Gelfond Problems on the Sum-of-digits Function and Subsequences of Automatic Sequences

Michael Drmota

Institut für Diskrete Mathematik und Geometrie
Technische Universität Wien

Erdős Centennial
Budapest, July 1–5, 2013

MAGYAR TUDOMÁNYOS AKADÉMIA
MATEMATIKAI KUTATÓ INTÉZETE

Budapest V., Reáltanoda u. 13—15.
Tel.: 182-875*
182-399*

MATHEMATICAL INSTITUTE OF THE
HUNGARIAN ACADEMY OF SCIENCES
Postal address:
Budapest, P.O.B. 127, H-1364
Tel.: 173-050
173-151

1990 VIII 12

Sehr geehrter Herr Dr Drmota,

Vielen Dank für Ihre lange und interessante Arbeit. Vielleicht kennen Sie folgendes alte Problem (Ich stellte die Frage in 1931!) Es sei

$$1 \le a_1 < a_2 < \dots < a_k \le n, \quad k \text{ maximal}$$

Die Summen $\sum_{i=1}^{k} \varepsilon_i a_i$ seien alle verschieden, $\varepsilon_i = 0$ oder 1 ($a_i = 2^i$ ist eine Lösung). Ist es aber wahr dass

$$k < \frac{\log n}{\log 2} + c$$

ist? Vielleicht ist $c = 3$.

Eine andere Frage: $f(n)$ sei multiplicativ, $f(n) = \pm 1$,

$$\sum_{f(p)=-1} \frac{1}{p} = \infty$$

(also ist $f(p) = -1$ ziemlich oft (p Primzahl)).

Ist es wahr dass $\sum_{n=1}^{x} f(n)$ unendlich oft 0 ist ($\overline{\lim} = +\infty$, $\underline{\lim} = -\infty$) wenn falsch genügt vielleicht

$$\sum_{\substack{f(p)=-1 \\ p<x}} 1 > c\,x/\log x \; ?$$

Es sei $1 < a_1 < a_2 < \dots < a_k \le n$, $[a_i, a_j] > n$, (also keine Zahl $m \le n$ ist ein vielfaches von 2 der a_i). Ist es wahr dass für $n > n_0$ $\sum \frac{1}{a_i} < 1$ ist? Wieviel Zahlen $\le n$ muss es geben die durch keine der a_i teilbar ist? $c\sqrt{n}$ ist trivial vielleicht gilt εn.

(Schinzel-Szekeres Sur un problème de Paul Erdős, Acta Szeged etwa 1960

Viele Grüsse
Ihr Paul Erdős

88896 Fnyv 11. — R 222

Summary

- ★ Binary Expansion of Primes
- ★ Thue-Morse sequence
- ★ Gelfond problems
- ★ Generalized Thue-Morse sequence and uniform distribution
- ★ Automatic sequences
- ★ Generalized Thue-Morse sequence of squares
- ★ The sum-of-digits function of polynomial values
- ★ The sum-of-digits function of primes

★ Binary Representation of Primes

2 extremal cases

$p = 2^k + 1$ Fermat prime ($k = 2^m$)

$p = 2^k + 2^{k-1} + \cdots + 2 + 1$ Mersenne prime ($k + 1 \in \mathbb{P}$)

★ Binary Representation of Primes

2 extremal cases

$p = 2^k + 1$ Fermat prime ($k = 2^m$)

$p = 2^k + 2^{k-1} + \cdots + 2 + 1$ Mersenne prime ($k + 1 \in \mathbb{P}$)

Question on the number of digits of primes (related to Bourgain and Green)

Given k, does there exist a prime p and $0 = j_1 < j_2 < \cdots < j_k$ with

$$p = 2^{j_1} + 2^{j_2} + \cdots + 2^{j_k} \text{ ??}$$

(This is equivalent to $s_2(p) = k$.)

★ Binary Representation of Primes

Answer for large k

Theorem (D., Mauduit, Rivat (2011))

$s_2(n)$ ... *number of powers of 2 in the binary expansion of* n

$$\#\{primes\ p < 2^{2k} : s_2(p) = k\} \sim \frac{2^{2k}}{\sqrt{2\pi}\log 2\, k^{\frac{3}{2}}}$$

★ Binary Representation of Primes

Answer for large k

Theorem (D., Mauduit, Rivat (2011))

$s_2(n)$ ... *number of powers of 2 in the binary expansion of n*

$$\#\{primes\ p < 2^{2k} : s_2(p) = k\} \sim \frac{2^{2k}}{\sqrt{2\pi}\log 2\, k^{\frac{3}{2}}}$$

Unfortunately this does not give a proper answer for $k = 2$ or $k = \lfloor \log_2 p \rfloor$.

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n \geqslant 0}$:

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n \geqslant 0}$:

0

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

01

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

0110

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n \geqslant 0}$:

01101001

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

$$0110100110010110$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

01101001100101101001011001101001

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n \geqslant 0}$:

$$01101001100101101001011001101001100101100 1101 \cdots$$

$$t_0 = 0, \qquad t_{2^n+k} = 1 - t_k \quad (0 \leqslant k < 2^n)$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n \geqslant 0}$:

$$0110100110010110100101100110100110010110 01101 \cdots$$

$$t_0 = 0, \qquad t_{2^n+k} = 1 - t_k \quad (0 \leqslant k < 2^n)$$

$$\boxed{t_n = s_2(n) \bmod 2}$$

$$n = \sum_{i=0}^{\ell-1} \varepsilon_i(n) q^i \qquad \varepsilon_i(n) \in \{0, 1, \ldots, q-1\}, \qquad s_q(n) = \sum_{i=0}^{\ell-1} \varepsilon_i(n)$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

$$011010011001011010010110011010011001011001101\cdots$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n \geqslant 0}$:

$$01\,1010011001011010010110011010011001011001101 \cdots$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

$$0110100110010110100101100110100110010110011010 \cdots$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

$$0110100110010110100101100110100110010110011010\cdots$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

$$0110100110010110100101100110100110010110011 01\cdots$$

$$\#\{0\leqslant n<N : t_n=0\}\sim\frac{N}{2}$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

$$0110100110010110100101100110100110010110011010 \cdots$$

$$\#\{0 \leqslant n < N : t_n = 0\} \sim \frac{N}{2}$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n \geqslant 0}$:

$$0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad \cdots$$

$$\# \{0 \leqslant n < N : t_n = 0\} \sim \frac{N}{2}$$

$$\# \{0 \leqslant n < N : t_{3n} = 0\} \sim \frac{N}{2}$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

$$011010011001011010010110011010011001011001101\cdots$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n \geqslant 0}$:

$$011010011001011010010110011010011001011001101 \cdots$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n \geqslant 0}$:

$$10\ 0\ 1\quad 1\ 1\quad 0\ 1\quad 0\quad\quad 0\ 1\quad\quad 1\quad 1\ 0\ \cdots$$

Mauduit and Rivat (2010):

$$\#\{0 \leqslant p < N : t_p = 0\} \sim \frac{\pi(N)}{2}$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

$$011010011001011010010110011010011001011001101\cdots$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

$$011010011001011010010110011010011001011001101\cdots$$

★ Thue-Morse sequence

Thue-Morse sequence $(t_n)_{n\geqslant 0}$:

$$01 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad \cdots$$

Mauduit and Rivat (2009):

$$\#\{0 \leqslant n < N : t_{n^2} = 0\} \sim \frac{N}{2}$$

★ Gelfond Problems

Gelfond 1967/1968

a, m ... positive integers, b, ℓ ... non-neg. integer, $(m, q-1) = 1$.

$$\Longrightarrow \quad \boxed{\#\{n < N : \ s_q(an+b) \equiv \ell \bmod m\} = \frac{N}{m} + O(N^\lambda)}$$

with $0 < \lambda < 1$.

★ Gelfond Problems

Gelfond 1967/1968

a, m ... positive integers, b, ℓ ... non-neg. integer, $(m, q-1) = 1$.

$$\Longrightarrow \quad \boxed{\#\{n < N : \; s_q(an+b) \equiv \ell \bmod m\} = \frac{N}{m} + O(N^\lambda)}$$

with $0 < \lambda < 1$.

In particular:

$$\begin{aligned} \#\{n < N : t_{an+b} = 0\} &= \#\{n < N : s_2(an+b) \equiv 0 \bmod 2\} \\ &= \frac{N}{2} + O(N^\lambda) \end{aligned}$$

★ Gelfond Problems

1. $q_1, q_2, \ldots, q_d \geqslant 2$, $(q_i, q_j) = 1$ for $i \ne j$, $(m_j, q_j - 1) = 1$:

$$\#\{n < N : s_{q_j}(n) \equiv \ell_j \bmod m_j,\ 1 \leqslant j \leqslant d\} = \frac{N}{m_1 \cdots m_d} + O(N^{1-\eta})$$

★ Gelfond Problems

1. $q_1, q_2, \ldots, q_d \geqslant 2$, $(q_i, q_j) = 1$ for $i \ne j$, $(m_j, q_j - 1) = 1$: Kim 1999

$$\#\{n < N : s_{q_j}(n) \equiv \ell_j \bmod m_j,\ 1 \leqslant j \leqslant d\} = \frac{N}{m_1 \cdots m_d} + O(N^{1-\eta})$$

★ Gelfond Problems

1. $q_1, q_2, \ldots, q_d \geqslant 2$, $(q_i, q_j) = 1$ for $i \neq j$, $(m_j, q_j - 1) = 1$: Kim 1999

$$\#\{n < N : s_{q_j}(n) \equiv \ell_j \bmod m_j,\ 1 \leqslant j \leqslant d\} = \frac{N}{m_1 \cdots m_d} + O(N^{1-\eta})$$

2. $(m, q-1) = 1$:

$$\#\{\text{primes } p < N : s_q(p) \equiv \ell \bmod m\} = \frac{\pi(N)}{m} + O(N^{1-\eta})$$

★ Gelfond Problems

1. $q_1, q_2, \ldots, q_d \geqslant 2$, $(q_i, q_j) = 1$ for $i \ne j$, $(m_j, q_j - 1) = 1$: Kim 1999

$$\#\{n < N : s_{q_j}(n) \equiv \ell_j \bmod m_j,\ 1 \leqslant j \leqslant d\} = \frac{N}{m_1 \cdots m_d} + O(N^{1-\eta})$$

2. $(m, q - 1) = 1$: Mauduit, Rivat 2010

$$\#\{\text{primes } p < N : s_q(p) \equiv \ell \bmod m\} = \frac{\pi(N)}{m} + O(N^{1-\eta})$$

★ Gelfond Problems

1. $q_1, q_2, \ldots, q_d \geqslant 2$, $(q_i, q_j) = 1$ for $i \neq j$, $(m_j, q_j - 1) = 1$: Kim 1999

$$\#\{n < N : s_{q_j}(n) \equiv \ell_j \bmod m_j,\ 1 \leqslant j \leqslant d\} = \frac{N}{m_1 \cdots m_d} + O(N^{1-\eta})$$

2. $(m, q - 1) = 1$: Mauduit, Rivat 2010

$$\#\{\text{primes } p < N : s_q(p) \equiv \ell \bmod m\} = \frac{\pi(N)}{m} + O(N^{1-\eta})$$

3. $(m, q - 1) = 1$, $P(x) \in \mathbb{N}[x]$:

$$\#\{n < N : s_q(P(n)) \equiv \ell \bmod m\} = \frac{N}{m} + O(N^{1-\eta})$$

★ Gelfond Problems

1. $q_1, q_2, \ldots, q_d \geqslant 2$, $(q_i, q_j) = 1$ for $i \neq j$, $(m_j, q_j - 1) = 1$: Kim 1999

$$\#\{n < N : s_{q_j}(n) \equiv \ell_j \bmod m_j,\ 1 \leqslant j \leqslant d\} = \frac{N}{m_1 \cdots m_d} + O(N^{1-\eta})$$

2. $(m, q-1) = 1$: Mauduit, Rivat 2010

$$\#\{\text{primes } p < N : s_q(p) \equiv \ell \bmod m\} = \frac{\pi(N)}{m} + O(N^{1-\eta})$$

3. $(m, q-1) = 1$, $P(x) \in \mathbb{N}[x]$: Mauduit, Rivat 2009 for $P(x) = x^2$

$$\#\{n < N : s_q(P(n)) \equiv \ell \bmod m\} = \frac{N}{m} + O(N^{1-\eta})$$

★ Gelfond Problems

1. $q_1, q_2, \ldots, q_d \geqslant 2$, $(q_i, q_j) = 1$ for $i \neq j$, $(m_j, q_j - 1) = 1$: Kim 1999

$$\#\{n < N : s_{q_j}(n) \equiv \ell_j \bmod m_j,\ 1 \leqslant j \leqslant d\} = \frac{N}{m_1 \cdots m_d} + O(N^{1-\eta})$$

2. $(m, q-1) = 1$: Mauduit, Rivat 2010

$$\#\{\text{primes } p < N : s_q(p) \equiv \ell \bmod m\} = \frac{\pi(N)}{m} + O(N^{1-\eta})$$

3. $(m, q-1) = 1$, $P(x) \in \mathbb{N}[x]$: Mauduit, Rivat 2009 for $P(x) = x^2$
Drmota, Mauduit, Rivat 2011 for **large bases** $q \geqslant q_0(\deg(P))$

$$\#\{n < N : s_q(P(n)) \equiv \ell \bmod m\} = \frac{N}{m} + O(N^{1-\eta})$$

★ Generalized Thue-Morse sequences

- H ... compact (Hausdorff) group
- $q \geqslant 2$ and $g_0, g_1, \ldots, g_{q-1} \in H$ with $g_0 = e$ (identity element)
- $G \leqslant H$ ... closure of the subgroup generated by $g_0, g_1, \ldots, g_{q-1}$

★ Generalized Thue-Morse sequences

- H ... compact (Hausdorff) group
- $q \geqslant 2$ and $g_0, g_1, \ldots, g_{q-1} \in H$ with $g_0 = e$ (identity element)
- $G \leqslant H$ ... closure of the subgroup generated by $g_0, g_1, \ldots, g_{q-1}$

$$n = \sum_{i=0}^{\ell-1} \varepsilon_i(n) q^i$$

★ Generalized Thue-Morse sequences

- H ... compact (Hausdorff) group
- $q \geqslant 2$ and $g_0, g_1, \ldots, g_{q-1} \in H$ with $g_0 = e$ (identity element)
- $G \leqslant H$ ... closure of the subgroup generated by $g_0, g_1, \ldots, g_{q-1}$

$$n = \sum_{i=0}^{\ell-1} \varepsilon_i(n) q^i$$

Generalized Thue-Morse sequence:

$$\boxed{T(n) := g_{\varepsilon_0(n)} g_{\varepsilon_1(n)} \cdots g_{\varepsilon_{\ell-1}(n)}}$$

★ Generalized Thue-Morse sequences

- H ... compact (Hausdorff) group
- $q \geqslant 2$ and $g_0, g_1, \ldots, g_{q-1} \in H$ with $g_0 = e$ (identity element)
- $G \leqslant H$ ... closure of the subgroup generated by $g_0, g_1, \ldots, g_{q-1}$

$$n = \sum_{i=0}^{\ell-1} \varepsilon_i(n) q^i$$

q-multiplicative function:

$$\boxed{T(j + qn) = g_j T(n) = T(j)T(n)} \qquad 0 \leqslant j < q$$

★ Generalized Thue-Morse sequences

Examples

- $H = \langle \mathbb{Z}/2\mathbb{Z}, +\rangle$, $q = 2$, $g_0 = 0$, $g_1 = 1$:

$$\boxed{T(n) = s_2(n) \bmod 2 = t_n}.$$

★ Generalized Thue-Morse sequences

Examples

- $H = \langle \mathbb{Z}/2\mathbb{Z}, +\rangle$, $q = 2$, $g_0 = 0$, $g_1 = 1$:

$$\boxed{T(n) = s_2(n) \bmod 2 = t_n}.$$

- $H = \langle \mathbb{Z}/m\mathbb{Z}, +\rangle$, $g_j = j$ $(0 \leqslant j < q)$:

$$\boxed{T(n) = s_q(n) \bmod m}.$$

★ Generalized Thue-Morse sequences

Examples

- $H = \langle \mathbb{Z}/2\mathbb{Z}, + \rangle$, $q = 2$, $g_0 = 0$, $g_1 = 1$:

$$\boxed{T(n) = s_2(n) \bmod 2 = t_n}.$$

- $H = \langle \mathbb{Z}/m\mathbb{Z}, + \rangle$, $g_j = j$ $(0 \leqslant j < q)$:

$$\boxed{T(n) = s_q(n) \bmod m}.$$

- $H = \langle \mathbb{R}/\mathbb{Z}, + \rangle$, $g_j = \alpha j$ $(0 \leqslant j < q)$:

$$\boxed{T(n) = \alpha\, s_q(n) \bmod 1}.$$

★ Generalized Thue-Morse sequences

Theorem

Let μ denote the Haar measure of G. Then $(T(n))_{n\geqslant 0}$ is μ-uniformly distributed in G, that is,

$$\frac{1}{N}\sum_{n=0}^{N-1}\delta_{T(n)} \to \mu.$$

★ Generalized Thue-Morse sequences

Theorem

Let μ denote the Haar measure of G. Then $(T(n))_{n\geqslant 0}$ is μ-uniformly distributed in G, that is,

$$\frac{1}{N}\sum_{n=0}^{N-1} f(T(n)) \to \int_G f\,\mathrm{d}\mu$$

(for all continuous functions $f : G \to \mathbb{R}$.)

★ Generalized Thue-Morse sequences

Theorem

Let μ denote the Haar measure of G. Then $(T(n))_{n \geqslant 0}$ is μ-uniformly distributed in G, that is,

$$\frac{1}{N} \sum_{n=0}^{N-1} f(T(n)) \to \int_G f \, \mathrm{d}\mu$$

(for all continuous functions $f : G \to \mathbb{R}$.)

Remark. Equivalently, a sequence (x_n) in G is μ-uniformly distributed if

$$\frac{1}{N} \left|\{n < N : x_n \in B\}\right| \to \mu(B)$$

holds for all μ-measurable sets $B \subseteq G$ with $\mu(\partial B) = 0$.

★ Generalized Thue-Morse sequences and Gelfond's 1st problem

Theorem

Let $q_1, \ldots, q_d \geqslant 2$, $(q_i, q_j) = 1$ *for* $i \neq j$ *and* $T_j(n)$, $1 \leqslant j \leqslant d$, *generalized Thue-Morse sequences with respect to* q_j *on groups* G_j *(with Haar measure* μ_j*).*
Then $(T_1(n), \ldots, T_d(n))$ *is* μ*-uniformly distributed in* $G = G_1 \times \cdots \times G_d$, *where* μ *denotes the product measure on* G*:*

$$\frac{1}{N} \sum_{n=0}^{N-1} \delta_{(T_1(n),\ldots,T_d(n))} \to \mu.$$

Theorem (D. and Morgenbesser, 2012)

Let $a \geqslant 1$ *and* $b \geqslant 0$ *be integers and set* $m' = \gcd(a, m)$ *(where* $m = m(q, g_0, \ldots, g_{q-1})$ *can be defined in a proper way). Set*

$$\mathrm{d}\nu' = m' \cdot \mathbf{1}_{T(b)U'}\,\mathrm{d}\mu,$$

where

- $\mu \ldots$ *Haar measure on G,*
- $U' = \mathrm{cl}(\{T(m'n) : n \geqslant 0\}) \ldots$ *normal subgroup of G of index* m'.

Then $(T(an+b))_{n\geqslant 0}$ *is* ν'*-uniformly distributed in G, that is,*

$$\boxed{\frac{1}{N}\sum_{n=0}^{N-1} \delta_{T(an+b)} \to \nu'}.$$

Theorem (D. and Morgenbesser, 2012)

There exists a positive integer $m = m(q, g_0, \ldots, g_{q-1})$ such that the following holds: Set

$$\mathrm{d}\nu = \sum_{v=0}^{m} \mathbf{1}_{g_v U} \cdot Q(v,m)\, \mathrm{d}\mu,$$

where

- $\mu \ldots$ *Haar measure on G,*
- $U = \mathrm{cl}(\{T(mn) : n \geqslant 0\}) \ldots$ *normal subgroup of G of index m,*
- $Q(v,m) = \#\{0 \leqslant n < m : n^2 \equiv v \bmod m\}$.

Then $(T(n^2))_{n\geqslant 0}$ is ν-uniformly distributed in G, that is,

$$\boxed{\frac{1}{N}\sum_{n=0}^{N-1} \delta_{T(n^2)} \to \nu}.$$

A **unitary group representation** is a continuous homomorphism $D : G \to U_n$ for some $n \geqslant 1$.

$U_n \ldots$ group of unitary $n \times n$ matrices over $\mathbb{C}$

D is irreducible if there is no proper subspace W of $\mathbb{C}^n$ with $D(x)W \subseteq W$ for all $x \in G$

A **unitary group representation** is a continuous homomorphism $D : G \to U_n$ for some $n \geqslant 1$.

$U_n \ldots$ group of unitary $n \times n$ matrices over $\mathbb{C}$

D is irreducible if there is no proper subspace W of $\mathbb{C}^n$ with $D(x)W \subseteq W$ for all $x \in G$

Lemma

Let G be a compact group and ν a regular normed Borel measure on G. Then a sequence $(x_n)_{n\geqslant 0}$ is ν-uniformly distributed in G iff

$$\frac{1}{N}\sum_{n=0}^{N-1} D(x_n) \to \int_G D\, \mathrm{d}\nu$$

holds for all irreducible unitary representations D of G.

Remarks:

- The integer $m = m(q, g_0, \ldots, g_{q-1})$ is the largest integer such that $m \mid q-1$ and such that there exists a representation D of G with

$$D(g_u) = e^{-2\pi i \frac{u}{m}} \qquad \text{for all } u \in \{0, 1, \ldots, q-1\}.$$

- $(T(n^2))_{n \geqslant 0}$ is uniformly distributed in G (i.e., $\nu = \mu$) iff $m \leqslant 2$.
- $(T(an+b))_{n \geqslant 0}$ is uniformly distributed in G (i.e., $\nu' = \mu$) iff $m' = \gcd(a, m) = 1$.

- If G is connected, then $T(n^2)$ and $T(an+b)$ are uniformly distributed in G.

★ Properties of the Fourier term

$$T_\lambda(n) := g_{\varepsilon_0(n)} g_{\varepsilon_1(n)} \cdots g_{\varepsilon_{\lambda-1}(n)} \quad \text{(periodic with period } q^\lambda\text{)}$$

$$F_\lambda(h) := \frac{1}{q^\lambda} \sum_{0 \leqslant u < q^\lambda} e^{-2\pi i \frac{hu}{q^\lambda}} D(T_\lambda(u))$$

Lemma

Set

$$\Psi_D(t) = \sum_{0 \leqslant u < q} e(tu) D(g_u),$$

then

$$F_\lambda(h) = \frac{1}{q^\lambda} \Psi_D\left(-\frac{h}{q^\lambda}\right) \Psi_D\left(-\frac{h}{q^{\lambda-1}}\right) \cdots \Psi_D\left(-\frac{h}{q}\right).$$

★ Properties of the Fourier term

Lemma

Suppose that $D \notin \{D_0, \ldots, D_{m-1}\}$ is an irreducible and unitary representation of G. Then there exists a constant $c > 0$ such that

$$\boxed{\max_{h\in\mathbb{Z}} \|F_\lambda(h)\|_2 \ll q^{-c\lambda}}.$$

★ Exercise on linear subsequences

$$\sum_{n<N} D(T(an+b))$$

$$= \sum_{0\leqslant u<q^\nu} \sum_{n<N} D(T(u)) \cdot \frac{1}{q^\lambda} \sum_{0\leqslant h<q^\lambda} \mathrm{e}\left(\frac{h(an+b-u)}{q^\lambda}\right)$$

$$= \sum_{0\leqslant h<q^\lambda} F_\lambda(h) \sum_{n<N} \mathrm{e}\left(\frac{h(an+b)}{q^\lambda}\right).$$

★ Exercise on linear subsequences

$$\sum_{n<N} D(T(an+b))$$
$$= \sum_{0\leqslant u<q^\nu} \sum_{n<N} D(T(u)) \cdot \frac{1}{q^\lambda} \sum_{0\leqslant h<q^\lambda} \mathrm{e}\left(\frac{h(an+b-u)}{q^\lambda}\right)$$
$$= \sum_{0\leqslant h<q^\lambda} F_\lambda(h) \sum_{n<N} \mathrm{e}\left(\frac{h(an+b)}{q^\lambda}\right).$$

$$\left\|\sum_{n<N} D(T(an+b))\right\|_2 \ll \sum_{0\leqslant h<q^\lambda} \|F_\lambda(h)\|_2 \cdot \min\left(N, \frac{1}{\left|\sin\frac{\pi ha}{q^\lambda}\right|}\right).$$

★ Sketch of the proof for squares

$$\boxed{\frac{1}{N} \sum_{0 \leqslant n < N} D(T(n^2))}$$

★ Sketch of the proof for squares

$$\boxed{\frac{1}{N}\sum_{0\leqslant n<N} D(T(n^2))}$$

- The representation $D_0, \ldots, D_{m-1}$ are special but easy:

$$D_k(g_u) = e^{-2\pi i \frac{k}{m} u} \qquad \text{for all } 0 \leqslant u < q \text{ and } 0 \leqslant k < m$$

$$D_k(T(n^2)) = e^{-2\pi i \frac{k}{m} n^2} \qquad \text{Gauss sums}$$

- For all other irreducible unitary representations ...

Van der Corput type inequality:

$$\left\| \sum_{0 \leqslant n < N} Z(n) \right\|_{\mathbb{F}} \leqslant \left(\frac{dN}{R} \sum_{|r| < R} \left(1 - \frac{|r|}{R}\right) \left\| \sum_{\substack{0 \leqslant n \leqslant B \\ 0 \leqslant n+r \leqslant B}} Z(n+r) Z(n)^H \right\|_{\mathbb{F}} \right)^{1/2} + \frac{f}{2} R$$

Van der Corput type inequality:

$$\left\| \sum_{0 \leqslant n < N} D(T(n^2)) \right\|_{\mathbb{F}} \leqslant \left(\frac{dN}{R} \sum_{|r| < R} \left(1 - \frac{|r|}{R}\right) \left\| \sum_{\substack{0 \leqslant n \leqslant B \\ 0 \leqslant n+r \leqslant B}} D(T(n+r)^2) D(T(n^2))^H \right\|_{\mathbb{F}} \right)^{1/2} + \frac{f}{2} R$$

Van der Corput type inequality:

$$\left\| \sum_{0 \leqslant n < N} D(T(n^2)) \right\|_{\mathbb{F}} \leqslant \left(\frac{dN}{R} \sum_{|r|<R} \left(1 - \frac{|r|}{R}\right) \left\| \sum_{\substack{0 \leqslant n \leqslant B \\ 0 \leqslant n+r \leqslant B}} D(T(n+r)^2) D(T(n^2))^H \right\|_{\mathbb{F}} \right)^{1/2} + \frac{f}{2} R$$

$$T\ (n) = g_{\varepsilon_0(n)} g_{\varepsilon_1(n)} \cdots g_{\varepsilon_{\lambda-1}(n)} g_{\varepsilon_\lambda(n)} \cdots g_{\varepsilon_{\ell-1}(n)}$$

Van der Corput type inequality:

$$\left\| \sum_{0 \leqslant n < N} D(T(n^2)) \right\|_{\mathbb{F}} \leqslant \left(\frac{dN}{R} \sum_{|r|<R} \left(1 - \frac{|r|}{R}\right) \left\| \sum_{\substack{0 \leqslant n \leqslant B \\ 0 \leqslant n+r \leqslant B}} D(T(n+r)^2) D(T(n^2))^H \right\|_{\mathbb{F}} \right)^{1/2} + \frac{f}{2} R$$

$$T_{\lambda}(n) = g_{\varepsilon_0(n)} g_{\varepsilon_1(n)} \cdots g_{\varepsilon_{\lambda-1}(n)}$$

Van der Corput type inequality:

$$\left\| \sum_{0\leqslant n<N} D(T(n^2)) \right\|_{\mathbb{F}} \leqslant \left(\frac{dN}{R} \sum_{|r|<R} \left(1-\frac{|r|}{R}\right) \left\| \sum_{\substack{0\leqslant n\leqslant B\\ 0\leqslant n+r\leqslant B}} D(T(n+r)^2) D(T(n^2))^H \right\|_{\mathbb{F}} \right)^{1/2} + \frac{f}{2}R$$

$$T_\lambda(n) = g_{\varepsilon_0(n)} g_{\varepsilon_1(n)} \cdots g_{\varepsilon_{\lambda-1}(n)}$$

$$(n+r)^2 = (\varepsilon_{\ell-1}\varepsilon_{\ell-2}\ldots\varepsilon_\lambda\ldots)_q, \qquad n^2 = (\varepsilon_{\ell-1}\varepsilon_{\ell-2}\ldots\varepsilon_\lambda\ldots)_q$$

Van der Corput type inequality:

$$\left\| \sum_{0\leqslant n<N} D(T(n^2)) \right\|_{\mathbb{F}} \leqslant \left(\frac{dN}{R} \sum_{|r|<R} \left(1-\frac{|r|}{R}\right) \left\| \sum_{\substack{0\leqslant n\leqslant B\\ 0\leqslant n+r\leqslant B}} D(T(n+r)^2) D(T(n^2))^H \right\|_{\mathbb{F}} \right)^{1/2} + \frac{f}{2}R$$

$$T_{\lambda}(n) = g_{\varepsilon_0(n)} g_{\varepsilon_1(n)} \cdots g_{\varepsilon_{\lambda-1}(n)}$$

$$(n+r)^2 = (\varepsilon_{\ell-1}\varepsilon_{\ell-2}\ldots\varepsilon_{\lambda}\ldots)_q, \qquad n^2 = (\varepsilon_{\ell-1}\varepsilon_{\ell-2}\ldots\varepsilon_{\lambda}\ldots)_q$$

$$D(T((n+r)^2)) D(T(n^2))^H$$

$$= D(T_{\lambda}((n+r)^2)) D(g_{\varepsilon_\lambda}) \cdots D(g_{\varepsilon_{\ell-1}}) D(g_{\varepsilon_{\ell-1}})^H \cdots D(g_{\varepsilon_\lambda})^H D(T_{\lambda}(n^2))^H$$

Van der Corput type inequality:

$$\left\| \sum_{0\leqslant n<N} D(T(n^2)) \right\|_{\mathbb{F}} \leqslant \left(\frac{dN}{R} \sum_{|r|<R} \left(1-\frac{|r|}{R}\right) \left\| \sum_{\substack{0\leqslant n\leqslant B\\ 0\leqslant n+r\leqslant B}} D(T(n+r)^2) D(T(n^2))^H \right\|_{\mathbb{F}} \right)^{1/2} + \frac{f}{2}R$$

$$T_\lambda(n) = g_{\varepsilon_0(n)} g_{\varepsilon_1(n)} \cdots g_{\varepsilon_{\lambda-1}(n)}$$

$$(n+r)^2 = (\varepsilon_{\ell-1}\varepsilon_{\ell-2}\ldots\varepsilon_\lambda\ldots)_q, \qquad n^2 = (\varepsilon_{\ell-1}\varepsilon_{\ell-2}\ldots\varepsilon_\lambda\ldots)_q$$

$$D(T((n+r)^2))D(T(n^2))^H$$

$$= D(T_\lambda((n+r)^2))D(g_{\varepsilon_\lambda})\cdots \overbrace{D(g_{\varepsilon_{\ell-1}})D(g_{\varepsilon_{\ell-1}})^H}^{I_n} \cdots D(g_{\varepsilon_\lambda})^H D(T_\lambda(n^2))^H$$

Van der Corput type inequality:

$$\left\| \sum_{0\leqslant n<N} D(T(n^2)) \right\|_{\mathbb{F}} \leqslant \left(\frac{dN}{R} \sum_{|r|<R} \left(1-\frac{|r|}{R}\right) \left\| \sum_{\substack{0\leqslant n\leqslant B\\ 0\leqslant n+r\leqslant B}} D(T(n+r)^2) D(T(n^2))^H \right\|_{\mathbb{F}} \right)^{1/2} + \frac{f}{2}R$$

$$T_{\lambda}(n) = g_{\varepsilon_0(n)} g_{\varepsilon_1(n)} \cdots g_{\varepsilon_{\lambda-1}(n)}$$

$$(n+r)^2 = (\varepsilon_{\ell-1}\varepsilon_{\ell-2}\ldots\varepsilon_{\lambda}\ldots)_q, \qquad n^2 = (\varepsilon_{\ell-1}\varepsilon_{\ell-2}\ldots\varepsilon_{\lambda}\ldots)_q$$

$$D(T((n+r)^2))D(T(n^2))^H$$

$$= D(T_{\lambda}((n+r)^2))D(g_{\varepsilon_\lambda})\cdots \overbrace{D(g_{\varepsilon_{\ell-1}})D(g_{\varepsilon_{\ell-1}})^H}^{I_n} \cdots D(g_{\varepsilon_\lambda})^H D(T_{\lambda}(n^2))^H$$
$$= D(T_{\lambda}((n+r)^2))D(T_{\lambda}(n^2))^H$$

$$T_{\lambda}(n) = g_{\varepsilon_0(n)} g_{\varepsilon_1(n)} \cdots g_{\varepsilon_{\mu-1}(n)} g_{\varepsilon_\mu(n)} \cdots g_{\varepsilon_{\lambda-1}(n)}$$

Fourier terms:

$$F_{\lambda}(h) = \frac{1}{q^\lambda} \sum_{0 \leqslant u < q^\lambda} e^{-2\pi i \frac{hu}{q^\lambda}} D(T_{\lambda}(u))$$

$$T_{\mu,\lambda}(n) = \qquad g_{\varepsilon_\mu(n)} \cdots g_{\varepsilon_{\lambda-1}(n)}$$

Fourier terms:

$$F_\lambda(h) = \frac{1}{q^\lambda} \sum_{0 \leqslant u < q^\lambda} e^{-2\pi i \frac{hu}{q^\lambda}} D(T_\lambda(u))$$

$$T_{\mu,\lambda}(n) = \qquad\qquad g_{\varepsilon_\mu(n)} \cdots g_{\varepsilon_{\lambda-1}(n)}$$

Fourier terms:

$$F_\lambda(h) = \frac{1}{q^\lambda} \sum_{0 \leqslant u < q^\lambda} e^{-2\pi i \frac{hu}{q^\lambda}} D(T_\lambda(u))$$

$$F_{\mu,\lambda}(h) := \frac{1}{q^\lambda} \sum_{0 \leqslant u < q^\lambda} e^{-2\pi i \frac{hu}{q^\lambda}} D(T_{\mu,\lambda}(u))$$

A subtle Fourier analysis of the double truncated sum (following the ideas of Mauduit and Rivat) leads to the following expression:

A subtle Fourier analysis of the double truncated sum (following the ideas of Mauduit and Rivat) leads to the following expression:

$$\frac{2}{\pi}\log\left(\frac{4e^{\pi/2}q^{\lambda}}{\pi}\right) q^{\lambda/2} \max_{0\leqslant \ell < q^{\lambda}} \sum_{d\mid q^{\lambda}} d^{1/2}$$

$$\cdot \sum_{\substack{0\leqslant h_1,h_2,h_3,h_4<q^{\lambda}\\ (h_1+h_2+h_3+h_4,q^{\lambda})=d \\ d\mid 2r(h_1+h_2)+2sq^{\mu}(h_2+h_3)+\ell}} \|F_{\mu,\lambda}(h_1)\|_{\mathbb{F}}\, \|F_{\mu,\lambda}(h_2)\|_{\mathbb{F}}\, \|F_{\mu,\lambda}(h_3)\|_{\mathbb{F}}\, \|F_{\mu,\lambda}(h_4)\|_{\mathbb{F}}$$

A subtle Fourier analysis of the double truncated sum (following the ideas of Mauduit and Rivat) leads to the following expression:

$$\frac{2}{\pi}\log\left(\frac{4e^{\pi/2}q^{\lambda}}{\pi}\right) q^{\lambda/2} \max_{0\leqslant \ell < q^{\lambda}} \sum_{d \mid q^{\lambda}} d^{1/2}$$

$$\cdot \sum_{\substack{0\leqslant h_1,h_2,h_3,h_4<q^{\lambda}\\ (h_1+h_2+h_3+h_4,q^{\lambda})=d \\ d \mid 2r(h_1+h_2)+2sq^{\mu}(h_2+h_3)+\ell}} \|F_{\mu,\lambda}(h_1)\|_{\mathbb{F}} \, \|F_{\mu,\lambda}(h_2)\|_{\mathbb{F}} \, \|F_{\mu,\lambda}(h_3)\|_{\mathbb{F}} \, \|F_{\mu,\lambda}(h_4)\|_{\mathbb{F}}$$

This term can be estimated by applying upper bounds on the Fourier terms (in a quite subtle way; an analogue of this expression appears in Mauduit and Rivat's work).

★ Applications

★ The sum-of-digits function:

Theorem (Mauduit and Rivat, 2009)

Let $q, m \geqslant 2$ *and set* $r = \gcd(q-1, m)$. *Then we have*

$$\boxed{\lim_{N\to\infty} \frac{1}{N} \# \{n < N : s_q(n^2) \equiv a \bmod m\} = \frac{1}{r} Q(a,r)},$$

where $Q(a,r) = \#\{0 \leqslant n < r : n^2 \equiv a \bmod r\}$.
Furthermore, $(\alpha s_q(n^2))_{n\in\mathbb{N}}$ *is uniformly distributed modulo* 1 *iff* α *is irrational.*

★ Applications

★ Invertible automatic sequences:

Theorem (D. and Morgenbesser, 2012)

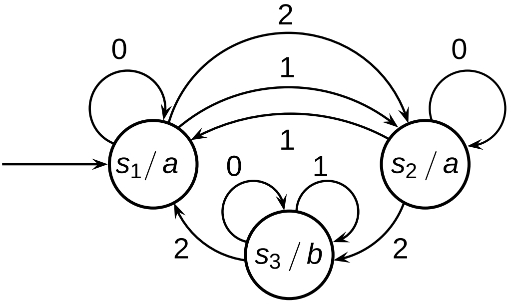
Let $q \geqslant 2$ and $(u_n)_{n\geqslant 0}$ be an invertible q-automatic sequence. Then the **frequency** *of each letter of the subsequence $(u_{n^2})_{n\geqslant 0}$ exists.*

Remark. In invertible automatic sequences the frequencies of the stated in the automaton is equidistributed. For the subsequenc of squares the limiting distribution might be different.

★ Automatic sequences

Definition

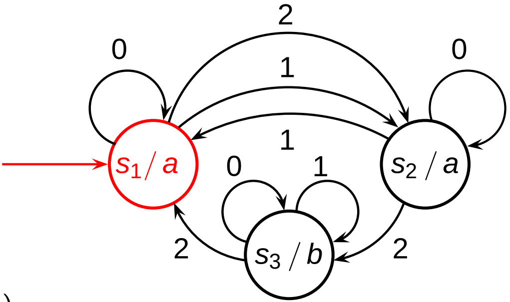
A sequence $(u_n)_{n \geqslant 0}$ is called a *q-automatic sequence*, if u_n is the output of an automaton when the input is the q-ary expansion of n.



★ Automatic sequences

Definition

A sequence $(u_n)_{n \geqslant 0}$ is called a *q-automatic sequence*, if u_n is the output of an automaton when the input is the q-ary expansion of n.

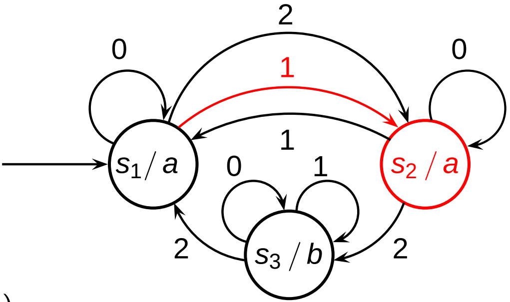


$32 = (1012)_3$

★ Automatic sequences

Definition

A sequence $(u_n)_{n \geqslant 0}$ is called a *q-automatic sequence*, if u_n is the output of an automaton when the input is the q-ary expansion of n.

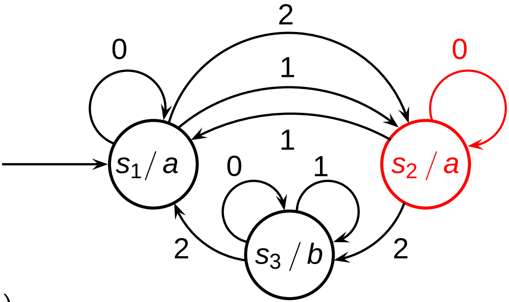


$32 = (1012)_3$

★ Automatic sequences

Definition

A sequence $(u_n)_{n\geqslant 0}$ is called a *q-automatic sequence*, if u_n is the output of an automaton when the input is the q-ary expansion of n.

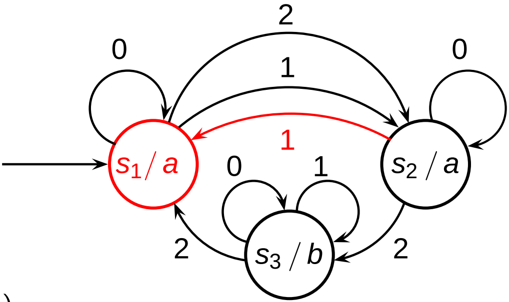


$32 = (1012)_3$

★ Automatic sequences

Definition

A sequence $(u_n)_{n\geqslant 0}$ is called a *q-automatic sequence*, if u_n is the output of an automaton when the input is the q-ary expansion of n.

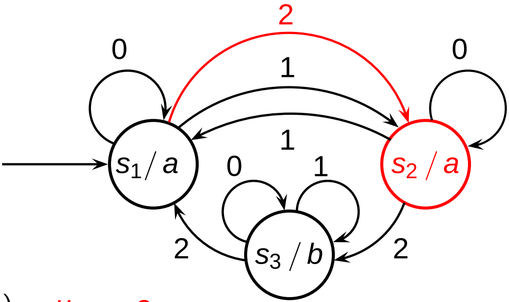


$32 = (1012)_3$

★ Automatic sequences

Definition

A sequence $(u_n)_{n\geqslant 0}$ is called a *q-automatic sequence*, if u_n is the output of an automaton when the input is the q-ary expansion of n.

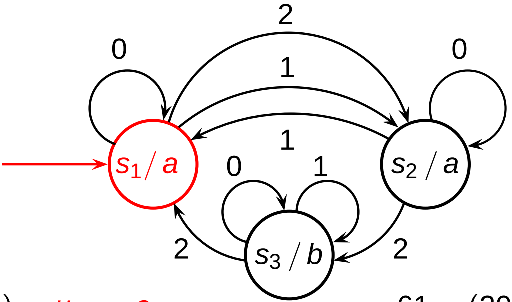


$32 = (1012)_3 \quad u_{32} = a,$

★ Automatic sequences

Definition

A sequence $(u_n)_{n\geqslant 0}$ is called a *q-automatic sequence*, if u_n is the output of an automaton when the input is the q-ary expansion of n.

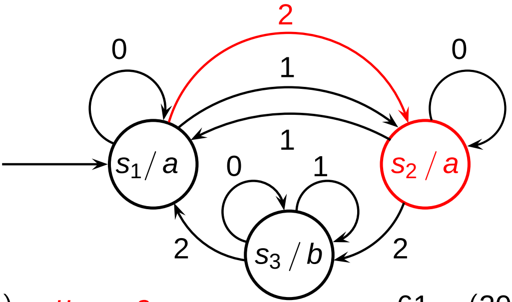


$32 = (1012)_3$ $\quad u_{32} = a$, $\qquad 61 = (2021)_3$

★ Automatic sequences

Definition

A sequence $(u_n)_{n\geqslant 0}$ is called a *q-automatic sequence*, if u_n is the output of an automaton when the input is the q-ary expansion of n.

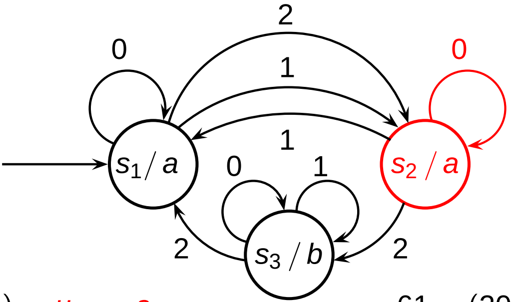


$32 = (1012)_3$ $\quad u_{32} = a$, $\qquad 61 = (2021)_3$

★ Automatic sequences

Definition

A sequence $(u_n)_{n\geqslant 0}$ is called a *q-automatic sequence*, if u_n is the output of an automaton when the input is the q-ary expansion of n.

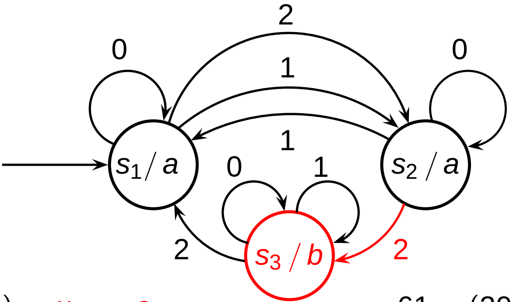


$32 = (1012)_3$ $\quad u_{32} = a$, $\qquad 61 = (2021)_3$

★ Automatic sequences

Definition

A sequence $(u_n)_{n\geqslant 0}$ is called a *q-automatic sequence*, if u_n is the output of an automaton when the input is the q-ary expansion of n.

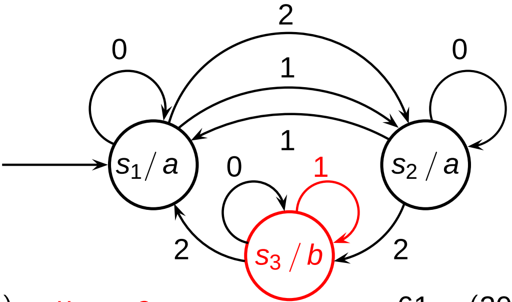


$32 = (1012)_3$ $u_{32} = a$, $61 = (2021)_3$

★ Automatic sequences

Definition

A sequence $(u_n)_{n\geqslant 0}$ is called a *q-automatic sequence*, if u_n is the output of an automaton when the input is the q-ary expansion of n.

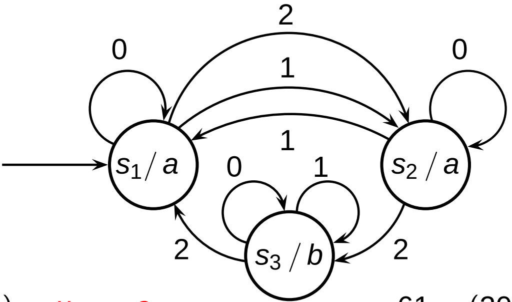


$32 = (1012)_3 \quad u_{32} = a,$ $\qquad$ $61 = (2021)_3 \quad u_{61} = b$

★ Automatic sequences

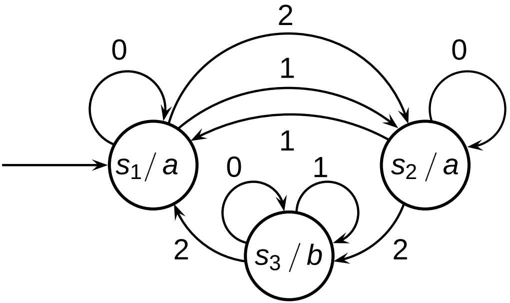
Definition

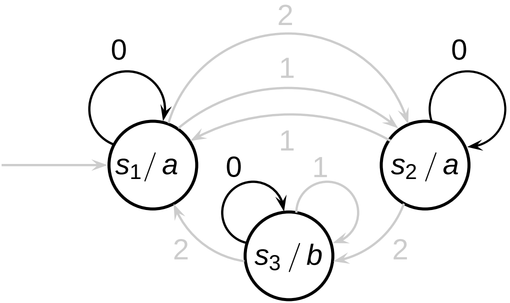
A sequence $(u_n)_{n\geqslant 0}$ is called a *q-automatic sequence*, if u_n is the output of an automaton when the input is the q-ary expansion of n.



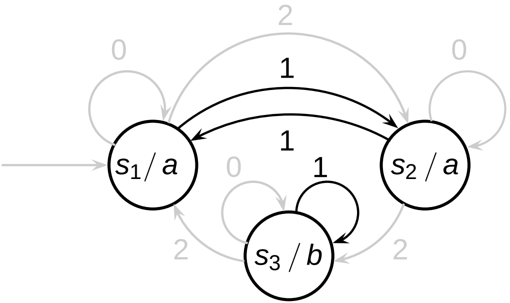
$32 = (1012)_3 \quad u_{32} = a,$ $61 = (2021)_3 \quad u_{61} = b$

$(u_n)_{n\geqslant 0}$: *aaaaabaabaabaaabbaaabaaabbaaabaaabbaaaaaaba*...

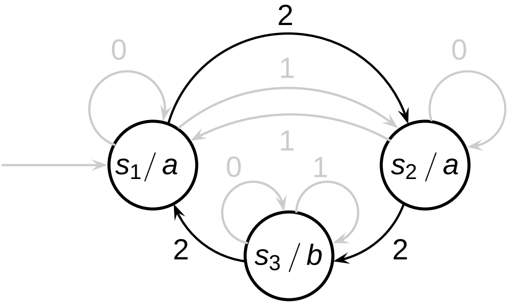

2
0
1
0
1
0
1
s_1 / a
s_2 / a
2
2
s_3 / b



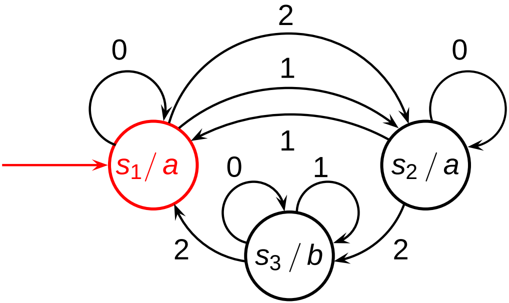
$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$



$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

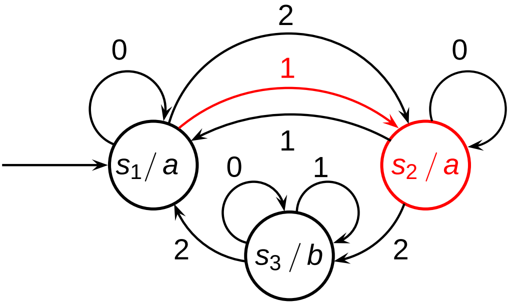


$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$



$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

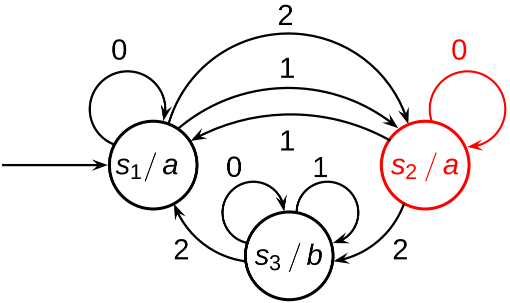
$$32 = (1012)_3 : \qquad \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$



$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

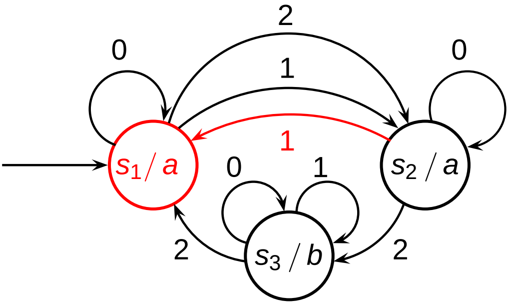
$32 = (1012)_3$:

$$M_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$



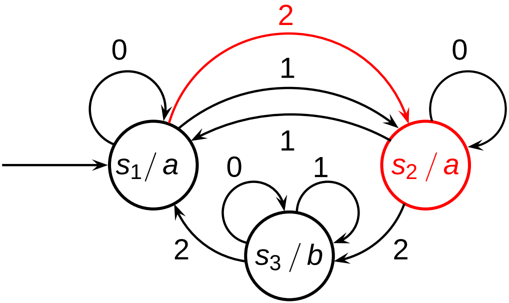
$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$32 = (1012)_3 : \qquad M_0 \circ M_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$



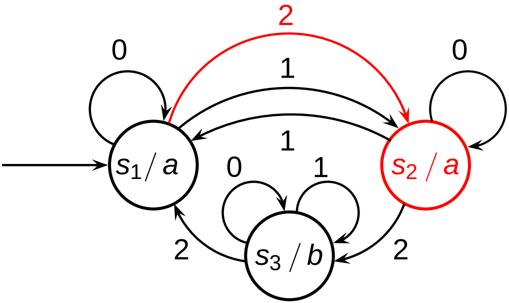
$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$32 = (1012)_3: \qquad M_1 \circ M_0 \circ M_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$



$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

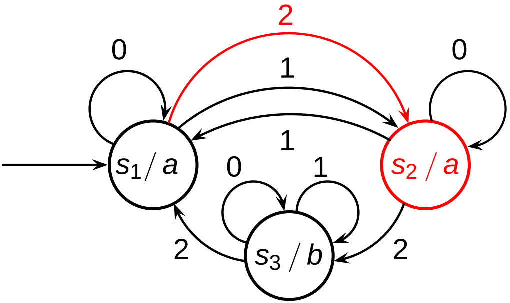
$$32 = (1012)_3 : \qquad M_2 \circ M_1 \circ M_0 \circ M_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$



$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\boxed{S(n) := M_{\varepsilon_0(n)} M_{\varepsilon_1(n)} \cdots M_{\varepsilon_{\ell-1}(n)}}$$

$$\boxed{u_n = f(S(n)\mathbf{e}_1)} \qquad \mathbf{e}_1 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T$$



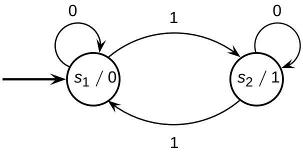
$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Definition

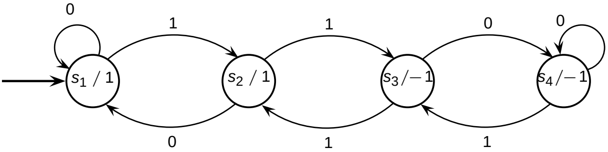
A q-automatic sequence is called *invertible* if there exists an automaton such that all transition matrices are invertible and M_0 is the identity matrix.

Examples of automatic sequences

Thue-Morse sequence (invertible):



Rudin-Shapiro sequence (**not** invertible):



★ Automatic Sequences and Generalized Thue-Morse sequences

- u_n ... invertible automatic sequence

$$\Longrightarrow \quad \boxed{u_n = f(S(n)\mathbf{e}_1)},$$

where $S(n)$ is a generalized Thue-Morse sequence on $H = \mathrm{SL}(m, \mathbb{R})$

★ Gelfond's 3rd problem on polynomial values

★ The sum-of-digits function:

Theorem (D., Mauduit and Rivat, 2011)

Let $d \geqslant 2$ be an integer, $\boxed{q \geqslant q_0(d)}$ a sufficently large **prime** *number, and $P \in \mathbb{N}[X]$ of degree d such the leading coefficient is co-prime to q. Set $r = \gcd(q-1, m)$. Then we have*

$$\boxed{\lim_{N\to\infty} \frac{1}{N} \#\{n < N : s_q(P(n)) \equiv a \bmod m\} = \frac{1}{r} Q(a,r)},$$

where $Q(a,r) = \#\{0 \leqslant n < r : P(n) \equiv a \bmod r\}$.
Furthermore, $(\alpha s_q(P(n)))_{n\in\mathbb{N}}$ is uniformly distributed modulo 1 iff α is irrational.

Remark. $q_0(d) \leqslant e^{67d^3(\log d)^2}$

★ Gelfond's 3rd problem on polynomial values

★ **Proof method:**

- Exponential sums ($e(x) := \exp(2\pi i x)$):

$$\sum_{n<N} e\left(\alpha s_q(P(n))\right)$$

- Van-der-Corput inequality
- Fourier terms

$$F_\lambda(\alpha, h) = \frac{1}{q^\lambda} \sum_{0 \leqslant u < q^\lambda} e\left(\alpha s_q(u) - huq^{-\lambda}\right)$$

- Estimates on Fourier terms and exponential sum estimates

★ Subsequences of the form $\lfloor n^c \rfloor$

★ The sum-of-digits function:

Theorem (Deshouillers, D. and Morgenbesser, 2012)

Let u_n be a q-automatic sequence (on an alphabet $\mathcal{A}$) and

$$1 < c < 7/5.$$

Then for each $\alpha \in \mathcal{A}$ then asymptotic density of α in the subsequence $u_{\lfloor n^c \rfloor}$ exists if and only if the asymptotic density of α in u_n exists (and they are the same).

In particular it follows that

$$\boxed{\lim_{x\to\infty} \frac{1}{N} \# \{n < N : s_q(\lfloor n^c \rfloor) \equiv a \bmod m\} = \frac{1}{m}}.$$

It is conjectured that this holds for all non-integers $c > 1$.

★ Gelfond's 2nd problem on primes

★ **The sum-of-digits function:**

Theorem (Mauduit and Rivat, 2010)

Let $q, m \geqslant 2$. *Then*

$$\boxed{\lim_{N\to\infty} \frac{1}{\pi(x; a, (m, q-1))} \# \{p < N : s_q(p) \equiv a \bmod m\} = \frac{(m, q-1)}{m}}.$$

Furthermore, $(\alpha s_q(p))_{p\in\mathbb{P}}$ *is uniformly distributed modulo* 1 *iff* α *is irrational.*

★ Local results the sum-of-digits function on primes

Theorem (D., Mauduit and Rivat, 2009)

Suppose that $(q, k-1) = 1$. *Then*

$$\#\{primes\ p < N : s_q(p) = k\}$$
$$= \frac{q-1}{\varphi(q-1)} \frac{\pi(N)}{\sqrt{2\pi\sigma_q^2 \log_q N}} \left(\exp\left(-\frac{(k-\mu_q \log_q N)^2}{2\sigma_q^2 \log_q N} \right) + O((\log N)^{-\frac{1}{2}+} \right.$$

where

$$\mu_q := \frac{q-1}{2}, \quad \sigma_q^2 := \frac{q^2-1}{12}.$$

Remark: This asymptotic expansion is only significant if

$$\left| k - \mu_q \log_q N \right| \leqslant C (\log N)^{\frac{1}{2}}$$

Note that $\frac{1}{\pi(N)} \sum_{p<N} s_q(p) \sim \mu_q \log_q N$.

★ Binary Representation of Primes

Corollary

Theorem (D., Mauduit, Rivat (2011))

$s_2(n)$ ... *number of powers of 2 in the binary expansion of n*

$$\#\{\text{primes } p < 2^{2k} : s_2(p) = k\} \sim \frac{2^{2k}}{\sqrt{2\pi}\log 2\, k^{\frac{3}{2}}}$$

★ Local results the sum-of-digits function on primes

Lemma

For every fixed integer $q \geq 2$ there exist two constants $c_1 > 0$, $c_2 > 0$ such that for every k with $(k, q-1) = 1$

$$\sum_{p \leqslant N\ p \equiv k \bmod q-1} e(\alpha s_q(p)) \ll (\log N)^3 N^{1-c_1\|(q-1)\alpha\|^2}$$

uniformly for real α with $\|(q-1)\alpha\| \geqslant c_2 (\log N)^{-\frac{1}{2}}$.

Remark. This is a refined version of the result by Mauduit and Rivat.

★ Local results the sum-of-digits function on primes

Lemma

Suppose that $0 < \nu < \frac{1}{2}$ *and* $0 < \eta < \frac{\nu}{2}$. *Then for every* k *with* $(k, q-1) = 1$ *we have*

$$\sum_{p \leqslant N,\ p \equiv k \bmod q-1} e(\alpha s_q(p)) = \frac{\pi(N)}{\varphi(q-1)} e(\alpha \mu_q \log_q N)$$

$$\times \left(e^{-2\pi^2\alpha^2\sigma_q^2 \log_q N} \left(1 + O\left(|\alpha|\right)\right) + O\left(|\alpha| (\log N)\right)\right.$$

uniformly for real α *with* $|\alpha| \leqslant (\log N)^{\eta - \frac{1}{2}}$.

Remark. This is a refined version of a **central limit theorem** and can be proved by a refined moment method.

Thank you!