Random functions from coupled dynamical systems

Lucilla Baldini and Josef Eschgfäller

Università degli Studi di Ferrara

lucilla.baldini@unife.it & esg@unife.it

Abstract

Let $f : T \longrightarrow T$ be a mapping and Ω be a subset of T which intersects every (positive) orbit of f. Assume that there are given a second dynamical system $\lambda : Y \longrightarrow Y$ and a mapping $\alpha : \Omega \longrightarrow Y$. For $t \in T$ let $\delta(t)$ be the smallest k such that $f^k(t) \in \Omega$ and let $t_\Omega := f^{\delta(t)}(t)$ be the first element in the orbit of t which belongs to Ω. Then we define a mapping $F : T \longrightarrow Y$ by $F(t) := \lambda^{\delta(t)}(t_\Omega)$.

Keywords: Random number generator, pseudorandom sequence, weak attractor, coupled dynamical systems, Möbius transformations, finite fields.

1. Weak attractors

We use the notation $\mathop{\bigcirc}\limits_x f(x)$, introduced in [**7**], for the mapping $x \longmapsto f(x)$. The symbol $\bigcirc$ can be obtained in Latex with

```
\newcommand {\Fun} {\mathop{\bigcirc}\limits}.
```

Standing hypothesis 1.1. Let T be a non-empty set and $f : T \longrightarrow T$ a mapping.

Definition 1.2. For a subset $A \subset T$ we put

$$f^*(A) := \{t \in T \mid f^k(t) \in A \text{ for some } k \in \mathbb{N}\} = \bigcup_{k=0}^{\infty} f^{-k}(A)$$

Definition 1.3. A subset $\Omega \subset T$ is called a *weak attractor* (of f), if $f^*(\Omega) = T$, i.e., if for every $t \in T$ there exists $k \in \mathbb{N}$ such that $f^k(t) \in \Omega$. In this case for $t \in T$ we put

$$\delta(t) := \delta(t, \Omega, f) := \min\{k \in \mathbb{N} \mid f^k(t) \in \Omega\}$$

$$t_\Omega := f^{\delta(t)}(t)$$

t_Ω is therefore the first element of Ω we reach from t using f.

Example 1.4. Let T be finite. It is well known that then T can be written as the disjoint union

$$T = f^*(M_1) \sqcup \ldots \sqcup f^*(M_m)$$

where $M_1, \ldots, M_m$ are the minimal orbits of the dynamical system (T, f). On each M_j the restriction $f_{M_j \longrightarrow M_j}$ is a bijection.

A subset $\Omega \subset T$ is a weak attractor iff $\Omega \cap M_j \neq \emptyset$ for every $j = 1, \ldots, m$.

Remark 1.5. Let Ω be a weak attractor and $t \in T \setminus \Omega$.

Then $\delta(f(t)) = \delta(t) - 1$. Therefore δ assumes all elements of $\{0, 1, \ldots, \delta(t)\}$ as values. Furthermore $\Omega = (\delta = 0)$.

Proposition 1.6. *Let $\epsilon : T \longrightarrow \mathbb{N}$ be a function which, for every $t \in T$, assumes all elements of $\{0, 1, \ldots, \epsilon(t)\}$ as values. Then:*

(1) $\Omega := (\epsilon = 0) \neq \emptyset$.

(2) There exists a mapping $g : T \longrightarrow T$ such that Ω is a weak attractor of g and $\epsilon(t) = \delta(t, \Omega, g)$ for every $t \in T$.

Proof. Easy. See Prop. 13.9 in [**2**].

2. Coupled dynamical systems

Standing hypothesis 2.1. Let the following data be given:

(1) A set T and a mapping $f : T \longrightarrow T$.

(2) A weak attractor Ω of f.

(3) A set Y and a mapping $\lambda : Y \longrightarrow Y$.

(4) A mapping $\alpha : \Omega \longrightarrow Y$.

We suppose that the sets T, Ω and Y be non-empty.

The triple of mappings (f, λ, α) is then called a *coupled dynamical system*.

Remark 2.2. In [**2**] a slightly more general concept of *automatic generator* (of pseudorandom functions) has been defined, mainly in order to include also *automatic sequences* (as defined for example in Allouche/Shallit [**1**]).

Proposition 2.3. *For $t \in T$ let*

$$F(t) := \begin{cases} \alpha(t) & \textit{if } t \in \Omega \\ \lambda(F(f(t))) & \textit{if } t \notin \Omega \end{cases}$$

In this way we obtain a well defined mapping $F : T \longrightarrow Y$ which extends α and which we call the pseudorandom function generated by the triple (f, λ, α).

Remark 2.4. In Proposition 2.3 for every $t \in T$ we have

$$F(t) = \lambda^{\delta(t)}(\alpha(f^{\delta(t)}(t))) = \lambda^{\delta(t)}(\alpha(t_\Omega))$$

Remark 2.5. If the mapping $\lambda : Y \longrightarrow Y$ is the identity, then $F(t) = \alpha(t_\Omega)$ for every $t \in T$.

Remark 2.6. The most studied classical random sequence generators derive from a mapping $\lambda : Y \longrightarrow Y$ which for every choice of an initial point $y_0 \in Y$ gives rise to a sequence

$$F := \bigcirc_{n} \lambda^n(y_0) : \mathbb{N} \longrightarrow Y$$

This can (in a trivial way) be considered as a special case of Proposition 2.3: It suffices to set $T := \mathbb{N}$, $\Omega := \{0\}$, and

$$f(n) := \begin{cases} n-1 & \text{if } n > 0 \\ 0 & \text{if } n = 0 \end{cases}$$

with $\alpha := \bigcirc_{0} y_0 : \Omega \longrightarrow Y$.

Then $\delta(n) = n$ for every $n \in \mathbb{N}$ and from Remark 2.4 we have $F(n) = \lambda^n(y_0)$ for every $n \in \mathbb{N}$.

Remark 2.7. In another trivial way one can obtain every mapping $F : T \longrightarrow Y$ with the construction of Proposition 2.3: We put $\Omega := T$, $\alpha := F$ with f and λ (both unused) chosen arbitrarily.

Remark 2.8. Let $a, b \in T \setminus \Omega$ be such that $f(a) = f(b)$.

Then $F(a) = F(b)$.

Proof. This follows from Proposition 2.3.

Lemma 2.9. *Let $a, b \in T$ and $j, k \in \mathbb{N}$ be such that the following conditions hold:*

(1) $j \leq \delta(a)$ and $k \leq \delta(b)$.
This means that $f^r(a) \notin \Omega$ for $0 \leq r < j$ and $f^r(b) \notin \Omega$ for $0 \leq r < k$.

(2) $j \leq k$.

(3) $f^j(a) = f^k(b)$.

Then $F(b) = \lambda^{k-j}(F(a))$.

Proof. Let $c := f^j(a) = f^k b)$ and $m := \delta(c)$. Then

$\delta(a) = m + j$ and $\delta(b) = m + k$. By condition (3)

$f^{j+m}(a) = f^{k+m}(b) =: \omega \in \Omega$

thus

$$F(a) = \lambda^{m+j}(\alpha(f^{m+j}(a))) = \lambda^{m+j}(\alpha(\omega))$$

and similarly

$$\begin{aligned} F(b) &= \lambda^{m+k}(\alpha(f^{m+k}(b))) \\ &= \lambda^{m+k}(\alpha(\omega)) = \lambda^{k-j+m+j}(\alpha(\omega)) \\ &= \lambda^{k-j}(\lambda^{m+j}(\alpha(\omega))) = \lambda^{k-j}(F(a)) \end{aligned}$$

Remark 2.10. The mapping $\delta : T \longrightarrow \mathbb{N}$ itself can be considered as a pseudo-random mapping and as a special case of Proposition 2.3. For this put

$$Y := \mathbb{N},\ \lambda := \bigcirc_{n} n+1,\ \alpha := \bigcirc_{\omega} 0 : \Omega \longrightarrow \mathbb{N}$$

Then $F(a) = \lambda^{\delta(a)}(0) = \delta(a)$ for every $a \in T$ and therefore $F = \delta$.

3. Examples

Standing hypothesis 3.1. In this section, for each coupled dynamical system $(f : T \longrightarrow T, \lambda : Y \longrightarrow Y, \alpha : \Omega \longrightarrow \Omega)$ we denote by F the function generated by the method of Proposition 2.3.

The examples have been calculated with Pari/GP ([102] und [103] in Baldini [**2**]).

For $a \in \mathbb{N}$ and $b \in \mathbb{N}+1$ we denote, as in Pari/GP, by $a \setminus b$ the integer quotient of a by b; e.g. $13 \setminus 5 = 2$. The remainder in the division is denoted by $a \bmod b$.

$\mathbb{P}$ is the set of primes.

Remark 3.2. Let α be constant, say $\alpha(\omega) = y_0$ for every $\omega \in \Omega$. Then $F(t) = \lambda^{\delta(t)}(y_0)$ for every $t \in T$.

As in Proposition 1.6 we don't need to specify $f : T \longrightarrow T$ and $\Omega \subset T$ explicitly; is suffices that there is given a function $\delta : T \longrightarrow \mathbb{N}$ which for every $t \in T$ assumes all elements of $\{0, 1, \ldots, \delta(t)\}$ as values.

Example 3.3. Let $T := \mathbb{N}$ and $f : \mathbb{N} \longrightarrow \mathbb{N}$ be defined by

$$f(n) = \begin{cases} n/3 & \text{if } n \in 3\mathbb{N} \\ (n+1) \setminus 2 & \text{if } n \in 3\mathbb{N}+1 \\ n-2 & \text{if } n \in 3\mathbb{N}+2 \end{cases}$$

Since $f(n) < n$ for every $n \geq 2$, we can choose the set $\Omega := \{0, 1, 2, 3\}$ as weak attractor. Define then $Y := \{0, 1\}$, $\alpha(n) := n \bmod 2$, $\lambda(y) := 1 - y$.

The following table gives the values of $F(n)$ for $n = 0, \ldots, 319$.

0	1	0	1	1	0	1	0	0	0	1	1	0	1	1	1	1	0	0	0	1	1	0	0	1	0	0	1	0	0	0	0	1	0	1	1	1	1	0	0
0	1	0	1	1	0	1	1	0	1	1	1	1	0	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0	1	0	0	0	0	1	1	1	0	1	1
0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	0	0	0	0	1	0	1	1	0	0	1	0	1	1	1	0	0	1	1	0
1	0	0	0	0	1	1	1	0	0	0	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	0	0	0	1	0	0	1	0	1	1	0	0	1	1
1	0	0	1	1	0	0	1	1	1	0	0	1	1	0	1	1	1	1	0	1	1	0	0	1	1	0	1	1	1	1	0	1	1	0	0	0	1	0	1
1	1	1	0	1	1	0	0	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	0	1	0	0	1	0	1	1	1	1	0	0	0	1	0	1	1
1	1	0	1	1	0	1	1	0	0	0	1	0	0	1	1	1	0	1	1	0	0	0	1	1	0	0	1	0	0	0	0	1	1	1	0	1	0	0	0
0	1	1	0	0	1	0	0	1	0	0	1	1	0	0	1	1	0	0	1	1	1	0	1	0	0	1	0	0	1	0	0	0	1	1	1	0	0	0	0

Remark 3.4. We shall often subsume the items in Proposition 2.3 within a table of the following form:

T	$\ldots$
$f(n)$	$\ldots$
Ω	$\ldots$
Y	$\ldots$
$\alpha(n)$	$\ldots$
$\lambda(y)$	$\ldots$

Example 3.5. For $n \in \mathbb{N}+1$ we denote by $\tau(n)$ the number of (positive) divisors of n. Consider then

T	$\mathbb{N}+2$
$f(n)$	$\tau(n)$
Ω	$\{2\}$
Y	$\{0,1\}$
$\alpha(n)$	0
$\lambda(y)$	$1-y$

Observe that $\tau(2)=2$ and $2 \le \tau(n) < n$ for $n \ge 3$, so that $\Omega := \{2\}$ is indeed a weak attractor of f.

We calculate the values of $F(n)$ for $2 \le n \le 321$:

```
0 1 0 1 1 1 1 0 1 1 0 1 1 1 0 1 0 1 0 1 1 1 0 0 1 1 0 1 0 1 0 1 1 1 1 1 1 1 0 1
0 1 0 0 1 1 0 0 0 1 0 1 0 1 0 1 1 1 1 1 1 0 0 1 0 1 0 1 0 1 1 1 1 0 0 1 0 1 0 0
1 1 1 1 1 1 0 1 1 1 0 1 1 1 1 1 0 0 1 1 0 1 0 0 1 1 1 1 0 1 0 1 0 1 0 0 1 1 1 0
1 1 0 1 1 1 0 1 0 1 1 1 1 0 0 1 0 1 1 1 1 1 0 1 1 0 0 1 1 1 0 0 0 1 1 1 1 1 1 1
0 1 0 0 1 1 1 0 0 0 0 1 0 0 0 1 1 1 1 1 0 1 0 1 0 1 0 0 0 1 0 1 1 0 1 1 1 1 1 1
1 1 1 1 1 0 0 1 1 1 0 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 0 0 0 1 1 1 0 1 0 1 1 1
0 0 0 0 0 1 0 1 0 1 1 1 1 0 1 1 0 1 1 0 1 1 1 1 0 1 0 1 1 1 0 0 1 0 1 1 1 0 1 1
0 1 0 0 0 1 1 0 0 1 0 1 1 1 0 0 1 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 1 0 1
```

Example 3.6. For $n \in \mathbb{N}+1$ we denote by $\sigma(n)$ the sum of all (positive) divisors of n. For $n \ge 2$ then $\sigma(n) \ge 1+n$, hence the mapping $\sigma - 1 : \mathbb{N}+2 \longrightarrow \mathbb{N}+2$ is well defined. The prime numbers are exactly the fixed points of $\sigma - 1$:

$$\mathbb{P} = \mathrm{Fix}(\sigma - 1)$$

It is not known whether all orbits of $\sigma - 1$ are finite and whether every orbit ends in a prime. In Guy [**8**, p. 149], this conjecture is attributed to Erds; the final primes of the first orbits are listed on OEIS as sequence A039654.

If we put $T := \mathbb{N}+2$, $f := \sigma - 1$ and assume the conjecture to be true, $\Omega := \mathbb{P}$ becomes a weak attractor of f.

T	$\mathbb{N}+2$
$f(n)$	$\sigma(n)-1$
Ω	$\mathbb{P}$
Y	$\{0,1,2,3,4\}$
$\alpha(n)$	$n \bmod 5$
$\lambda(y)$	$(3y+2) \bmod 5$

```
2 3 2 0 0 2 0 0 3 1 1 3 1 1 2 2 4 4 0 0 1 3 4 2 0 3 2 4 0 1 3 3 1 3 0 2 4 2 4 1
2 3 1 3 0 2 1 2 1 0 3 3 0 0 0 4 4 4 3 1 2 1 2 1 1 2 3 2 1 1 0 3 1 1 4 2 3 4 1 4
3 3 1 3 0 0 4 4 1 2 3 3 1 0 0 2 4 2 4 1 0 3 4 0 2 2 2 4 0 0 3 3 4 1 4 0 4 1 4 0
1 3 1 2 0 2 0 1 0 1 1 2 4 4 4 2 0 4 1 0 0 3 2 4 2 3 4 4 2 1 0 1 0 0 2 2 4 0 4 0
4 3 1 0 0 2 4 0 4 0 3 3 4 3 2 4 4 4 4 1 1 3 4 3 1 0 1 4 4 1 1 3 1 1 4 2 3 4 4 0
3 4 1 0 0 0 1 4 0 1 4 0 4 1 4 2 0 4 1 0 2 3 1 2 0 2 1 4 0 1 4 3 4 0 4 4 0 4 1 1
4 4 1 0 1 2 4 1 3 1 3 0 1 0 2 2 2 1 3 4 4 3 4 4 4 4 4 4 4 1 3 4 4 2 0 2 4 0 4 1
0 3 1 4 1 1 4 2 0 2 2 3 1 4 4 4 4 1 1 0 2 3 4 2 0 2 0 0 0 1 4 3 3 4 1 2 3 4 0 0
```

Lemma 3.7. *Let* $a, b \in \mathbb{N}+1$ *and* $a \neq b$. *Then*

$$\max(|a-b|, (a+b) \setminus 2) < \max(a,b)$$

Proof. We may assume $a > b$. By hypothesis $b > 0$, hence

$$|a-b| = a-b < a = \max(a,b)$$

Also

$$(a+b) \setminus 2 \leq \frac{a+b}{2} < \frac{a+a}{2} = a = \max(a,b)$$

Corollary 3.8. *Define* $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ *by*

$$f(a,b) := \begin{cases} (a,a) & \textit{if } b = 0 \\ (b,b) & \textit{if } a = 0 \\ (|a-b|, (a+b) \setminus 2) & \textit{otherwise} \end{cases}$$

Then the diagonal $\Omega := \{(n,n) \mid n \in \mathbb{N}\}$ *is a weak attractor.*

Let Y *be another set. A map* $\alpha : \Omega \longrightarrow Y$ *can be identified with a map* $\alpha_0 : \mathbb{N} \longrightarrow Y$.

Given α_0, *for every map* $\lambda : Y \longrightarrow Y$ *we obtain a map* $F : \mathbb{N} \times \mathbb{N} \longrightarrow Y$.

Example 3.9.

T	$\mathbb{N} \times \mathbb{N}$
$f(n)$	as in Cor. 3.8
Ω	$\{(n,n) \mid n \in \mathbb{N}\}$
Y	$\{0,1,2,3\}$
$\alpha(n,n)$	$(3n+2) \bmod 4$
$\lambda(y)$	$(3y+1) \bmod 4$

```
2 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2
0 1 0 1 0 1 0 2 1 1 0 2 0 1 3 1 0 0 2 0 1 1 0 3 2 1 0 1 1 1 3 3 1 2 0 0 2 0 0 1
1 0 0 1 0 2 3 0 1 3 0 0 0 1 0 3 0 0 1 2 0 1 0 1 3 1 0 0 0 0 2 2 0 1 1 3 1 0 3 0
2 1 1 3 0 1 1 0 0 1 0 2 1 3 1 0 2 3 2 1 3 1 1 0 0 2 2 3 2 1 1 1 3 1 0 1 0 0 1 0
3 0 0 0 2 1 3 0 2 1 0 2 3 1 1 0 0 2 1 1 1 0 1 0 2 0 2 0 1 1 3 1 1 0 0 1 0 0 2 0
0 1 2 1 1 1 0 2 0 1 3 0 2 1 0 1 0 2 0 1 3 1 0 0 0 2 3 0 0 0 1 3 0 3 0 0 0 2 2 1
1 0 3 1 3 0 0 1 1 1 3 1 0 1 3 1 0 2 3 0 1 0 3 0 2 2 1 0 1 1 0 1 3 2 3 1 0 0 0 3
2 2 0 0 0 2 1 3 3 0 1 0 0 2 0 1 0 0 2 0 0 1 3 1 0 0 3 2 1 1 3 1 3 0 1 0 0 0 0 1
```

We obtain a map F that can be considered as an infinite pseudorandom matrix, which is symmetric by construction.

The principal diagonal is the periodic sequence $2103210321032103\ldots$. Indeed we have $F(n,n) = \alpha(n,n) = (3n+2) \bmod 4$ for all n.

Remark 3.10. Let $m \in \mathbb{N}+2$ and consider a coupled dynamical system $(f : T \longrightarrow T, \lambda : Y \longrightarrow Y, \alpha : \Omega \longrightarrow Y)$ in which $Y = \{0, 1, \ldots, m-1\}$ and $\lambda(y) = (y+1) \bmod m$ for every $y \in Y$. For $0 \le j \le m-1$ let $\Omega_j := \alpha^{-1}(j)$.

For $k \in \mathbb{N}$ and $y \in Y$ then $\lambda^k(y) = (y+k) \bmod m$ and therefore

$$F(t) = (j + \delta(t)) \bmod m$$

for $t \in \Omega_j$.

If in particular $\alpha = 0$, then $F(t) = \delta(t) \bmod 2$ for every $t \in T$.

Example 3.11. We show that the Thue-Morse sequence can be obtained by the method indicated at the end of Remark 3.10. The sequence can be defined in the following way (cf. Berstel/Karhumki [**3**, p. 69]):

$$x_0 = 0, \quad x_{2n} = x_n, \quad x_{2n+1} = 1 - x_n$$

Let $T := \mathbb{N}, \Omega := \{0\}, Y := \{0,1\}, \alpha(0) = 0, \lambda(y) = 1 - y$ and define the mapping $f : \mathbb{N} \longrightarrow \mathbb{N}$ by

$$f(n) := \begin{cases} n+1 & \text{if } n \text{ is even} \\ n \setminus 2 & \text{otherwise} \end{cases}$$

It is clear that then Ω is a weak attractor of f and that

$$\begin{aligned} \delta(0) &= 0 \\ \delta(2n) &= \delta(n) + 2 \text{ for every } n \ge 1 \\ \delta(2n+1) &= \delta(n) + 1 \text{ for every } n \ge 0 \end{aligned}$$

and therefore, by Remark 3.10,

$$\begin{aligned} F(0) &= 0 \\ F(2n) &= \delta(2n) \bmod 2 = \delta(n) \bmod 2 = F(n) \\ F(2n+1) &= (\delta(n)+1) \bmod 2 = 1 - \delta(n) \bmod 2 = 1 - F(n) \end{aligned}$$

This shows that $F(n) = x_n$ for every $n \in \mathbb{N}$.

The Thue-Morse sequence F can therefore be defined by the table

T	$\mathbb{N}$
$f(n)$	$n+1$ for n even
	$n \setminus 2$ for n odd
Ω	$\{0\}$
Y	$\{0,1\}$
$\alpha(0)$	0
$\lambda(y)$	$1-y$

Example 3.12. Define $f : \mathbb{N}+1 \longrightarrow \mathbb{N}+1$ by

$$f(n) := \begin{cases} 1 & \text{if } n = 1 \\ n - g(n) & \text{otherwise} \end{cases}$$

where $g(n)$ is the greatest divisor $\neq n$ of n. Therefore, if n is prime, then $g(n) = 1$ and $f(n) = n - 1$.

The dynamical system $(\mathbb{N}+1, f)$ has been studied by Collatz (cf. Lagarias [**10**, p. 241]). For $n > 1$ one has $f(n) < n$, therefore $\Omega := \{1\}$ is a weak attractor of f.

T	$\mathbb{N}+1$
$f(n)$	1 if $n = 1$
	$n - g(n)$ otherwise
$g(n)$	greatest divisor $\neq n$ of n
Ω	$\{1\}$
Y	$\{0,1\}$
$\alpha(n)$	0
$\lambda(y)$	$1-y$

```
0 1 0 0 1 1 0 1 0 0 1 0 1 1 1 0 1 1 0 1 0 0 1 1 0 0 0 0 1 0 1 1 1 0 1 0 1 1 1 0
1 1 0 1 1 0 1 0 0 1 1 1 0 1 0 1 0 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 0 0 0 0 1 0 1 1
0 0 1 0 0 1 1 0 1 0 1 1 1 0 1 1 0 1 1 0 1 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 0 1 0
0 1 1 1 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 1 1 0 0 0 0 1 0 1 0 1 0 1 1 0 0 1 0 0 0 0
1 1 0 1 0 0 1 1 0 1 0 0 1 0 0 1 1 0 1 1 0 0 0 0 0 0 0 1 0 0 1 0 1 1 0 0 1 0 1 1
1 0 1 1 0 0 1 1 1 0 1 0 1 1 1 1 1 0 0 0 0 0 1 1 0 0 1 0 1 1 1 0 1 0 0 1 1 0 1 1
0 1 0 0 1 0 1 0 1 0 1 0 0 1 0 0 1 1 1 0 1 1 0 0 1 1 1 1 0 0 1 1 1 0 1 1 0 0 1 0
1 0 1 1 1 1 1 1 0 1 0 0 1 1 0 0 1 1 0 0 0 1 1 0 1 0 1 1 1 1 0 0 1 1 1 1 0 1 0 1
```

Example 3.13. Mimicking Example 3.12, we define

$$f(n) := \begin{cases} 1 & \text{if } n \leq 1 \\ n - h(n) & \text{otherwise} \end{cases}$$

where, for $n \geq 2$, $h(n)$ is the smallest divisor $\neq 1$ of n. Hence $f(p) = 0$ if p is prime. We obtain a dynamical system $(\mathbb{N}, f)$.

For $n > 1$ one has $f(n) < n$, therefore $\Omega := \{0, 1\}$ is a weak attractor.

T	$\mathbb{N}$
$f(n)$	n if $n \leq 1$
	$n - h(n)$ otherwise
$h(n)$	smallest divisor $\neq 1$ of n
Ω	$\{0, 1\}$
Y	$\{0, 1\}$
$\alpha(n)$	n
$\lambda(y)$	$1 - y$

```
0 1 1 1 0 1 1 1 0 0 1 1 0 1 1 1 0 1 1 1 0 0 1 1 0 1 1 1 0 1 1 1 0 0 1 0 0 1 1 1
0 1 1 1 0 0 1 1 0 0 1 1 0 1 1 0 0 0 1 1 0 1 1 1 0 1 1 1 0 0 1 1 0 1 1 1 0 0 1 1
0 0 1 1 0 1 1 1 0 1 1 1 0 0 1 0 0 1 1 1 0 1 1 1 0 0 1 1 0 1 1 1 0 1 1 0 0 0 1 1
0 0 1 1 0 1 1 1 0 0 1 1 0 0 1 1 0 1 1 1 0 0 1 1 0 1 1 1 0 1 1 1 0 0 1 0 0 1 1 1
0 0 1 1 0 0 1 1 0 1 1 1 0 1 1 0 0 0 1 1 0 1 1 1 0 1 1 1 0 0 1 1 0 1 1 1 0 1 1 1
0 0 1 1 0 1 1 1 0 0 1 1 0 0 1 0 0 0 1 1 0 1 1 1 0 0 1 1 0 1 1 1 0 1 1 0 0 0 1 1
0 1 1 1 0 1 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 0 1 1 0 1 1 1 0 1 1 1 0 0 1 0 0 1 1 1
0 1 1 1 0 0 1 1 0 1 1 1 0 1 1 0 0 0 1 0 0 0 1 1 0 1 1 1 0 0 1 1 0 1 1 1 0 1 1 1
```

Remark 3.14. In the following examples we use the b-adic representation of a natural number $n \in \mathbb{N} + 1$, where $b \in \mathbb{N} + 2$. We use the notation

$$n = (a_0, a_1, \ldots, a_k)_b = a_0 + a_1 b + \ldots + a_k b^k$$

where we require $a_k \neq 0$.

Let $P : \{0, 1, \ldots, b-1\} \longrightarrow \mathbb{N}$ be a mapping. We define then $f : \mathbb{N}+1 \longrightarrow \mathbb{N}+1$ by $f(n) := \sum_{j=0}^{k} P(a_j)$. The dynamic properties of this type of functions have been studied by numerous authors, in particular by te Riele [**12**] and Stewart [**13**]. They are rather complicated, but in some cases one can find weak attractors, as we shall see in the following examples.

Example 3.15. In Remark 3.14 assume $b = 10$, $P(a) = a^2$, so that $f(n) = \sum_{j=0}^{k} a_j^2$.

Porges, in a paper cited in Stewart [**13**, p. 374] has shown that every orbit ends up in the fixed point 1 or in the cycle (4 16 37 58 89 145 42 20).

Therefore $\Omega := \{1, 37\}$ is a weak attractor.

We choose $Y := \{0, 1\}$, $\alpha(n) = n \bmod 2$ and $\lambda(y) := 1 - y$ and obtain a sequence F which begins with

```
1 0 0 1 1 0 0 0 1 0 1 0 1 1 1 0 0 0 1 0 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 1 0 0 1
1 1 1 1 0 1 0 1 1 1 1 0 0 0 0 1 1 0 1 0 0 0 1 1 1 0 1 1 1 0 0 1 1 0 1 1 0 1 0 0
0 0 0 1 0 1 1 1 1 1 1 1 0 1 1 1 0 1 1 0 1 0 1 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 1 0
1 0 0 1 1 0 1 0 0 1 0 0 0 1 1 0 0 1 0 1 1 1 1 0 0 1 1 1 0 1 0 1 1 0 0 1 0 0 1 0
1 0 0 1 1 0 0 0 0 0 0 1 0 1 0 0 0 0 1 0 1 0 1 1 0 0 0 1 0 1 1 0 0 0 1 0 1 0 1 0
0 1 0 1 0 0 1 0 1 0 1 0 0 1 1 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 0 1 0 0 1 0 1 1 0 1
```

Lemma 3.16. *Let $b \in \mathbb{N}+2$, $P : \{0, 1, \dots, b-1\} \longrightarrow \mathbb{N}$ and $f : \mathbb{N}+1 \longrightarrow \mathbb{N}+1$ be defined as in Remark 3.14.*

Then there exists $n_0 \in \mathbb{N}+1$ such that $f(n) < n$ for every $n \geq n_0$.

Proof. We follow the proof of Theorem 1 in Stewart [**13**, p. 375].

Let $M := \max(P(0), \dots, P(b-1))$. Since $\lim\limits_{r\to\infty} \dfrac{b^r}{r+1} = \infty$, there must exist $r_0 \in \mathbb{N}$ such that $\dfrac{b^r}{r+1} > M$ for every $r \geq r_0$.

Set $n := (a_0, \dots, a_k)_b \in \mathbb{N}+1$ (with $a_k \neq 0$). Then $b^k \leq n$, and

$f(n) = \sum\limits_{j=0}^{k} P(a_j) \leq (k+1)M < b^k \leq n$ for $k \geq r_0$, thus $f(n) < n$ for $k \geq r_0$, that is, for $n \geq b^{r_0}$.

Corollary 3.17. *Let f be defined as in Remark 3.14. Then:*

(1) Every orbit of f is finite.

(2) There exists only a finite number of cycles of f and every orbit ends up in exactly one of these cycles.

Proof. (1) Choose n_0 as in Lemma 3.16 and let $n \in \mathbb{N}+2$.

Each time when $f^j(n) \geq n_0$, after a finite number of steps from $f^j(n)$ one arrives at a value $< n_0$. But the set $\{1, \dots, n_0 - 1\}$ is finite, therefore there have to exist repetitions in the set $\{f^j(n) \mid j \in \mathbb{N}\}$. This implies that the orbit of n is finite.

(2) Every cycle intersects the set $\{1, \dots, n_0 - 1\}$; but the cycles of f are disjoint.

Example 3.18. Choose $b = 10$ and $P(a) = a^4$ in Remark 3.14. In Chikawa a.o. [**6**] the authors show that the cycles of f are (1), (1634), (8208), (9474), $(2178\ 6514)$ and $(13139\ 6725\ 4338\ 4514\ 1138\ 4179\ 9219)$.

Therefore we may choose $\Omega := \{1, 1634, 8208, 9474, 2178, 1138\}$.

Let Y, $\alpha : \Omega \longrightarrow Y$ and $\lambda : Y \longrightarrow Y$ be as in Example 3.15.

```
1 0 1 1 1 0 1 1 1 0 1 0 0 1 1 1 1 0 1 0 0 0 1 0 1 0 1 1 0 1 0 1 1 0 1 0 0 0 1 1
1 0 0 1 0 1 0 1 1 1 1 1 1 0 1 0 0 1 1 0 1 0 0 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 1
0 1 0 1 1 0 0 1 0 1 1 0 1 1 1 1 0 0 0 0 1 0 0 1 1 1 1 0 1 1 0 1 1 0 0 1 0 0 0 0
1 0 1 0 0 0 1 1 0 0 1 1 1 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 1 1 0 0 1 0 1 1 0 1 0 1
1 0 0 0 1 0 1 1 1 1 0 1 0 0 0 1 0 0 1 0 0 1 0 0 1 1 0 1 1 1 0 0 0 1 0 1 1 1 0 0
0 0 1 0 1 0 1 1 0 0 1 0 1 0 0 0 1 1 0 0 0 0 0 0 1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 0
0 0 1 0 0 1 1 1 0 1 0 1 0 0 1 0 0 1 0 0 0 0 1 1 0 0 1 1 1 1 1 1 1 1 0 1 1 1 0 1
1 1 0 1 1 1 1 1 0 0 0 0 0 0 0 1 0 0 1 1 0 1 1 0 1 0 0 0 1 0 1 1 1 0 1 0 0 0 0 1
```

Example 3.19. For $n = (a_0, \dots, a_k)_{10} \in \mathbb{N}+1$ let $f(n) := (a_0 + a_1 + \ldots + a_k)^2$. Mohanty/Kumar [**11**] show that every orbit of f ends up in one of the cycles (1), (81) and $(169\ 256)$. We may therefore choose the weak attractor $\Omega := \{1, 81, 169\}$.

Let Y, $\alpha : \Omega \longrightarrow Y$ and $\lambda : Y \longrightarrow Y$ be as in Example 3.15.

1 0 1 1 1 0 1 1 1 0 1 0 0 1 1 1 1 0 1 0 0 0 1 0 1 0 1 1 0 1 0 1 1 0 1 0 0 0 1 1
1 0 0 1 0 1 0 1 1 1 1 1 1 0 1 0 0 1 1 0 1 0 0 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 1
0 1 0 1 1 0 0 1 0 1 1 0 1 1 1 1 0 0 0 0 1 0 0 1 1 1 1 0 1 1 0 1 1 0 0 1 0 0 0 0
1 0 1 0 0 0 1 1 0 0 1 1 1 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 1 1 0 0 1 0 1 1 0 1 0 1
1 0 0 0 1 0 1 1 1 1 0 1 0 0 0 1 0 0 1 0 0 1 0 0 1 1 0 1 1 1 0 0 0 1 0 1 1 1 0 0
0 0 1 0 1 0 1 1 0 0 1 0 1 0 0 0 1 1 0 0 0 0 0 0 1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 0
0 0 1 0 0 1 1 1 0 1 0 1 0 0 1 0 0 1 0 0 0 0 1 1 0 0 1 1 1 1 1 1 1 1 0 1 1 1 0 1
1 1 0 1 1 1 1 1 0 0 0 0 0 0 0 1 0 0 1 1 0 1 1 0 1 0 0 0 1 0 1 1 1 0 1 0 0 0 0 1

Example 3.20. For $n = (a_0, \dots, a_k)_{10} \in \mathbb{N} + 1$ let $f(n) := \prod_{j=0}^{k} (a_j + 1)$. In Wagstaff [**14**, p. 342], it is shown that every orbit ends up in one of the cycles (18) and $(2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10)$. We choose $\Omega := \{18, 2\}$.

Let Y, $\alpha : \Omega \longrightarrow Y$ and $\lambda : Y \longrightarrow Y$ be as in Example 3.15.

1 0 0 1 0 1 0 1 0 1 0 0 0 0 1 1 0 0 0 1 0 1 1 0 1 1 1 0 1 0 0 1 0 0 1 1 0 0 0 1
0 0 0 0 1 0 0 0 1 0 1 1 1 1 0 1 1 0 0 1 1 1 1 0 1 0 0 0 1 0 0 1 0 0 1 0 1 0 0 1
1 0 0 0 0 0 0 0 1 0 0 1 0 1 0 1 0 1 0 1 0 0 0 0 1 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0
1 1 1 1 0 1 1 0 0 0 0 1 0 0 1 0 1 0 0 0 0 1 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 0 1 1
1 1 0 1 1 0 0 0 1 0 0 1 1 0 0 0 1 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 1
0 1 1 0 1 1 1 0 1 0 1 1 1 1 0 1 1 0 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 0 0 1 0 0 1 0
1 0 0 0 1 0 1 0 0 1 0 0 0 1 0 0 0 0 0 1 1 0 1 0 0 1 1 1 1 1 1 0 0 1 0 1 1 0 1 0
0 0 0 0 0 1 0 1 0 1 0 1 1 0 0 1 1 0 1 0 0 1 0 0 1 1 0 0 0 0 0 1 0 0 1 0 1 0 0 1

Lemma 3.21. *Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ be any function.*

Then $\Omega := \{n \in \mathbb{N} \mid f(n) \geq n\}$ is a weak attractor of f.

Proof. Suppose that there exists $n \in \mathbb{N}$ such that $f^k(n) \notin \Omega$ for every $k \in \mathbb{N}$. By definition of Ω this implies that

$$\begin{aligned} f(n) &< n \\ f^2(n) &< f(n) \\ f^3(n) &< f^2(n) \\ &\dots \end{aligned}$$

In this manner we obtain an infinite and strictly decreasing sequence of natural numbers

$n > f(n) > f^2(n) > f^3(n) > \dots$

and this is impossible.

Corollary 3.22. *Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ be any function and $U : \mathbb{N} \longrightarrow \mathbb{N}$ be a mapping such that $U(n) \leq n$ for every $n \in \mathbb{N}$.*

Then $\Omega' := \{n \in \mathbb{N} \mid f(n) \geq U(n)\}$ is a weak attractor of f.

Proof. $f(n) \geq n$ implies $f(n) \geq U(n)$. With Ω as in Lemma 3.21 we have $\Omega \subset \Omega'$.

Corollary 3.23. *Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ be any function and $V : \mathbb{N} \longrightarrow \mathbb{N}$ be another mapping such that $V(n) \geq n$ for every $n \in \mathbb{N}$.*

Then $\Omega'' := \{n \in \mathbb{N} \mid V(f(n)) \geq n\}$ is a weak attractor of f.

Proof. $f(n) \geq n$ implies $V(f(n)) \geq n$. With Ω as in Lemma 3.21 we have $\Omega \subset \Omega''$.

Example 3.24.

T	$\mathbb{N}$
$f(n)$	$(n^n + 1) \bmod (2n+1)$
Ω	$\{n \mid 3f(n) \geq 2n\}$
Y	$\{0, 1\}$
$\alpha(n)$	$n \bmod 2$
$\lambda(y)$	$1 - y$

```
0 1 1 1 0 0 1 1 0 0 1 1 0 1 1 1 0 1 1 1 0 0 1 1 0 1 1 1 0 0 1 1 0 0 0 1 0 1 0 1
0 0 0 1 0 1 0 1 0 1 1 1 0 0 1 1 0 0 1 1 0 1 0 1 0 0 0 1 0 0 0 1 0 0 1 1 0 1 1 1
0 0 0 1 0 1 1 1 0 0 1 1 0 0 0 1 0 1 1 1 0 1 0 1 0 0 0 1 0 1 0 1 1 0 1 1 0 1 1 1
0 0 0 1 0 0 0 1 0 1 1 1 0 1 1 1 0 1 1 1 0 0 1 0 1 1 1 1 0 1 0 1 0 0 1 1 0 1 1 0
0 1 0 1 0 0 1 1 0 1 0 0 0 0 1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 0 1 1 1 0 1 1 1
0 1 0 1 0 1 0 1 0 0 1 1 0 1 0 1 0 1 1 1 0 0 0 1 0 1 0 1 0 1 1 1 0 0 1 1 0 1 0 1
0 0 0 1 0 0 0 0 0 0 0 1 0 1 1 1 0 0 0 1 0 0 0 1 0 0 0 1 0 1 1 1 0 0 0 1 0 1 1 1
0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 0 0 0 1 1 1 0 1 0 1 0 1
```

Example 3.25.

T	$\mathbb{N} + 2$
$f(n)$	$\Big(13n(n-1)(n-2) + \frac{n(n-1)}{2} \bmod (n+1)\Big)$
Ω	$\{n \mid f(n) \geq n\}$
Y	$\{0, 1\}$
$\alpha(n)$	$n \bmod 2$
$\lambda(y)$	$1 - y$

```
0 0 1 0 1 1 0 1 1 0 0 1 0 1 1 0 0 0 0 1 0 0 1 1 0 0 0 1 0 1 1 1 1 0 0 1 0 1 1 1
0 0 0 1 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 1 1 0 0 0 0 1 0 1 0 1 1 0 0
0 0 1 1 0 1 1 1 1 1 0 0 1 1 1 1 1 1 0 0 1 0 1 1 1 0 0 0 0 0 1 0 1 0 0 1 1 1 1 0
0 1 1 0 1 1 1 0 1 1 1 0 1 0 1 0 1 1 0 0 0 0 0 1 1 0 1 0 0 1 0 1 0 0 1 1 1 1 0 0
1 1 0 0 0 0 1 1 0 0 0 0 0 1 1 1 0 0 0 1 0 0 1 0 1 1 0 1 0 1 1 1 0 0 0 1 1 1 0 0
0 0 0 1 0 1 0 1 0 0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 1 0 1 1 1 0 0 0 0 0 1 1 0 1 1 1
1 0 0 0 1 0 1 1 1 0 0 1 1 1 1 1 1 1 0 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 0 1 0
1 0 1 0 1 1 1 0 1 0 0 1 0 1 0 1 1 1 1 0 0 1 0 0 0 1 1 0 1 0 0 1 1 1 0 1 0 1 1 0
```

Proposition 3.26. *Let* $m = 2^k \geq 4$ *and* $a, b \in \mathbb{N} + 1$.

With $T := \{0, 1, \ldots, 2^k - 1\}$ *let* $f : T \longrightarrow T$ *be defined by*

$f(n) := (an + b) \bmod m$

Then the following conditions are equivalent:

(1) f *is a cyclic permutation of* T.

(2) $a \in 4\mathbb{N} + 1$ *and* b *is odd.*

Proof. This is well known, see e.g. Knuth [**9**].

Corollary 3.27. *Let* $k \in \mathbb{N}$ *and* $f_k := \bigcirc_x (5x+1) \bmod 2^k$.

Then f_k *is a cyclic permutation of* $\{0, 1, \ldots, 2^k - 1\}$.

Example 3.28. Since

$$\mathbb{N} + 1 = \bigsqcup_{k=0}^{\infty} \{2^k, 2^k + 1, \ldots, 2^k + 2^k - 1\}$$

we can construct a function $f : \mathbb{N} + 1 \longrightarrow \mathbb{N} + 1$ by defining

$$f(2^k + x) := 2^k + ((5x + 1) \bmod 2^k)$$

for $x \in \{0, 1, \ldots, 2^k - 1\}$. By Corollary 3.27 the orbits of f are exactly the intervals $\{2^k, \ldots, 2^k + 2^k - 1\}$ and on each of these intervals f operates as a cyclic permutation.

We obtain a weak attractor of f, if we choose at least one element from each of these intervals. In particular

$$\Omega := \{2^k \mid k \in \mathbb{N}\}$$

is a weak attractor.

T	$\mathbb{N} + 1$
$f(2^k + x)$	$2^k + ((5x + 1) \bmod 2^k)$
Ω	$\{2^k \mid k \in \mathbb{N}\}$
Y	$\{0, 1, 2\}$
$\alpha(n)$	$n \bmod 3$
$\lambda(y)$	$(y + 1) \bmod 3$

```
1 2 0 1 1 0 2 2 0 1 0 0 2 2 1 1 1 2 2 2 1 0 0 0 2 0 1 1 0 1 2 2 0 1 1 0 0 2 1 1
0 1 0 2 2 2 0 0 2 0 0 1 2 1 2 2 1 2 2 0 1 0 1 1 1 2 0 1 2 0 0 0 1 0 1 0 0 1 1 2
1 2 1 2 0 0 1 1 2 1 1 1 0 2 2 0 2 0 2 2 1 1 2 2 2 2 2 1 1 0 2 1 0 1 2 0 1 2 0 0
0 0 0 2 2 1 0 2 0 0 1 0 0 2 1 1 0 1 2 2 2 0 2 0 0 1 0 1 2 1 0 2 0 2 2 0 2 1 1 1
0 2 0 0 2 2 0 0 0 0 1 2 2 2 1 2 2 0 0 1 2 0 2 1 2 1 1 0 1 0 1 0 2 1 2 2 1 1 2 2
2 2 0 1 1 2 0 1 2 0 2 0 1 2 2 0 1 0 0 2 1 0 0 2 1 1 1 1 0 0 1 1 1 1 0 0 0 1 0 0
1 2 1 2 0 1 1 2 1 2 2 1 0 2 2 1 1 1 0 2 1 0 2 2 1 0 0 1 0 1 0 2 1 0 2 0 1 2 1 0
1 0 1 2 0 0 2 0 1 0 1 1 1 1 2 1 1 2 0 0 0 0 0 1 1 2 2 2 1 1 1 2 1 2 2 1 0 2 2 2
```

Remark 3.29. Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ be defined by

$$f(n) := \begin{cases} 1 & \text{for } n = 0 \\ f(n \setminus 2) & \text{for } n \text{ odd} \\ f(n/2) + f(n/2 - 1) & \text{for } n \text{ even } > 0 \end{cases}$$

In Calkin/Wilf [**4**] it is shown that the sequence of quotients $f(n)/f(n+1)$ contains every rational number > 0 exactly once .

Remark 3.30. Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ be defined as in Remark 3.29.

Then $f(n) \leq n/2$ for every $n \geq 5$.

<u>Proof.</u> Induction on $n \geq 5$.

Since $f(5) = 2$, $f(6) = 3$, $f(7) = 1$, $f(8) = 4$, $f(9) = 3$, $f(10) = 5$, $f(11) = 2$, we have $f(n) \leq n/2$ for $5 \leq n \leq 11$, hence in particular for $n = 5$.

$n - 1 \longrightarrow n$: (i) Assume first that $n \geq 6$ is even.

Then $f(n) = f(n/2) + f(n/2 - 1)$.

If $n/2 - 1 \geq 5$, by induction we have

$$f(n) \leq \frac{n}{4} + \frac{n}{4} - \frac{1}{2} = \frac{n}{2} - \frac{1}{2} \leq \frac{n}{2}$$

Otherwise $n = 10, 8, 6$.

(ii) Suppose $n \geq 7$ is odd. Then $f(n) = f((n-1)/2)$. If $\frac{n-1}{2} \geq 5$, then by induction

$$f((n-1)/2) \leq \frac{n-1}{4} \leq \frac{n}{2}$$

Otherwise $n = 11, 9, 7$.

Example 3.31. Let f be defined as in Remark 3.29. From Remark 3.30 it follows that $\Omega := \{1, 2\}$ is a weak attractor of f.

We can therefore define a coupled dynamical system by the table

T	$\mathbb{N}$
$f(n)$	1 for $n = 0$
	$f(n \setminus 2)$ for n odd
	$f(n/2) + f(n/2 - 1)$ for n even > 0
Ω	$\{0, 1\}$
Y	$\{0, 1\}$
$\alpha(n)$	$n \bmod 2$
$\lambda(y)$	$1 - y$

```
0 1 0 0 1 1 1 0 0 1 0 1 0 1 0 0 0 0 1 1 1 0 1 1 1 0 1 1 1 0 0 0 0 0 0 0 0 1 1 1
0 1 0 0 1 1 0 1 0 1 1 0 0 1 0 1 1 1 0 0 0 0 0 0 1 0 0 0 1 0 0 0 1 0 0 1 1 1 0 1
1 0 0 1 1 0 0 0 1 1 0 1 1 0 0 1 0 0 1 1 0 1 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 0 1 0
0 0 1 0 0 0 1 0 1 1 0 0 1 0 1 0 0 1 0 0 0 0 1 0 0 1 0 0 1 0 1 1 0 1 0 1 0 0 1 1
1 1 1 0 1 0 0 1 1 1 1 0 1 0 0 0 0 1 1 1 1 0 0 1 0 1 1 0 0 0 0 1 0 0 0 0 1 1 0 1
0 0 1 1 1 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1 1 1 1 1 0 0 1 0 1 0 1 1 0 1 0 0 1 0 0
1 0 0 0 0 1 0 0 1 0 1 0 0 1 1 0 0 1 1 1 0 0 0 0 0 1 0 0 0 1 1 0 0 0 1 1 0 0 1 0
1 0 1 0 1 1 1 0 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1 1 1 0 0 1 0 0 0 1 1 0 1 0 1 1 0 1
```

4. Möbius transformations on finite fields

Lemma 4.1. *Let $K = GF(q)$ be a finite field of characteristic $\neq 2$ and $\alpha \in K \setminus 0$. Then the equation $x^2 = \alpha$ has two distinct roots in $L := GF(q^2)$.*

Proof. We can choose an algebraic field extension of K in which the equation has a root β: $\beta^2 = \alpha$.

We must show that $\beta \in L$, i.e., that $\beta^{q^2-1} = 1$, being necessarily $\beta \neq 0$.
Since $q^2 - 1$ is even, we have

$$\beta^{q^2-1} = (\beta^2)^{\frac{q^2-1}{2}} = \alpha^{\frac{q^2-1}{2}} = \alpha^{(q+1)(q-1)/2} = \alpha^{2(q-1)/2} = \alpha^{q-1} = 1$$

The second root is then $-\beta$. Finally $\beta \neq -\beta$, since $\operatorname{char} K \neq 2$.

Corollary 4.2. *Let $K = GF(q)$ be a finite field of characteristic $\neq 2$ and $b, c \in K$. Then the equation $x^2+bx+c = 0$ has the solutions $x = \dfrac{-b \pm \sqrt{b^2-4c}}{2}$, where by Lemma 4.1 we can calculate the square roots $\pm\sqrt{b^2-4c}$ in $GF(q^2)$.*

Proposition 4.3. *Let $K = GF(q)$ be a finite field of characteristic $\neq 2$ and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, K)$.*

Let $\alpha, \beta \in GF(q^2)$ be the roots of the characteristic polynomial $x^2 - (a+d)x + ad - bc$ of A. Suppose that the multiplicative order of α/β in $GF(q^2)$ is $q+1$ (this implies that the characteristic polynomial is irreducible).

Define $f : K \longrightarrow K$ by

$$f(t) := \begin{cases} \dfrac{at+b}{ct+d} & \textit{if } ct+d \neq 0 \\ a/c & \textit{otherwise} \end{cases}$$

Then f is a cyclic permutation of K.

Proof. Çeşmelioğlu/W. Meidl/A. Topuzoğlu [**5**, p. 597].

Remark 4.4. We use Pari/GP for verifying the hypotheses of Proposition 4.3 for the matrix $A := \begin{pmatrix} 3 & 2 \\ 5 & 1 \end{pmatrix}$ and $K := GF(1907)$.

The characteristic polynomial $x^2 - 4x - 7$ has the roots $\alpha := 2 + \sqrt{11}$ and $\beta := 2 - \sqrt{11}$ which must be calculated in $L := GF(1907^2)$.

First we find a generator e of the field L:

```
q=1907; q2=q^2; e=ffgen(q2,'e)
```

then we find α and β with

```
r=sqrt(11+0*e); alfa=2+r; beta=2-r;
```

Now we can verify that the multiplicative order of α/β is equal to $1907 + 1 = 1908$ using

```
t_out(fforder(alfa/beta)) \\ 1908
```

Example 4.5. We can thus apply Proposition 4.3 in order to obtain a coupled dynamical system:

T	$GF(1907)$
$f(t)$	$\dfrac{3t+2}{5t+1}$ if $5t+1 \neq 0$ $3/5$ otherwise
Ω	$\{1, 100, 900\}$
Y	$\{0, 1\}$
$\alpha(t)$	0
$\lambda(y)$	$1 - y$

```
1 0 0 0 1 1 1 1 1 1 1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 1 0 0 1 0 0 1 0 1 1 0 0 0 1 0
0 0 1 1 1 1 0 1 1 0 1 0 0 1 1 0 0 1 1 0 1 1 0 1 0 1 1 0 0 0 1 1 0 0 0 0 1 0 0 1
1 0 0 0 0 0 1 1 0 1 0 0 0 0 0 1 1 0 1 1 0 0 0 1 0 0 0 1 0 0 0 1 1 0 0 0 0 0 1 0
1 1 1 0 0 0 1 1 1 0 0 1 0 0 1 0 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1 0 0 1 1 1 1 0 0 1
0 0 0 1 1 1 0 0 0 1 0 1 0 0 1 1 1 1 0 0 1 0 1 1 0 1 1 0 0 1 0 0 1 0 1 1 1 1 1 1
0 1 0 1 0 1 0 0 1 0 1 1 0 1 0 1 1 0 1 0 0 1 1 1 1 1 1 0 0 0 1 0 1 0 1 0 1 1 1 1
0 0 0 0 0 0 0 1 1 1 1 0 0 0 1 0 1 0 1 1 1 1 1 0 1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0
0 1 1 0 1 0 1 1 1 0 0 1 1 1 1 1 1 1 0 0 0 1 0 1 1 1 1 0 0 1 1 0 1 0 1 1 1 0 1 0
```

Here, after defining the fields K and L as in Remark 4.4, we obtained the first terms of the sequence F with

```
f (t) = {my (u);
t=t+0*e; u=5*t+1; if (u, (3*t+2)/u, 3/5)}

inomega (t) = t_pos(t,[1,100,900])

alfa (t) = 0

lam (y) = 1-y

F (t) = if (inomega(t), alfa(t), lam(F(f(t))))

t_fvo(F,[0..799],40)
```

using, as in the other examples, the functions `t_pos` and `t_fvo` from *paritools* available on felix.unife.it/++/paritools.

Concluding remark. The first author's thesis [**2**] contains more examples, graphical representations, Fourier transforms and tests.

References

[1] **J. Allouche/J. Shallit:** Automatic sequences. Cambridge UP 2003.

[2] **L. Baldini:** Analisi armonica e successioni automatiche generalizzate. Tesi LM Univ. Ferrara 2015.

[3] **J. Berstel/J. Karhumäki:** Combinatorics on words - a tutorial. Bull. EATCS 79 (2003), 178-228.

[4] **N. Calkin/H. Wilf:** Recounting the rationals. Am. Math. Monthly 107/4 (2000), 360-363.

[5] **A. Çeşmelioğlu/W. Meidl/A. Topuzoğlu:** On the cycle structure of permutation polynomials. Finite Fields Appl. 14 (2008), 593-614.

[6] **K. Chikawa/K. Iseki/T. Kusakabe:** On a problem by H. Steinhaus. Acta Arithmetica 7 (1962), 251-252.

[7] **J. Eschgfäller:** Almost topological spaces. Ann. Univ. Ferrara 30 (1984), 163-183.

[8] **R. Guy:** Unsolved problems in number theory. Springer 2004.

[9] **D. Knuth:** The art of computer programming. Volume 2. Addison-Wesley.

[10] **J. Lagarias:** The ultimate challenge - the 3x+1 problem. AMS 2010.

[11] **S. Mohanty/H. Kumar:** Powers of sums of digits. Math. Magazine 52/5 (1979), 310-312.

[12] **H. te Riele:** Iteration of number theoretic functions. Nieuw Arch. Wiskunde 1 (1983), 345-360.

[13] **B. Stewart:** Sums of functions of digits. Can. J. Math. 12 (1960), 374-389.

[14] **S. Wagstaff:** Iterating the product of shifted digits. Fibonacci Quart. 19 (1981), 340-347.