Primzahlen und automatische Folgen

Michael Drmota

Institut für Diskrete Mathematik und Geometrie
Technische Universität Wien

ÖMG – Lehrer/innen/fortbildungstagung
Univ. Wien, 21. April 2017

Wie unabhängig agieren Addition und Multiplikation der natürlichen Zahlen und wie kann das quantifiziert werden?

Insbesondere wie kann die Komplexität der Multiplikation beschrieben werden?

★ Addition und Multiplikation

Addition: $n = 1 + 1 + \cdots + 1$ (1 Erzeuger)

★ Addition und Multiplikation

Addition: $n = 1 + 1 + \cdots + 1$ (1 Erzeuger)

Multiplikation: $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ (unendliche viele Erzeuger)

★ Addition und Multiplikation

Addition: $n = 1 + 1 + \cdots + 1$ (1 Erzeuger)

Multiplikation: $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ (unendliche viele Erzeuger)

$\rightarrow$ *Primzahlen*

★ Quadratfreie Zahlen

Quadratfreie Zahlen: $n = p_1 p_2 \cdots p_r$

($p_1, \ldots, p_r$ verschiedene Primzahlen)

★ Quadratfreie Zahlen

Quadratfreie Zahlen: $n = p_1 p_2 \cdots p_r$

($p_1, \ldots, p_r$ verschiedene Primzahlen)

Anteil der quadratfreien Zahlen:

$$= \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right)\cdots = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^2}\right) = \frac{6}{\pi^2} \approx 0.6$$

★ Möbius-Funktion

Definition (Möbius-Funktion)

$$\mu(n) = \begin{cases} 1 & n = 1, \\ (-1)^r & n = p_1 p_2 \cdots p_r, \\ 0 & n \text{ is nicht quadratfrei.} \end{cases}$$

★ Möbius-Funktion

Definition (Möbius-Funktion)

$$\mu(n) = \begin{cases} 1 & n = 1, \\ (-1)^r & n = p_1 p_2 \cdots p_r, \\ 0 & n \text{ is nicht quadratfrei.} \end{cases}$$

$\mu(3) = \mu(5) = -1$, $\mu(6) = \mu(35) = 1$

★ Möbius-Funktion

Satz

Für alle natürlichen Zahlen $n > 1$ gilt

$$\sum_{d|n} \mu(d) = 0.$$

★ Möbius-Funktion

Satz

Für alle natürlichen Zahlen $n > 1$ gilt

$$\sum_{d|n} \mu(d) = 0.$$

Sei etwa $n = p_1^{k_1} p_2^{k_2}$. Dann gilt

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(p_1) + \mu(p_2) + \mu(p_1 p_2) = 1 - 1 - 1 + 1 = 0.$$

Allgemein gilt für $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

$$\sum_{d|n} \mu(d) = \prod_{j=1}^{r} (\mu(1) + \mu(p_j)) = 0.$$

★ Möbius-Funktion

Was bedeutet

$$\sum_{d|n} \mu(d) = 0 \quad ?$$

★ Möbius-Funktion

Was bedeutet

$$\sum_{d|n} \mu(d) = 0 \quad ?$$

Es bedeutet, dass die **Hälfte** der (quadratfreien) Teiler von n eine **gerade Anzahl** von Primteilern hat und die andere **Hälfte** eine **ungerade Anzahl** von Primteilner hat.

★ Möbius-Funktion

Was bedeutet

$$\sum_{d|n} \mu(d) = 0 \quad ?$$

Es bedeutet, dass die **Hälfte** der (quadratfreien) Teiler von n eine **gerade Anzahl** von Primteilern hat und die andere **Hälfte** eine **ungerade Anzahl** von Primteilner hat.

Was wird für

$$\sum_{n=1}^{N} \mu(n) = \mu(1) + \mu(2) + \cdots + \mu(N)$$

erwartet?

★ Möbius-Funktion

Satz

$$\sum_{n=1}^{N} \mu(n) = o(N) \qquad (N \to \infty)$$

Etwa die **Hälfte** *der (quadratfreien) Zahlen* $n \leqslant N$ *haben eine* **gerade Anzahl** *von Primteilern hat und die andere* **Hälfte** *eine* **ungerade Anzahl** *von Primteilner hat.*

★ Möbius-Funktion

Satz

$$\sum_{n=1}^{N} \mu(n) = o(N) \qquad (N \to \infty)$$

Etwa die **Hälfte** *der (quadratfreien) Zahlen $n \leqslant N$ haben eine* **gerade Anzahl** *von Primteilern hat und die andere* **Hälfte** *eine* **ungerade Anzahl** *von Primteilner hat.*

Interessanterweise gibt es einen direkten Zusammenhang zum **Primzahlsatz**:

$$\sum_{n=1}^{N} \mu(n) = o(N) \quad \Longleftrightarrow \quad \pi(x) \sim \frac{x}{\log x}$$

Dabei ist

$$\pi(x) = \text{Anzahl der Primzahlen } p \leqslant x.$$

★ Primzahlsatz

Satz (Primzahlsatz)

$$\pi(x) \sim \frac{x}{\log x} \qquad (x \to \infty)$$

★ Primzahlsatz

Satz (Primzahlsatz)

$$\pi(x) \sim \frac{x}{\log x} \qquad (x \to \infty)$$

Satz (Dirichletscher Primzahlsatz)

$$\pi(x; a, m) \sim \frac{1}{\varphi(m)} \frac{x}{\log x} \qquad (x \to \infty)$$

für alle natürlichen Zahlen a, m *mit* $\operatorname{ggT}(a, m) = 1$ *und den Bezeichungen*

$$\pi(x; a, m) = \textit{Anzahl der Primzahlen } p \leqslant x \textit{ mit } p \equiv a \bmod m,$$

$$\varphi(m) = \textit{Anzahl der Restklassen } a \bmod m \textit{ mit } \operatorname{ggT}(a, m) = 1.$$

★ Möbius-Funktion in Restklassen

Was kann man zB über

$$\sum_{n\leqslant N,\, n\equiv 1 \bmod 4} \mu(n)$$

sagen?

★ Möbius-Funktion in Restklassen

Was kann man zB über

$$\sum_{n\leqslant N,\, n\equiv 1 \bmod 4} \mu(n)$$

sagen?

Satz

$$\sum_{n\leqslant N,\, n\equiv a \bmod m} \mu(n) = o(N) \qquad (N\to\infty)$$

für alle natürlichen Zahlen a, m.

★ Möbius-Funktion in Restklassen

Was kann man zB über

$$\sum_{n\leqslant N,\, n\equiv 1 \bmod 4} \mu(n)$$

sagen?

Satz

$$\sum_{n\leqslant N,\, n\equiv a \bmod m} \mu(n) = o(N) \qquad (N\to\infty)$$

für alle natürlichen Zahlen a, m.

Dieser Satz ist äquivalent zum Dirichletschen Primzahlsatz.

★ Möbius-Funktion in Restklassen

Für Zahlen a, m mit $\mathrm{ggT}(a, m) = 1$ gilt

$$\sum_{n \leqslant N,\, n \equiv a \bmod m} \mu(n) = o(N) \quad \Longleftrightarrow \quad \pi(x; a, m) \sim \frac{1}{\varphi(m)} \frac{x}{\log x}.$$

★ Möbius-Funktion in Restklassen

Für Zahlen a, m mit $\operatorname{ggT}(a, m) = 1$ gilt

$$\sum_{n \leqslant N,\, n \equiv a \bmod m} \mu(n) = o(N) \quad \Longleftrightarrow \quad \pi(x; a, m) \sim \frac{1}{\varphi(m)} \frac{x}{\log x}.$$

Ist $\operatorname{ggT}(a, m) > 1$, kann die Summe über die Möbius-Funktion auf den Fall $\operatorname{ggT}(a, m) = 1$ zurückgeführt werden. Z.B. gilt

$$\begin{aligned}\sum_{n \leqslant N,\, n \equiv 2 \bmod 4} \mu(n) &= \sum_{k \leqslant N/2,\, k \equiv 1 \bmod 2} \mu(2k) \\ &= -\sum_{k \leqslant N/2,\, k \equiv 1 \bmod 2} \mu(k) \\ &= o(N).\end{aligned}$$

★ Möbius-Funktion und Addition

Was kann über

$$\sum_{n\leqslant N} \mu(n)\mu(n+2)$$

gesagt werden?

★ Möbius-Funktion und Addition

Was kann über

$$\sum_{n\leqslant N} \mu(n)\mu(n+2)$$

gesagt werden?

Vermutung (Chowla-Vermutung)

Für alle $k \geqslant 1$ und natürliche Zahlen $0 < \ell_1 < \ell_2 < \cdots \ell_k$ gilt

$$\sum_{n\leqslant N} \mu(n)\mu(n+\ell_1)\mu(n+\ell_2)\cdots\mu(n+\ell_k) = o(N) \qquad (N \to \infty).$$

★ Möbius-Funktion und Addition

Was kann über

$$\sum_{n\leqslant N} \mu(n)\mu(n+2)$$

gesagt werden?

Vermutung (Chowla-Vermutung)

Für alle $k \geqslant 1$ und natürliche Zahlen $0 < \ell_1 < \ell_2 < \cdots \ell_k$ gilt

$$\sum_{n\leqslant N} \mu(n)\mu(n+\ell_1)\mu(n+\ell_2)\cdots\mu(n+\ell_k) = o(N) \qquad (N \to \infty).$$

Diese Vermutung ist vollkommen offen. Das einzige Resultat in diese Richtung stammt von **Terence Tao**:

$$\sum_{n\leqslant N} \frac{\mu(n)\mu(n+\ell)}{n} = o(\log N).$$

★ Möbius-Zufallsprinzip

Folkore (Möbius-Zufallsprinzip)

Für jede **nicht komplizierte Folge** (x_n) gilt

$$\sum_{n \leqslant N} \mu(n) x_n = o(N) \qquad (N \to \infty).$$

★ Möbius-Zufallsprinzip

Folkore (Möbius-Zufallsprinzip)

Für jede **nicht komplizierte Folge** (x_n) gilt

$$\sum_{n\leqslant N} \mu(n)x_n = o(N) \qquad (N \to \infty).$$

Was ist eine **nicht komplizierte Folge**?
Beispielsweise ist eine $x_n = 1$ nicht kompliziert, denn es gilt

$$\sum_{n\leqslant N} \mu(n) = o(N) \qquad (N \to \infty).$$

★ Möbius-Zufallsprinzip

Folkore (Möbius-Zufallsprinzip)

Für jede **nicht komplizierte Folge** (x_n) gilt

$$\sum_{n\leqslant N} \mu(n)x_n = o(N) \qquad (N \to \infty).$$

Was ist eine **nicht komplizierte Folge**?
Beispielsweise ist eine $x_n = 1$ nicht kompliziert, denn es gilt

$$\sum_{n\leqslant N} \mu(n) = o(N) \qquad (N \to \infty).$$

Andererseits ist die Folge $x_n = \mu(n)$ eine **komplizierte Folge**:

$$\sum_{n\leqslant N} \mu(n)\mu(n) \sim \frac{6}{\pi^2} N \qquad (N \to \infty).$$

★ Möbius-Zufallsprinzip

Satz (Periodische Folgen sind nicht kompliziert)

Für jede periodische Folge (x_n) *gilt*

$$\sum_{n \leqslant N} \mu(n) x_n = o(N) \qquad (N \to \infty).$$

★ Möbius-Zufallsprinzip

Satz (Periodische Folgen sind nicht kompliziert)

Für jede periodische Folge (x_n) *gilt*

$$\sum_{n\leqslant N} \mu(n)x_n = o(N) \qquad (N \to \infty).$$

Sei m die Periode von (x_n). Dann gilt

$$\begin{aligned}\sum_{n\leqslant N} \mu(n)x_n &= \sum_{r=1}^{m} x_r \sum_{n\leqslant N,\, n\equiv r \bmod m} \mu(n)\\ &= \sum_{r=1}^{m} x_r \cdot o(N) = o(N).\end{aligned}$$

★ Komplexität einer Folge

Definition

Sei (x_n) eine Folge, die nur endlich viele Werte annimmt. Dann ist

$$L(m) = \text{Anzahl der verschiedenen Blöcke der Länge } m, \text{ die in } (x_n) \text{ insgesamt auftreten}$$

die (Teilwort-)**Komplexität** der Folge (x_n).

★ Komplexität einer Folge

Definition

Sei (x_n) eine Folge, die nur endlich viele Werte annimmt. Dann ist

$$L(m) = \text{Anzahl der verschiedenen Blöcke der Länge } m, \text{ die in } (x_n) \text{ insgesamt auftreten}$$

die (Teilwort-)**Komplexität** der Folge (x_n).

Beispiel. $(x_n) = (0, 0, 0, 0, 0, \ldots)$: $L(m) = 1, \ (m \geqslant 1)$.

★ Komplexität einer Folge

Definition

Sei (x_n) eine Folge, die nur endlich viele Werte annimmt. Dann ist

$$L(m) = \text{Anzahl der verschiedenen Blöcke der Länge } m, \text{ die in } (x_n) \text{ insgesamt auftreten}$$

die (Teilwort-)**Komplexität** der Folge (x_n).

Beispiel. $(x_n) = (0, 0, 0, 0, 0, \ldots)$: $L(m) = 1, \ (m \geqslant 1)$.

Beispiel. $(x_n) = (0, 1, 0, 1, 0, \ldots)$: $L(m) = 2, \ (m \geqslant 1)$.

★ Komplexität einer Folge

Definition

Sei (x_n) eine Folge, die nur endlich viele Werte annimmt. Dann ist

$$L(m) = \text{Anzahl der verschiedenen Blöcke der Länge } m, \text{ die in } (x_n) \text{ insgesamt auftreten}$$

die (Teilwort-)**Komplexität** der Folge (x_n).

Beispiel. $(x_n) = (0, 0, 0, 0, 0, \ldots)$: $L(m) = 1, \ (m \geqslant 1)$.

Beispiel. $(x_n) = (0, 1, 0, 1, 0, \ldots)$: $L(m) = 2, \ (m \geqslant 1)$.

Beispiel. (x_n) sei eine **zufällige** Folge: $L(m) = 2^m, (m \geqslant 1)$.

★ Entropie einer Folge

Definition

Sei (x_n) eine Folge, die nur q verschiedene Werte annimmt und $L(m)$ die (Teilwort-)Komplexität von (x_n). Dann ist

$$h = \lim_{m\to\infty} \frac{\log_q L(m)}{m}$$

die (toplogische) **Entropie** von (x_n).

★ Entropie einer Folge

Definition

Sei (x_n) eine Folge, die nur q verschiedene Werte annimmt und $L(m)$ die (Teilwort-)Komplexität von (x_n). Dann ist

$$h = \lim_{m\to\infty} \frac{\log_q L(m)}{m}$$

die (toplogische) **Entropie** von (x_n).

Beispiel. $(x_n) = (0, 0, 0, 0, 0, \ldots)$: $h = 0$.

★ Entropie einer Folge

Definition

Sei (x_n) eine Folge, die nur q verschiedene Werte annimmt und $L(m)$ die (Teilwort-)Komplexität von (x_n). Dann ist

$$h = \lim_{m\to\infty} \frac{\log_q L(m)}{m}$$

die (toplogische) **Entropie** von (x_n).

Beispiel. $(x_n) = (0, 0, 0, 0, 0, \ldots)$: $h = 0$.

Beispiel. $(x_n) = (0, 1, 0, 1, 0, \ldots)$: $h = 0$.

★ Entropie einer Folge

Definition

Sei (x_n) eine Folge, die nur q verschiedene Werte annimmt und $L(m)$ die (Teilwort-)Komplexität von (x_n). Dann ist

$$h = \lim_{m\to\infty} \frac{\log_q L(m)}{m}$$

die (toplogische) **Entropie** von (x_n).

Beispiel. $(x_n) = (0, 0, 0, 0, 0, \ldots)$: $h = 0$.

Beispiel. $(x_n) = (0, 1, 0, 1, 0, \ldots)$: $h = 0$.

Beispiel. (x_n) sei eine **zufällige** Folge: $h = 1$.

★ Deterministische Folgen

Definition

Sei (x_n) eine Folge, die nur endliche viele Werte annimmt, heißt **deterministisch**, wenn die (topologische) Entropie

$$h = 0$$

ist. Das heißt, für alle $\varepsilon > 0$ gilt

$$L(m) = O\left(e^{\varepsilon n}\right).$$

★ Deterministische Folgen

Definition

Sei (x_n) eine Folge, die nur endliche viele Werte annimmt, heißt **deterministisch**, wenn die (topologische) Entropie

$$h = 0$$

ist. Das heißt, für alle $\varepsilon > 0$ gilt

$$L(m) = O\left(e^{\varepsilon n}\right).$$

Beispiel. Konstante und periodische Folgen sind deterministisch.

★ Sarnak-Vermutung

Vermutung (Sarnak-Vermutung)

Für jede **deterministische Folge** (x_n) gilt

$$\sum_{n \leqslant N} \mu(n) x_n = o(N) \qquad (N \to \infty),$$

d.h., determinische Folgen erfüllen das Möbius-Zufallsprinzip.

★ Sarnak-Vermutung

Vermutung (Sarnak-Vermutung)

Für jede **deterministische Folge** (x_n) gilt

$$\sum_{n \leqslant N} \mu(n) x_n = o(N) \qquad (N \to \infty),$$

d.h., determinische Folgen erfüllen das Möbius-Zufallsprinzip.

Satz (Sarnak)

Die Sarnak-Vermutung folgt aus der Chowla-Vermutung.

★ Sarnak-Vermutung

Vermutung (Sarnak-Vermutung)

Für jede **deterministische Folge** (x_n) gilt

$$\sum_{n \leqslant N} \mu(n) x_n = o(N) \qquad (N \to \infty),$$

d.h., determinische Folgen erfüllen das Möbius-Zufallsprinzip.

Satz (Sarnak)

Die Sarnak-Vermutung folgt aus der Chowla-Vermutung.

Die Sarnak-Vermutung wurde bereits für viele deterministische Folgen bestätigt: *quasi-periodische Folgen* (Sarnak), *Nil-Folgen* (Green+Tao), *Horocycle flows* (Bourgain+Tao+Ziegler), *Thue-Morse-Folge* (Dartyge+Tenenbaum), *Rudin-Shapiro-Folge* (Mauduit+Rivat, Tao), ...

★ Thue-Morse-Folge

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

★ Thue-Morse-Folge

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

0

★ Thue-Morse-Folge

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

01

★ Thue-Morse-Folge

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

0110

★ Thue-Morse-Folge

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

01101001

★ Thue-Morse-Folge

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

$$0110100110010110$$

★ Thue-Morse-Folge

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

$$0110100110010110100101100110100 1$$

★ Thue-Morse-Folge

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

$$01101001100101101001011001101001100101101001\cdots$$

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

★ Thue-Morse-Folge

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

$$01101001100101101001011001101001100101101001\cdots$$

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

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

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

★ Thue-Morse-Folge

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

$$01101001100101101001011001101001100101101001\cdots$$

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

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

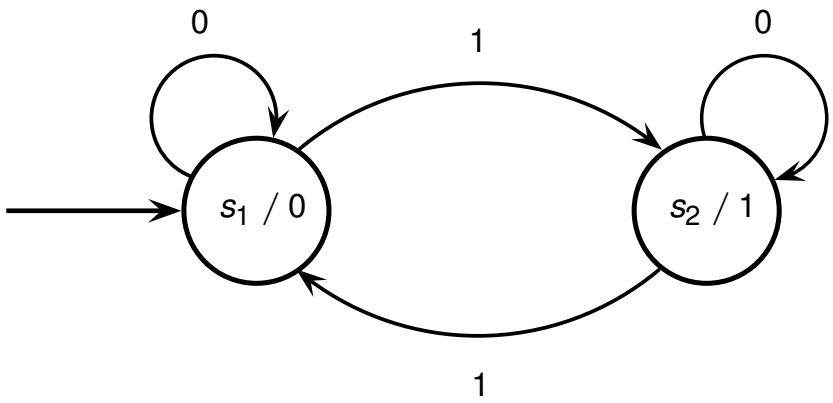
$$n = \sum_{i=0}^{\ell-1} \varepsilon_i(n) q^i \qquad \varepsilon_i(n) \in \{0, 1, \ldots, q-1\}, \qquad s_q(n) = \sum_{i=0}^{\ell-1} \varepsilon_i(n)$$

★ Thue-Morse-Folge

- TM-Folge ist **nicht periodisch** und **kubenfrei**.
- TM-Folge ist **fast-periodisch**:
  Jeder auftretende Block tritt unendlich oft mit beschränkten Abständen auf.
- **Sublineare Komplexität**: $L(m) \leqslant \frac{10}{3} m$
- **Entropie** $h = 0$.
- **Lineare Teilfolgen** $(t_{an+b})_{n \geqslant 0}$ haben dieselben Eigenschaften.
- Die TM-Folge (und ihre linearen Teilfolgen) sind **automatische Folgen**.

★ Thue-Morse-Folge

Automat, der die Thue-Morse-Folge erzeugt: $t_n = \sum_{j \geqslant 0} \varepsilon_j(n) \bmod 2$



★ Rudin-Shapiro-Folge

Rudin-Shapiro-Folge $(r_n)_{n\geqslant 0}$:

★ Rudin-Shapiro-Folge

Rudin-Shapiro-Folge $(r_n)_{n\geqslant 0}$:

$$0001001000011101000100101110001000010010000111011111\cdots$$

★ Rudin-Shapiro-Folge

Rudin-Shapiro-Folge $(r_n)_{n\geqslant 0}$:

$$0001001000011101000100101110001000010010000111011111\cdots$$

$$r_0 = 0, \qquad r_{2k} = r_k, \qquad r_{2k+1} = \begin{cases} r_k & \text{wenn } k \text{ gerade,} \\ 1 - r_k & \text{wenn } k \text{ ungerade.} \end{cases}$$

★ Rudin-Shapiro-Folge

Rudin-Shapiro-Folge $(r_n)_{n\geqslant 0}$:

$$0001001000011101000100101110001000010010000111011111\cdots$$

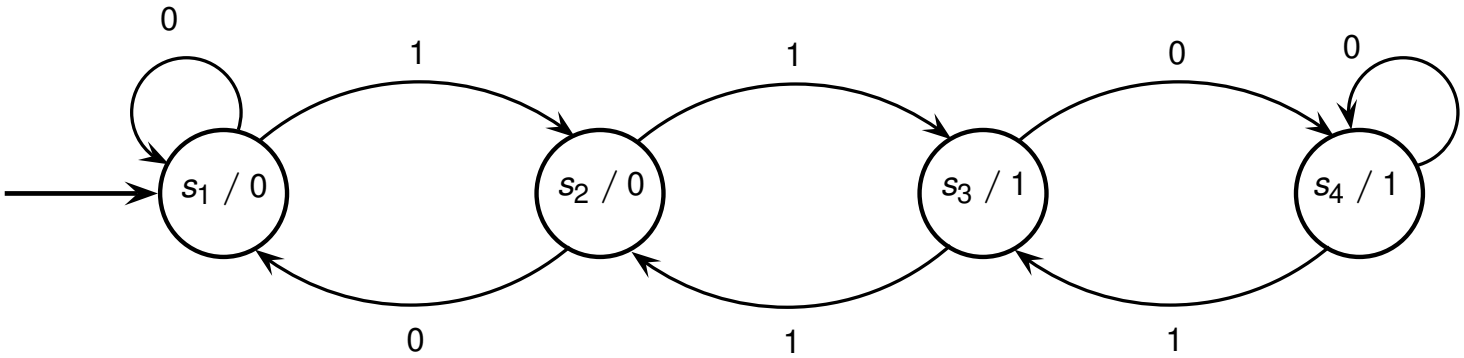
$$r_0 = 0, \qquad r_{2k} = r_k, \qquad r_{2k+1} = \begin{cases} r_k & \text{wenn } k \text{ gerade,} \\ 1 - r_k & \text{wenn } k \text{ ungerade.} \end{cases}$$

$$\boxed{r_n = \sum_{i\geqslant 0} \varepsilon_i(n)\varepsilon_{i+1}(n) \bmod 2}$$

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

★ Rudin-Shapiro-Folge

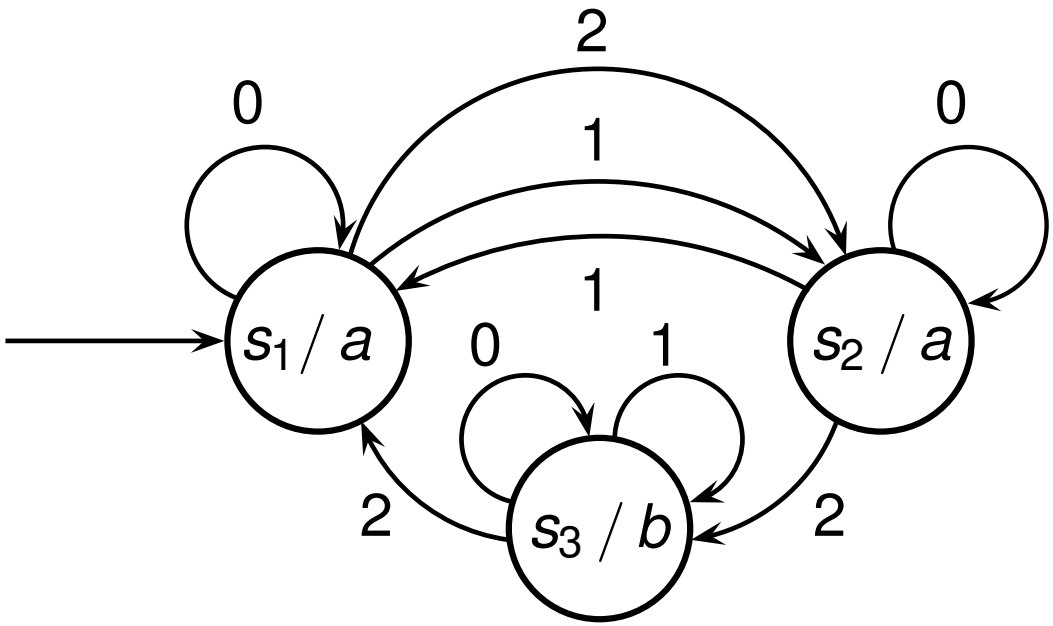
Automat, der die Rudin-Shapiro-Folge erzeugt:
$r_n = \sum_{j \geqslant 0} \varepsilon_j(n)\varepsilon_{j+1}(n) \bmod 2$



★ Automatische Folgen

Definition

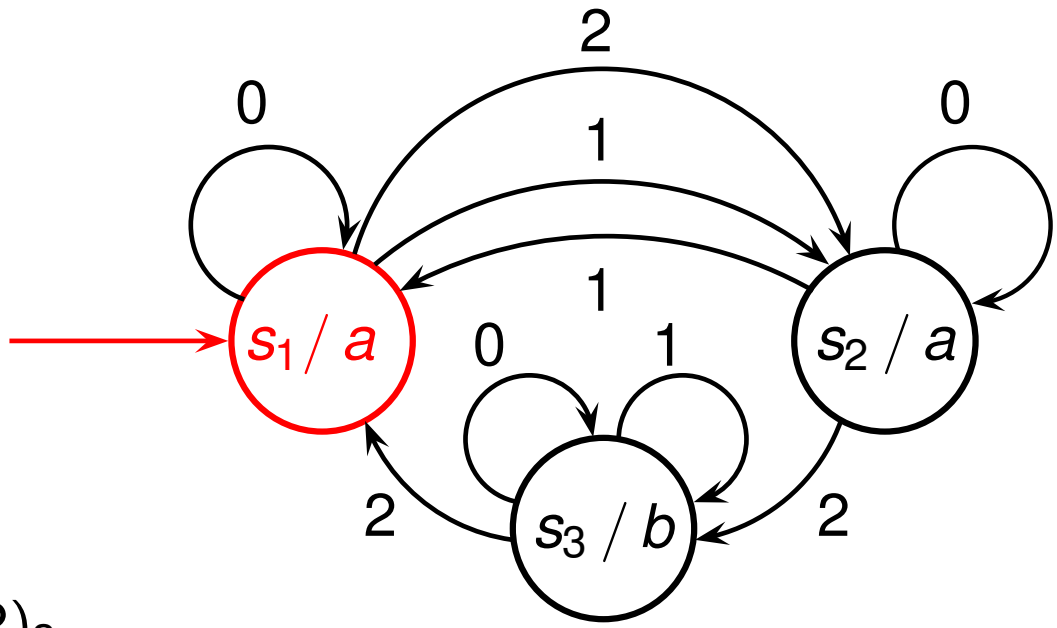
Eine Folge $(u_n)_{n\geqslant 0}$ heißt *q-automatische Folge*, wenn sie u_n als Output eines Automaten auftritt, dessen Input die q-adische Ziffernentwicklung von n ist.



★ Automatische Folgen

Definition

Eine Folge $(u_n)_{n\geqslant 0}$ heißt *q-automatische Folge*, wenn sie u_n als Output eines Automaten auftritt, dessen Input die q-adische Ziffernentwicklung von n ist.

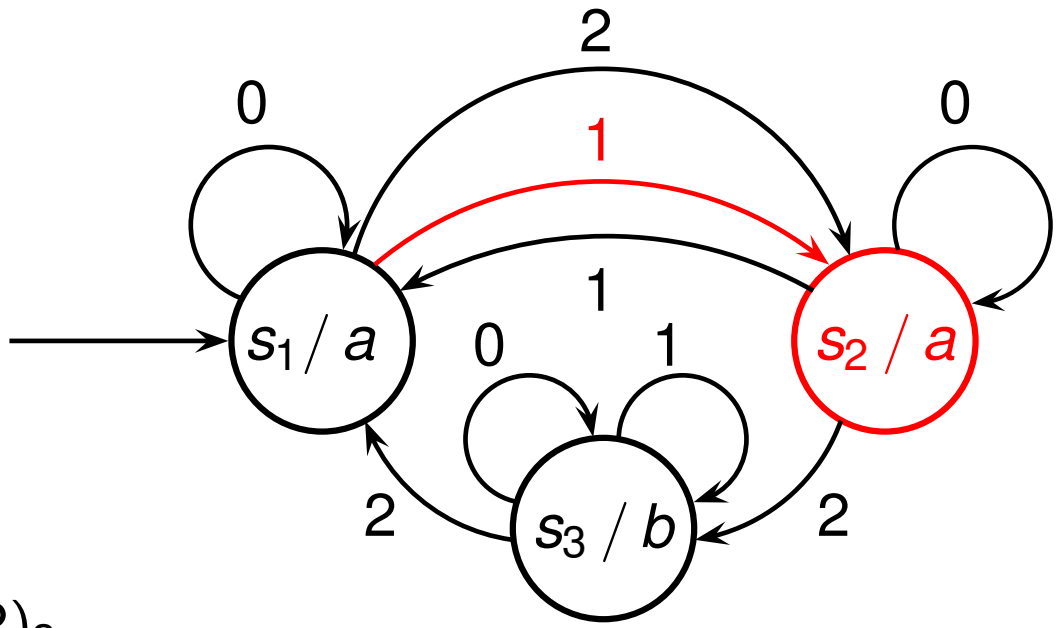


$32 = (1012)_3$

★ Automatische Folgen

Definition

Eine Folge $(u_n)_{n\geqslant 0}$ heißt *q-automatische Folge*, wenn sie u_n als Output eines Automaten auftritt, dessen Input die q-adische Ziffernentwicklung von n ist.

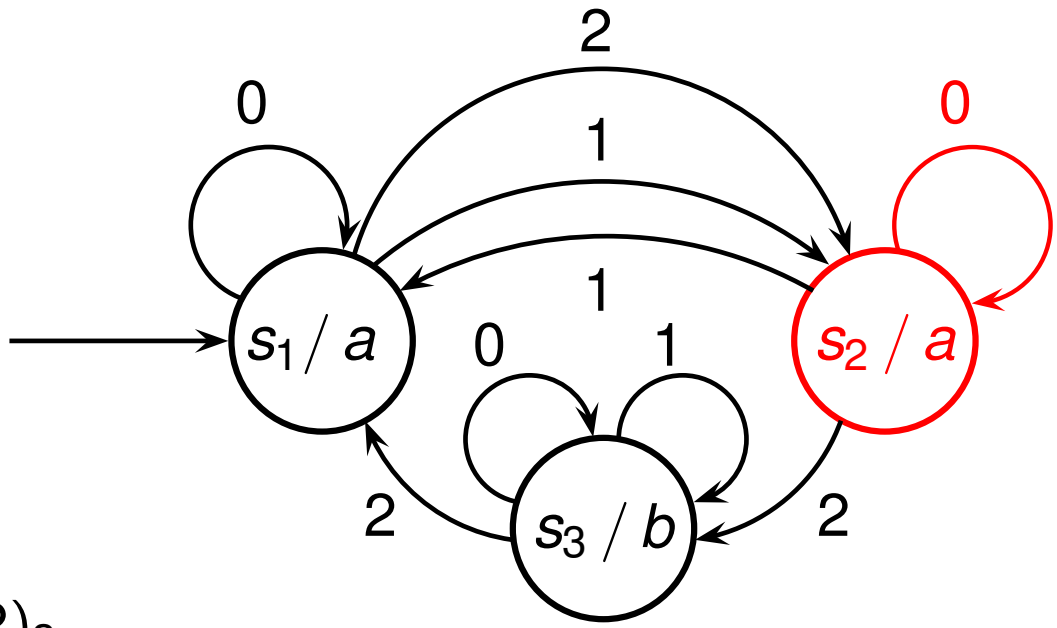


$32 = (1012)_3$

★ Automatische Folgen

Definition

Eine Folge $(u_n)_{n\geqslant 0}$ heißt *q-automatische Folge*, wenn sie u_n als Output eines Automaten auftritt, dessen Input die q-adische Ziffernentwicklung von n ist.

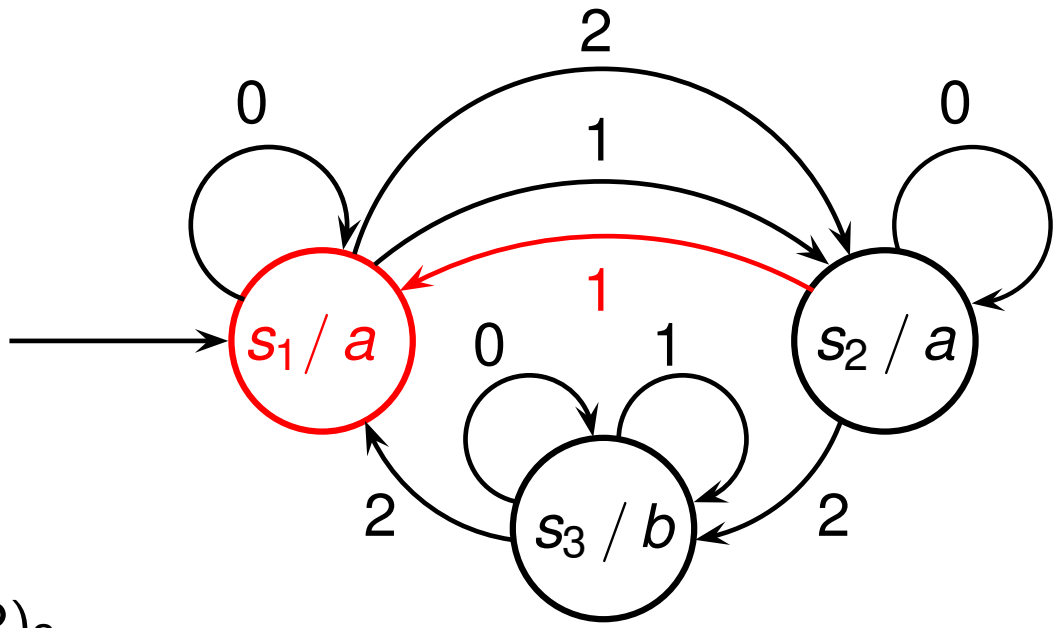


$32 = (1012)_3$

★ Automatische Folgen

Definition

Eine Folge $(u_n)_{n\geqslant 0}$ heißt *q-automatische Folge*, wenn sie u_n als Output eines Automaten auftritt, dessen Input die q-adische Ziffernentwicklung von n ist.

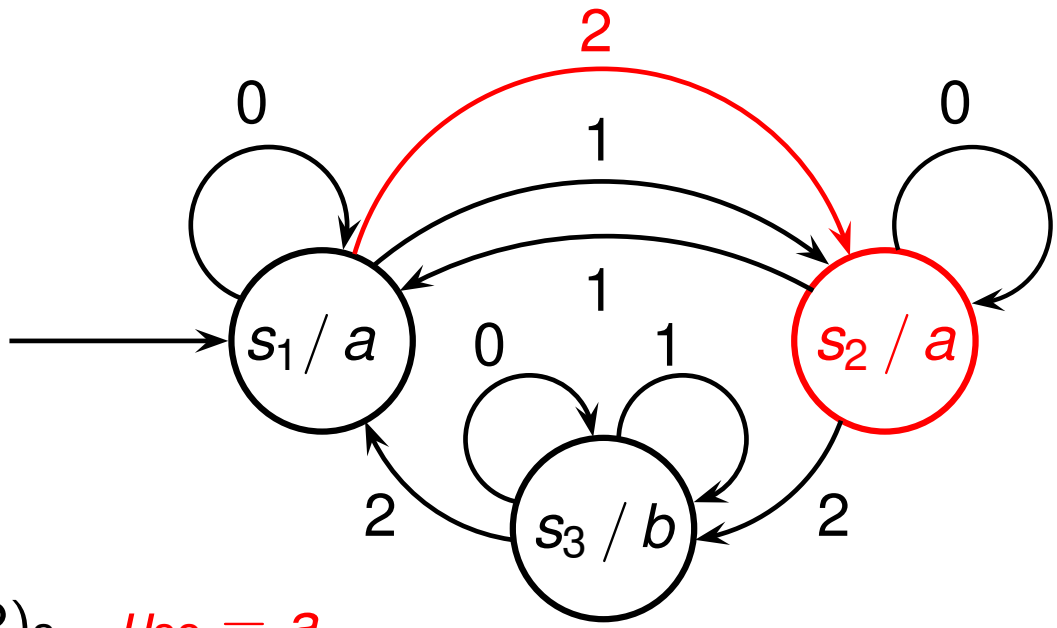


$32 = (1012)_3$

★ Automatische Folgen

Definition

Eine Folge $(u_n)_{n\geqslant 0}$ heißt *q-automatische Folge*, wenn sie u_n als Output eines Automaten auftritt, dessen Input die q-adische Ziffernentwicklung von n ist.

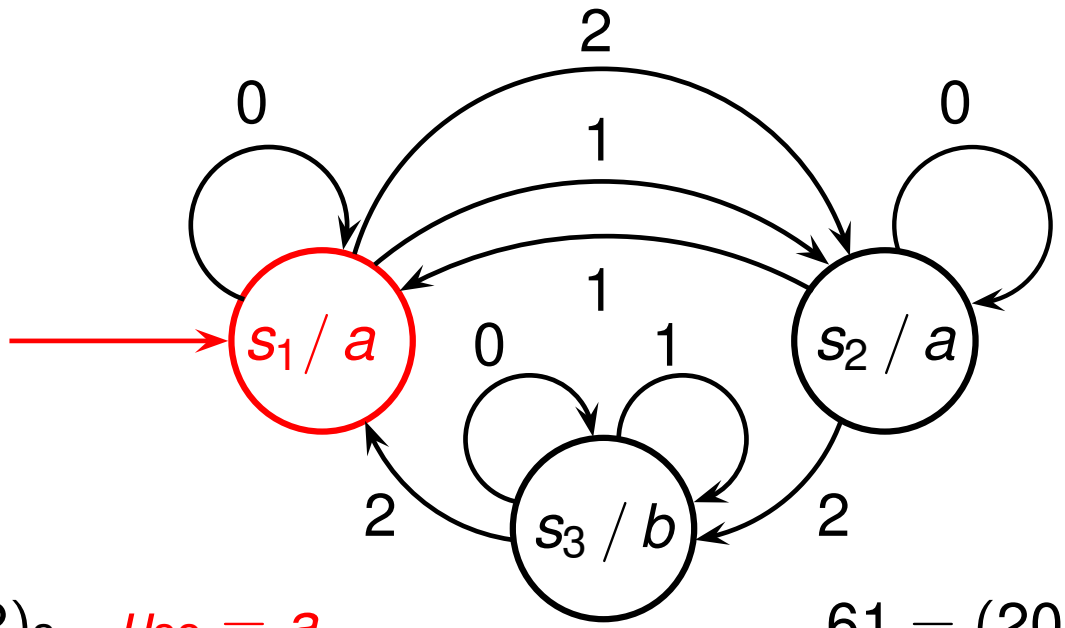


$32 = (1012)_3 \quad u_{32} = a,$

★ Automatische Folgen

Definition

Eine Folge $(u_n)_{n\geqslant 0}$ heißt *q-automatische Folge*, wenn sie u_n als Output eines Automaten auftritt, dessen Input die q-adische Ziffernentwicklung von n ist.

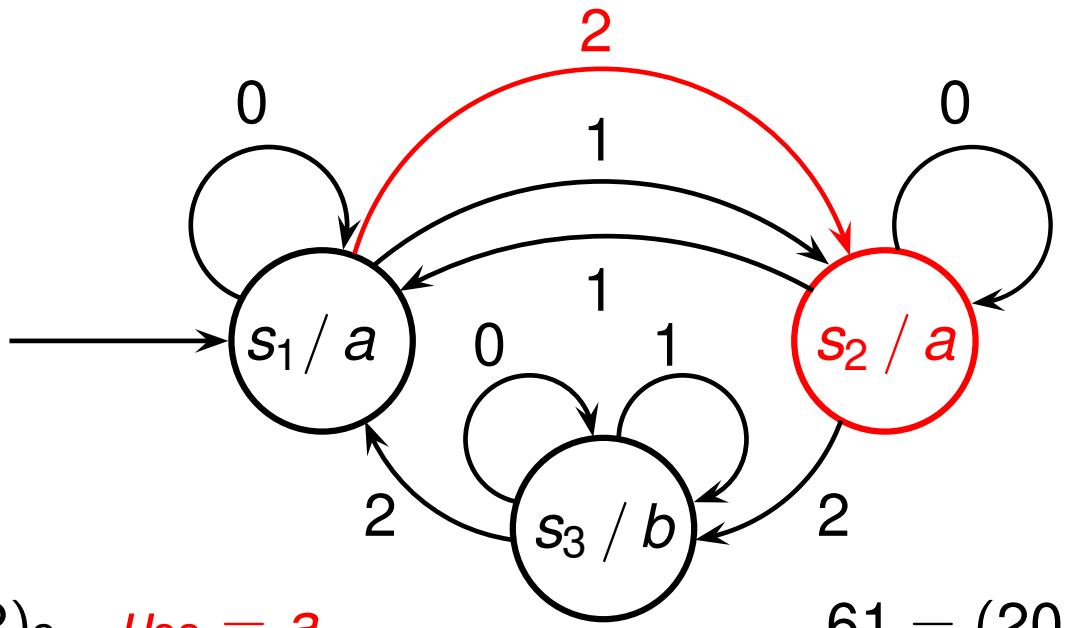


$32 = (1012)_3 \quad u_{32} = a, \qquad 61 = (2021)_3$

★ Automatische Folgen

Definition

Eine Folge $(u_n)_{n\geqslant 0}$ heißt *q-automatische Folge*, wenn sie u_n als Output eines Automaten auftritt, dessen Input die q-adische Ziffernentwicklung von n ist.

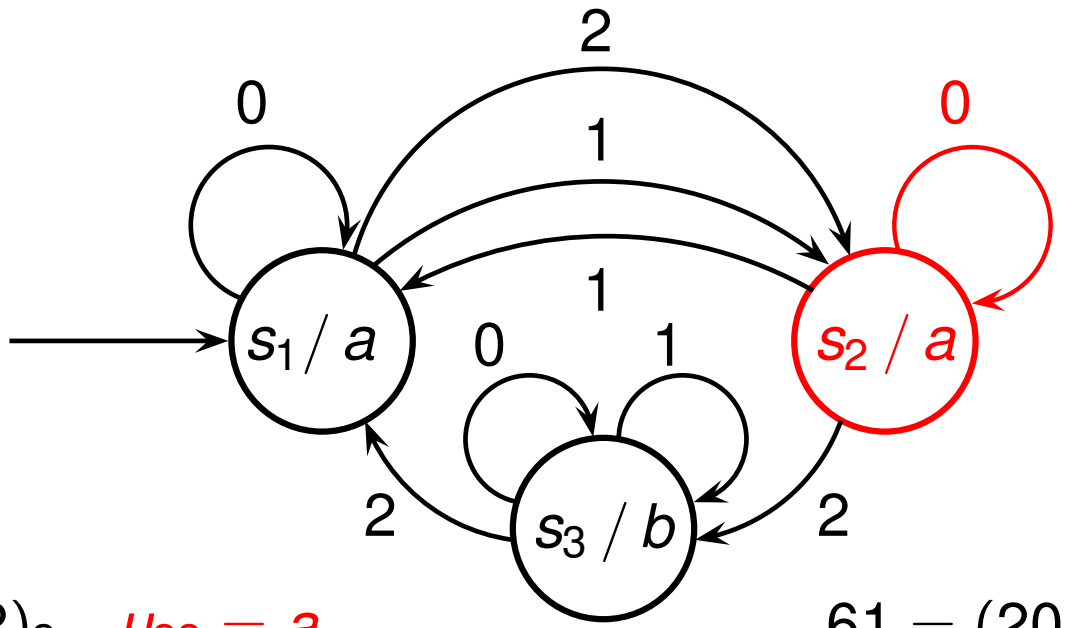


$32 = (1012)_3 \quad u_{32} = a, \qquad 61 = (2021)_3$

★ Automatische Folgen

Definition

Eine Folge $(u_n)_{n\geqslant 0}$ heißt *q-automatische Folge*, wenn sie u_n als Output eines Automaten auftritt, dessen Input die q-adische Ziffernentwicklung von n ist.

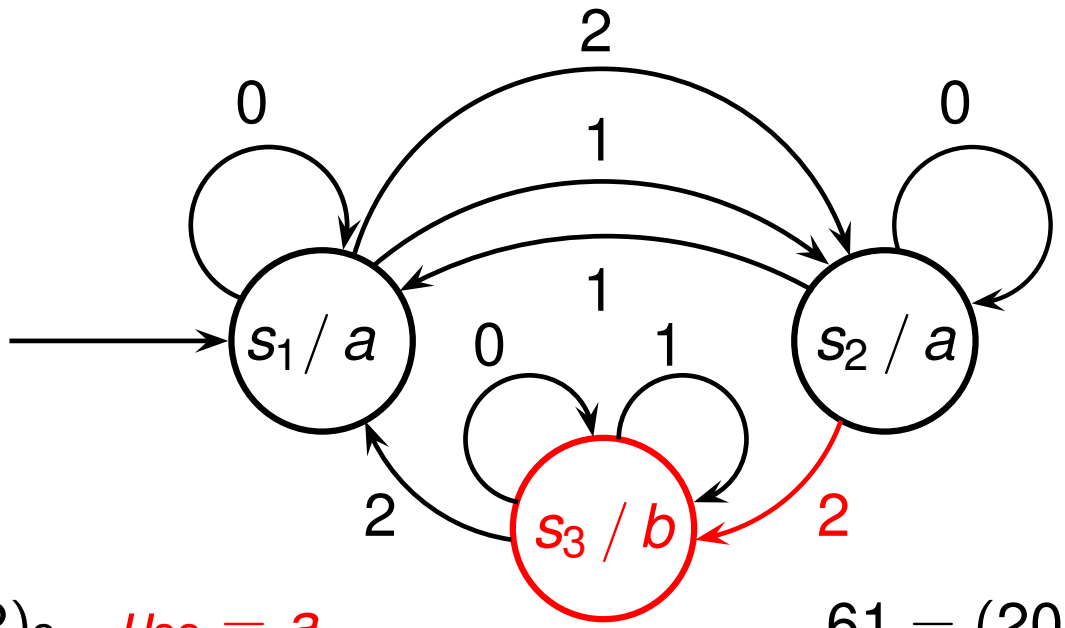


$32 = (1012)_3 \quad u_{32} = a, \qquad 61 = (2021)_3$

★ Automatische Folgen

Definition

Eine Folge $(u_n)_{n\geqslant 0}$ heißt *q-automatische Folge*, wenn sie u_n als Output eines Automaten auftritt, dessen Input die q-adische Ziffernentwicklung von n ist.

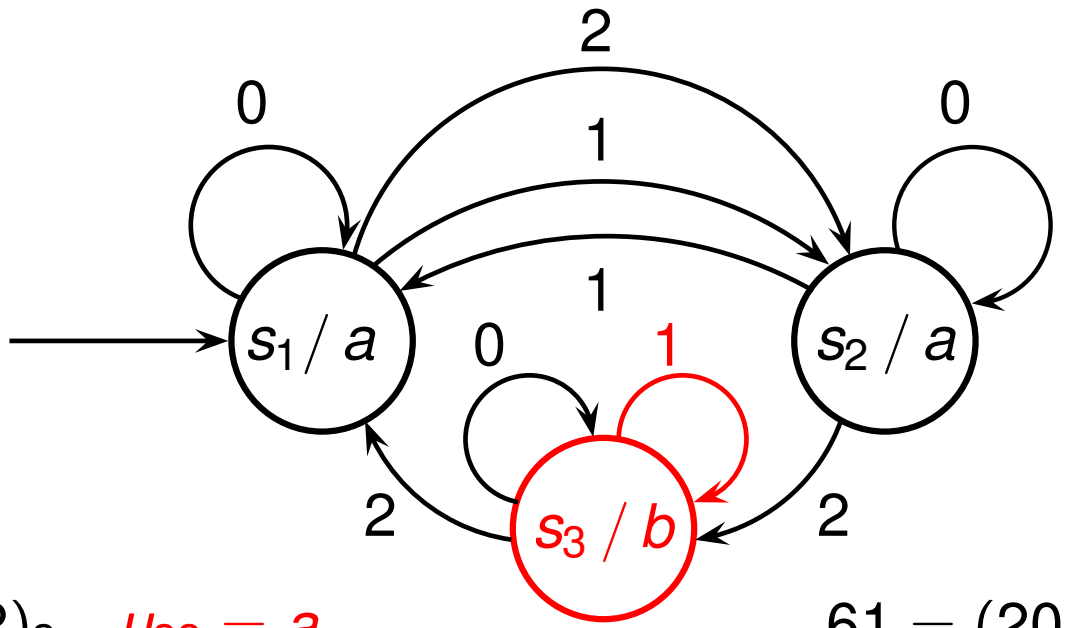


$32 = (1012)_3 \quad u_{32} = a, \qquad 61 = (2021)_3$

★ Automatische Folgen

Definition

Eine Folge $(u_n)_{n\geqslant 0}$ heißt *q-automatische Folge*, wenn sie u_n als Output eines Automaten auftritt, dessen Input die q-adische Ziffernentwicklung von n ist.

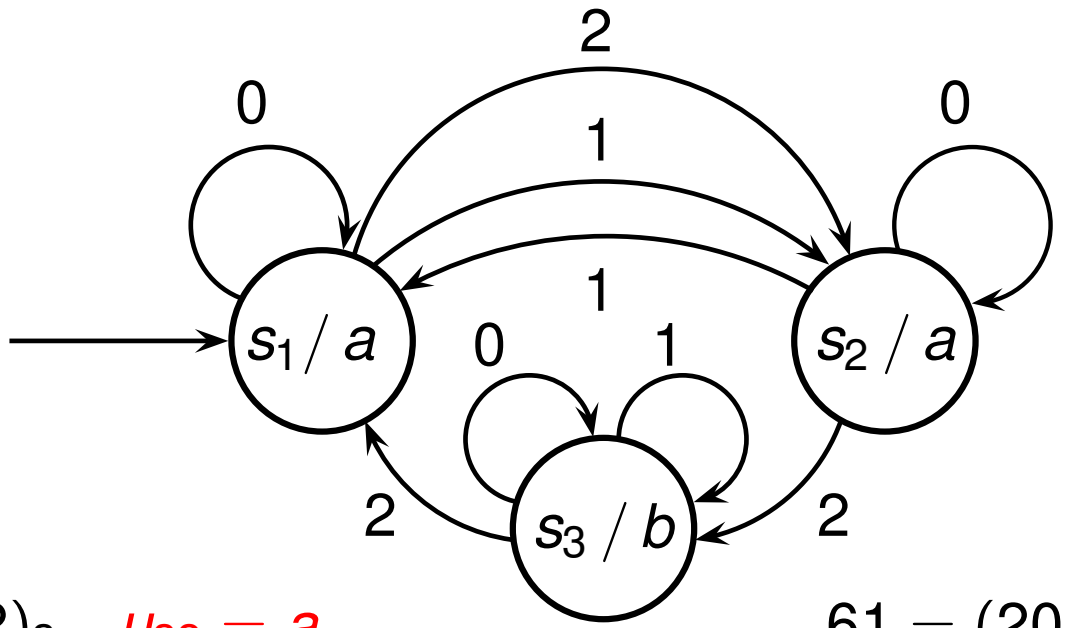


$32 = (1012)_3 \quad u_{32} = a,$ $\qquad$ $61 = (2021)_3 \quad u_{61} = b$

★ Automatische Folgen

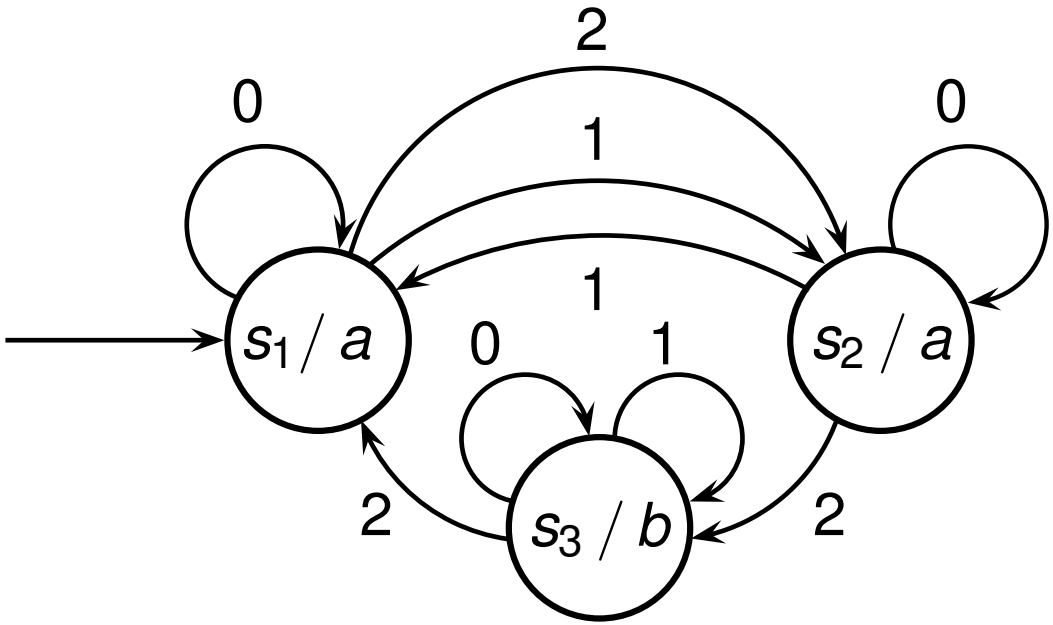
Definition

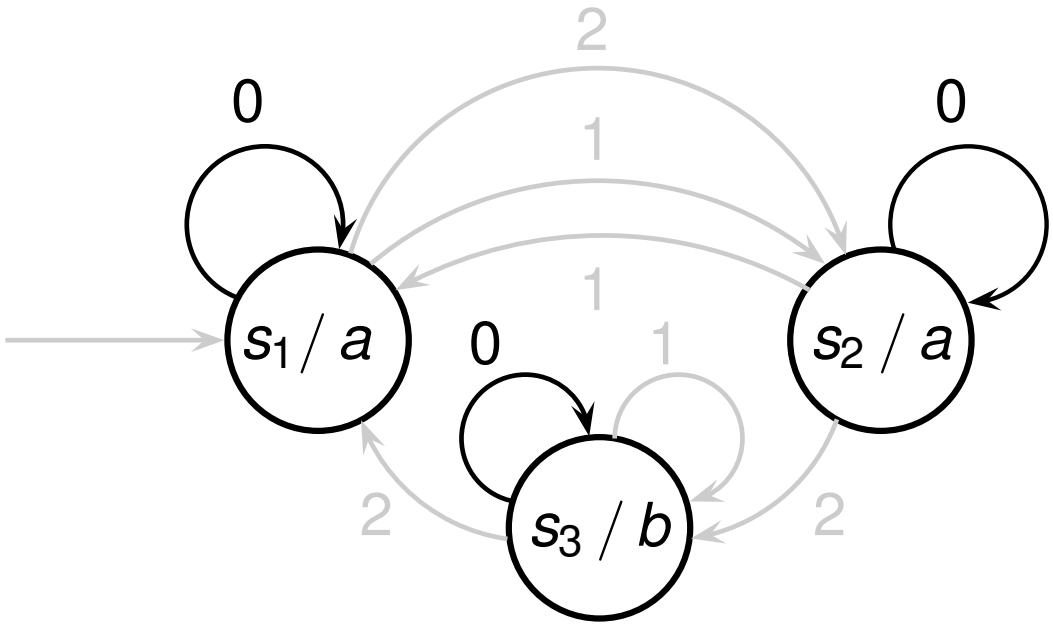
Eine Folge $(u_n)_{n\geqslant 0}$ heißt *q-automatische Folge*, wenn sie u_n als Output eines Automaten auftritt, dessen Input die q-adische Ziffernentwicklung von n ist.



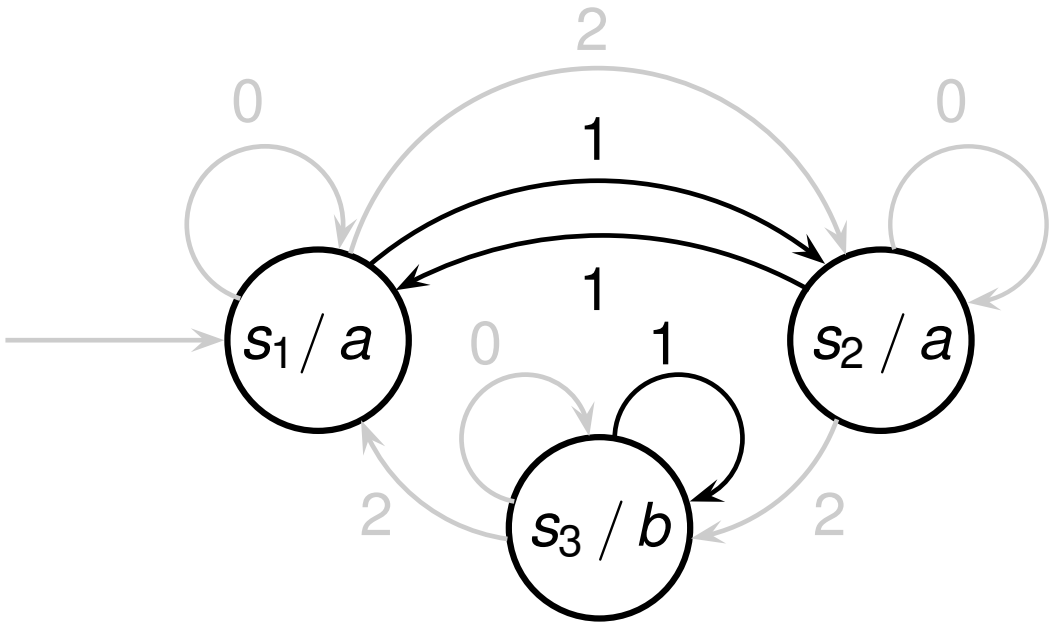
$32 = (1012)_3 \quad u_{32} = a,$ $\qquad 61 = (2021)_3 \quad u_{61} = b$

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

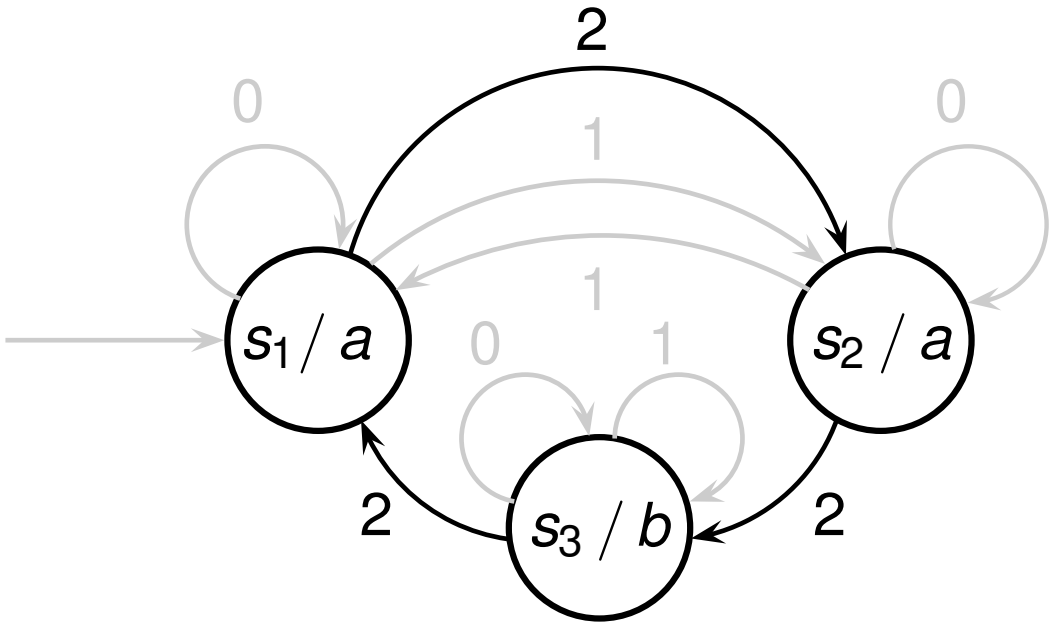

2
0
1
0
1
s_1 / a
0
1
s_2 / a
2
s_3 / b
2



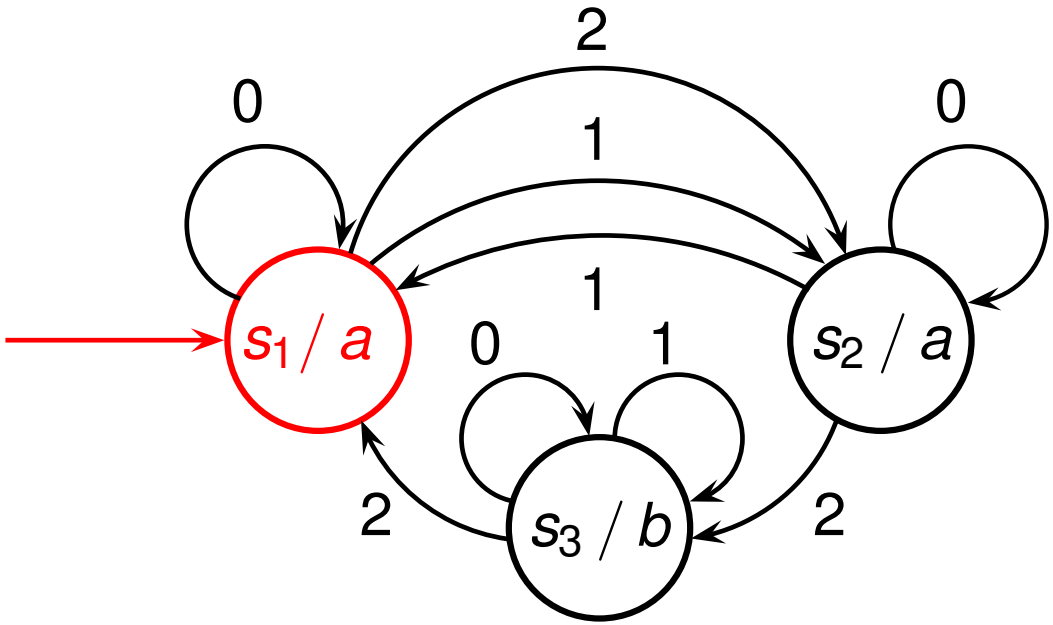
$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$



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



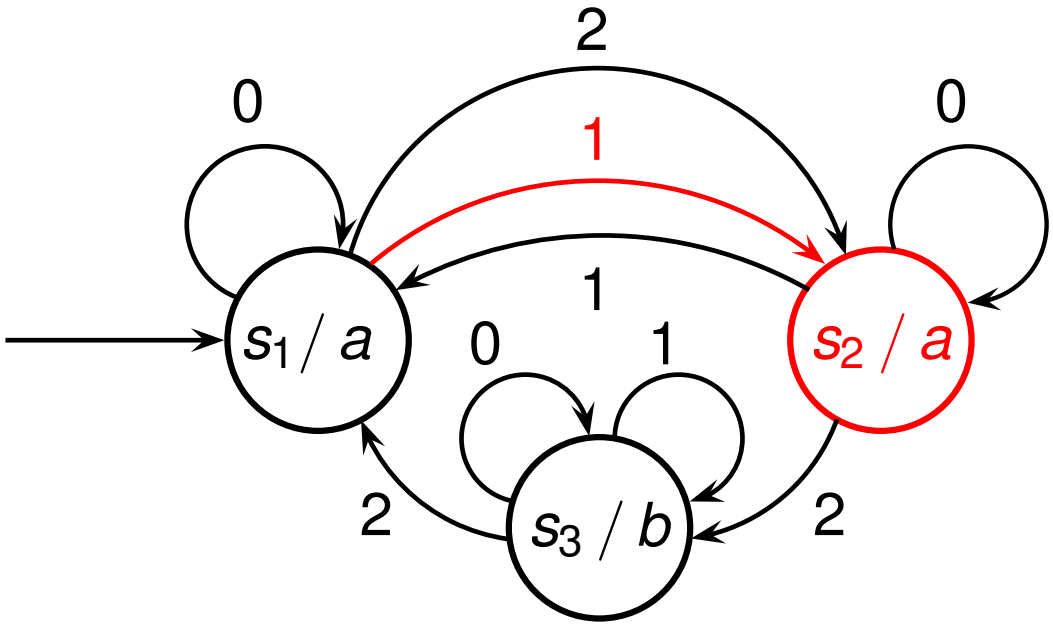
$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$



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

$32 = (1012)_3$:

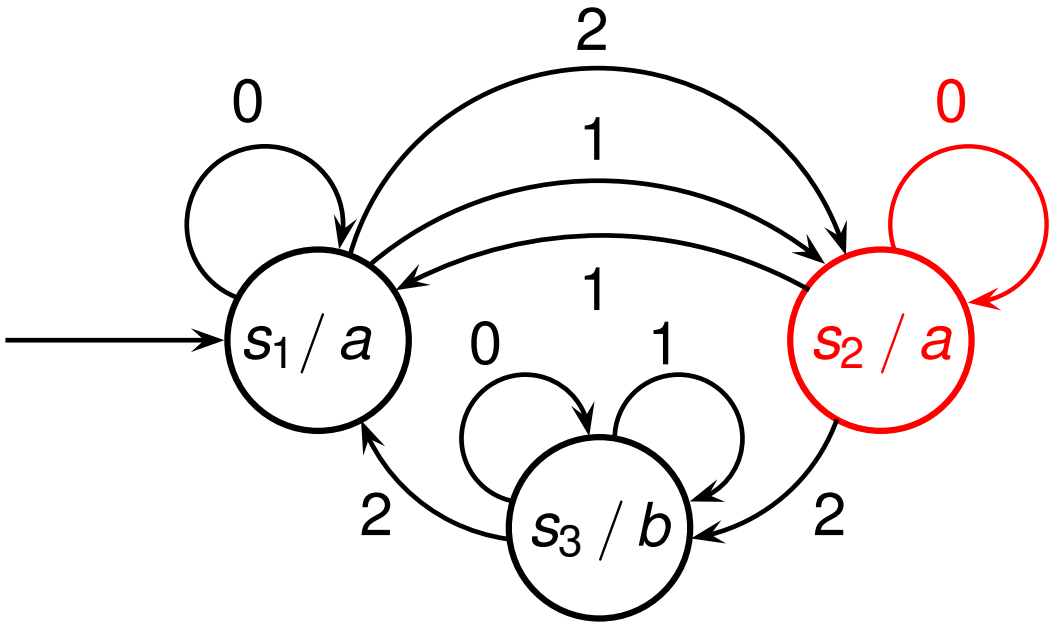
$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$



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

$32 = (1012)_3$:

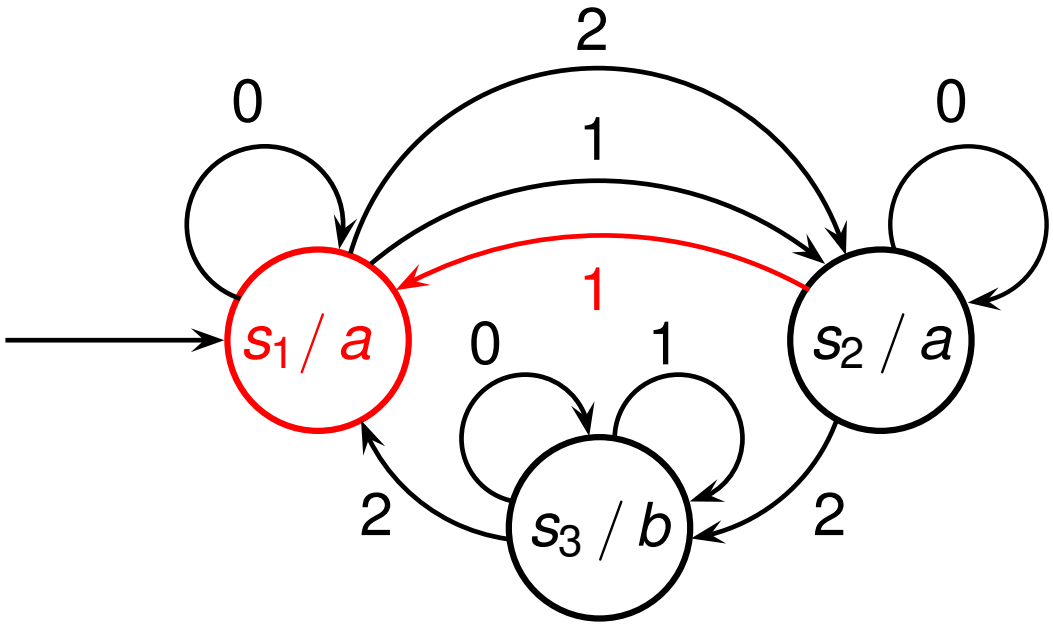
$$M_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$



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

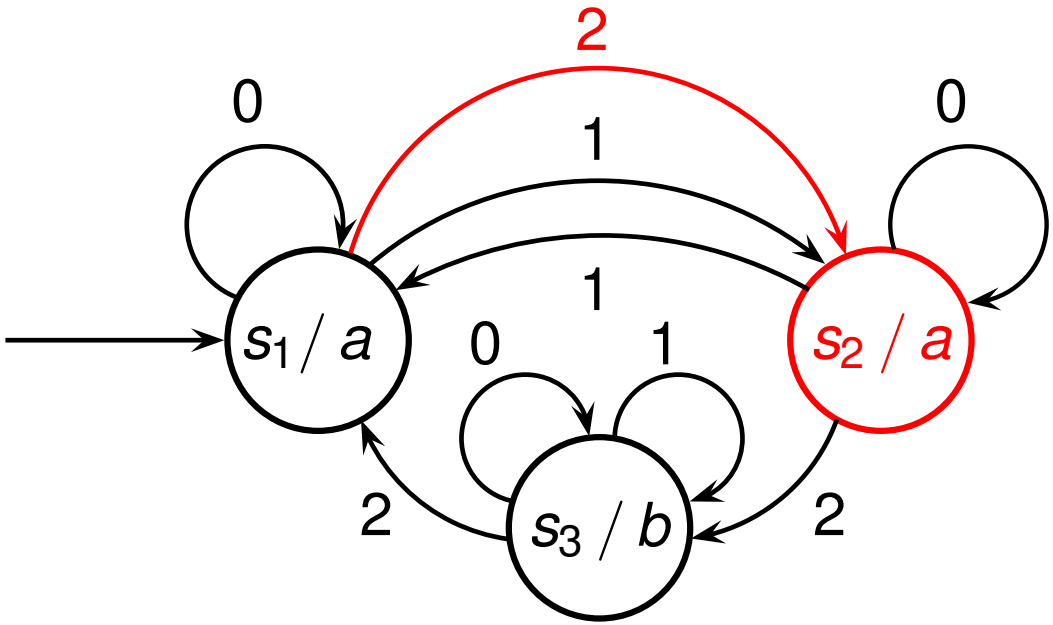
$32 = (1012)_3$:

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



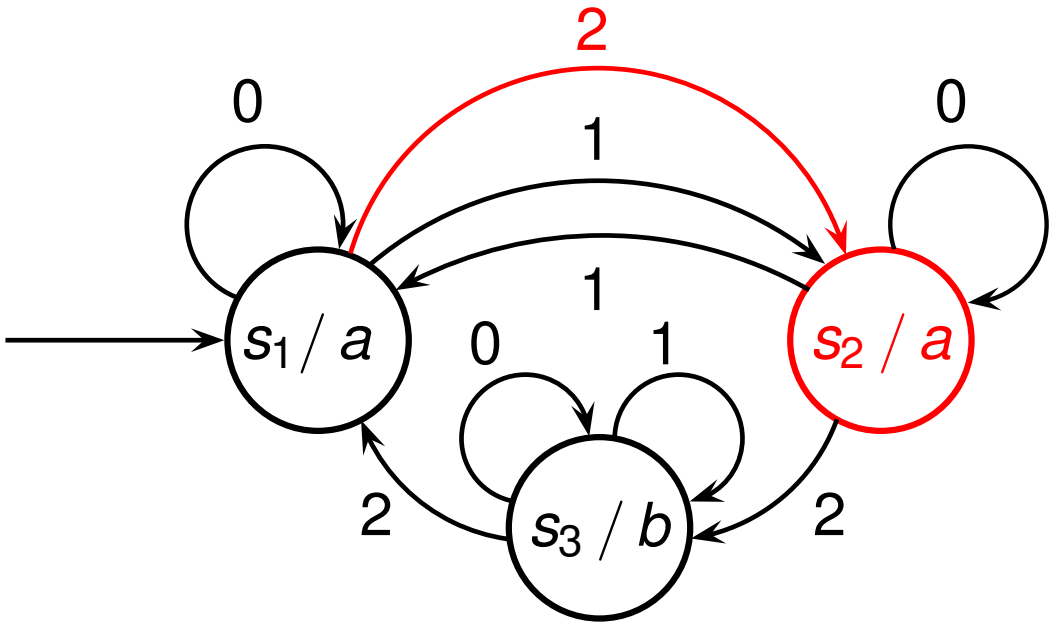
$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

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



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

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



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

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

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

★ Automatische Folgen

Satz

Die Komplexität einer automatischen Folge (u_n) *ist sub-linear, d.h. es gibt eine Konstante* $C > 0$ *mit*

$$L(m) \leqslant C\, m \qquad (m \geqslant 1).$$

Insbesondere gilt daher

$$h = \lim_{m\to\infty} \frac{\log L(m)}{m} = 0,$$

d.h. jede automatische Folge ist deterministisch.

★ Automatische Folgen

Satz

Die Komplexität einer automatischen Folge (u_n) *ist sub-linear, d.h. es gibt eine Konstante* $C > 0$ *mit*

$$L(m) \leqslant C\, m \qquad (m \geqslant 1).$$

Insbesondere gilt daher

$$h = \lim_{m\to\infty} \frac{\log L(m)}{m} = 0,$$

d.h. jede automatische Folge ist deterministisch.

Die Sarnak-Vermutung sollte daher für alle automatische Folgen (u_n) gelten:

$$\sum_{n\leqslant N} \mu(n) u_n = o(N) \qquad (N \to \infty).$$

★ Automatische Folgen und die Sarnak-Vermutung

Satz (Clemens Müllner, 2016+)

Jede automatische Folge (u_n) *erfüllt die Sarnak-Vermutung.*

★ Automatische Folgen und die Sarnak-Vermutung

Satz (Clemens Müllner, 2016+)

Jede automatische Folge (u_n) *erfüllt die Sarnak-Vermutung.*

Vorarbeiten:

- *Thue-Morse-Folge* (Dartyge+Tenenbaum)
- *Rudin-Shapiro-Folge* (Mauduit+Rivat, Tao)
- *Invertierbare automatische Folgen* (Drmota, Ferenczi et al.)
- *Synchronisierende automatische Folgen* (Deshouillers+D.+Müllner)

★ Automatische Folgen und Primzahlen

Man sagt, eine Teilmenge $\mathcal{L}$ der natürlichen Zahlen **wird von einem Automaten A erkannt**, wenn

$$\mathcal{L} = \{n \in \mathbb{N} : u_n = a\}$$

für die automatische Folge u_n, die von A erzeugt wird, und für ein a.

★ Automatische Folgen und Primzahlen

Man sagt, eine Teilmenge $\mathcal{L}$ der natürlichen Zahlen **wird von einem Automaten A erkannt**, wenn

$$\mathcal{L} = \{n \in \mathbb{N} : u_n = a\}$$

für die automatische Folge u_n, die von A erzeugt wird, und für ein a.

Beispiel:

$$\begin{aligned}\mathcal{L} &= \{n \in \mathbb{N} : t_n = 0\} \\ &= \{n \in \mathbb{N} : s_2(n) \equiv 0 \bmod 2\} \\ &= \{0, 3, 5, 6, 9, 10, 12, 15, \ldots\}\end{aligned}$$

($s_2(n)$ ... binäre Ziffernsumme, $t(n) = s_2(n) \bmod 2$)

★ Automatische Folgen und Primzahlen

Satz (Clemens Müllner, 2016+)

Sei A ein stark zusammenhängender Automat mit der Eigenschaft, dass ein 0-Input im Anfangszustand keinen Zustandswechsel verursacht. Weiters sei $\mathcal{L}$ eine nicht-leere Teilmenge der natürlichen Zahlen, die von A erkannt wird. Dann gilt

$$\text{Anzahl der Primzahlen } p \text{ in } \mathcal{L} \text{ mit } p \leqslant x \sim c\frac{x}{\log x}$$

für eine positive Zahl c.

★ Automatische Folgen und Primzahlen

Satz (Clemens Müllner, 2016+)

Sei A ein stark zusammenhängender Automat mit der Eigenschaft, dass ein 0-Input im Anfangszustand keinen Zustandswechsel verursacht. Weiters sei $\mathcal{L}$ eine nicht-leere Teilmenge der natürlichen Zahlen, die von A erkannt wird. Dann gilt

$$\textit{Anzahl der Primzahlen } p \textit{ in } \mathcal{L} \textit{ mit } p \leqslant x \sim c\frac{x}{\log x}$$

für eine positive Zahl c.

Beispiel (Mauduit+Rivat):

$$\text{Anzahl der Primzahlen } p \leqslant x \text{ mit } s_2(p) \equiv 0 \bmod 2 \sim \frac{1}{2}\frac{x}{\log x}$$

★ Automatische Folgen und Primzahlen

Satz (Drmota+Mauduit+Rivat, 2009)

$$\textit{Anzahl der Primzahlen } p \leqslant 2^{2k} \textit{ mit } s_2(p) = k \ \sim \frac{2^{2k}}{\sqrt{2\pi}\log 2\, k^{\frac{3}{2}}}$$

★ Automatische Folgen und Primzahlen

Satz (Drmota+Mauduit+Rivat, 2009)

$$\textit{Anzahl der Primzahlen } p \leqslant 2^{2k} \textit{ mit } s_2(p) = k \ \sim \frac{2^{2k}}{\sqrt{2\pi}\log 2\, k^{\frac{3}{2}}}$$

Im speziellen gibt es für jede (genügend große) natürliche Zahl k eine Primzahl p mit

$$s_2(p) = k.$$

Vielen Dank für die Aufmerksamkeit!