} \in K$.
- This means that $G/K = \mathbb{Z}/m\mathbb{Z}$ and $\bar{\lambda}(n) = n \bmod m$, as needed.

Characteristic factors

Lemma

There is a maximal normal subgroup $K < G$ such that the factor $(G/K, \bar{\lambda})$ is characteristic. It is the group generated by $h \in G$ such that $(h, \mathrm{id}_G, \mathrm{id}_G, \mathrm{id}_G) \in \mathcal{Q}^{[2]}$.

- Let $r = |G|$, and let $n \in \mathbb{N}$ be arbitrary. *For notational clarity, suppose $k = 10$.*
- Put $e_0 = 10^{2r}n + 1$, $e_1 = 10^{2r} - 10^r$, $e_2 = 10^r - 1$.
- We can compute the group labels:

$$\lambda(e_0) = \lambda((n)_{10}\underbrace{0\ldots00}_{r}\underbrace{0\ldots01}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0 + e_1) = \lambda((n)_{10}\underbrace{9\ldots99}_{r}\underbrace{0\ldots01}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0 + e_2) = \lambda((n)_{10}\underbrace{0\ldots01}_{r}\underbrace{0\ldots00}_{r}) = \lambda(n)\lambda(1)$$

$$\lambda(e_0 + e_1 + e_2) = \lambda((n+1)_{10}\underbrace{0\ldots00}_{r}\underbrace{0\ldots00}_{r}) = \lambda(n+1).$$

- As a consequence, $\lambda(n+1)(\lambda(n)\lambda(1))^{-1} \in K$ and by induction: $\lambda(n)\lambda(1)^{-n} \in K$.
- This means that $G/K = \mathbb{Z}/m\mathbb{Z}$ and $\bar{\lambda}(n) = n \bmod m$, as needed.

Thank you for your attention!