Algebraic structure and numeration systems for circular words

Isabelle Dubois

Laboratoire IECL - Metz - Université de Lorraine

Numeration - June 2017

Joint work with Benoît Rittaud, still in progress

Starting point:

Consider the addition of two rationals, but focus only on the periods.

Let $A = 178/55 = 3,2\overline{36}...$ and $B = 421/330 = 1,2\overline{75}\ldots$.
Then $A + B = 4,5\overline{12}\ldots$.
Or, if we make only the addition for the periods we have:

$$\begin{aligned}\overline{3\ 6} + \overline{7\ \ 5} = \overline{10\ 11} \quad &\approx \quad \overline{(10+1)\ (11-10)} = \overline{(11)\ 1} \\ &\approx \quad \overline{(11-10)\ (1+1)} = \overline{1\ 2}\end{aligned}$$

Starting point:

Consider the addition of two rationals, but focus only on the periods.

Let $A = 178/55 = 3,2\overline{36}...$ and $B = 421/330 = 1,2\overline{75}\ldots$.
Then $A + B = 4,5\overline{12}\ldots$.
Or, if we make only the addition for the periods we have:

$$\begin{aligned}\overline{3\ 6} + \overline{7\ \ 5} = \overline{10\ 11} \quad &\approx \quad \overline{(10+1)\ (11-10)} = \overline{(11)\ 1} \\ &\approx \quad \overline{(11-10)\ (1+1)} = \overline{1\ 2}\end{aligned}$$

We can interpret this operation in term of an addition of two circular words of length 2, with respect to the base 10 numeration:

$$(3\ 6) + (7\ 5) \approx_{\text{base } 10} (1\ 2).$$

Starting point:

Consider the addition of two rationals, but focus only on the periods.

Let $A = 178/55 = 3,2\overline{36}...$ and $B = 421/330 = 1,2\overline{75}\ldots$.
Then $A + B = 4,5\overline{12}\ldots$.
Or, if we make only the addition for the periods we have:

$$\begin{aligned}\overline{3\ 6} + \overline{7\ \ 5} = \overline{10\ 11} \quad &\approx \quad \overline{(10+1)\ (11-10)} = \overline{(11)\ 1} \\ &\approx \quad \overline{(11-10)\ (1+1)} = \overline{1\ 2}\end{aligned}$$

We can interpret this operation in term of an addition of two circular words of length 2, with respect to the base 10 numeration:

$$(3\ 6) + (7\ 5) \approx_{\text{base } 10} (1\ 2).$$

The notion of circular word was first introduced by B. Rittaud and L. Vivier (2011-2012), in the context of the Fibonacci numeration.

I have discovered this notion when Benoît gave a talk on this topic in Nancy, which led to a collaboration.

Presentation Outline

Let $\ell \in \mathbb{N}^*$ be fixed.

Definition (Circular word of length ℓ)

A circular word of length ℓ is a finite word $(w_0 \ldots w_i \ldots w_{\ell-1})$ made of ℓ letters on the alphabet $\mathbb{Z}$ and indexed by $\mathbb{Z}/\ell\mathbb{Z}$.

The set of circular words of length ℓ is an abelian group:

$$W + W' = ((w_0 + w'_0) \ldots (w_i + w'_i) \ldots (w_{\ell-1} + w'_{\ell-1}))$$

Let P be an integral polynomial $P(X) = \sum_{0 \leq i \leq d} a_i X^i \in \mathbb{Z}[X]$ ($d \in \mathbb{N}^*$).

Definition (Carry equivalence defined by P)

The carry equivalence $\approx_P$ defined by P on circular words $W = (w_0 \ldots w_{\ell-1})$ is based on the relations: for all i modulo ℓ,

$$W \approx_P (w_0 \ldots (w_{i-d} + a_0) \ldots (w_{i-1} + a_{d-1})(w_i + a_d) w_{i+1} \ldots w_{\ell-1}).$$

Let $\ell \in \mathbb{N}^*$ be fixed.

Definition (Circular word of length ℓ)

A circular word of length ℓ is a finite word $(w_0 \dots w_i \dots w_{\ell-1})$ made of ℓ letters on the alphabet $\mathbb{Z}$ and indexed by $\mathbb{Z}/\ell\mathbb{Z}$.

The set of circular words of length ℓ is an abelian group:

$$W + W' = ((w_0 + w'_0) \dots (w_i + w'_i) \dots (w_{\ell-1} + w'_{\ell-1}))$$

Let P be an integral polynomial $P(X) = \sum_{0 \le i \le d} a_i X^i \in \mathbb{Z}[X]$ $(d \in \mathbb{N}^*)$.

Definition (Carry equivalence defined by P)

The carry equivalence $\approx_P$ defined by P on circular words $W = (w_0 \dots w_{\ell-1})$ is based on the relations: for all i modulo ℓ,

$$W \approx_P (w_0 \dots (w_{i-d} + a_0) \dots (w_{i-1} + a_{d-1})(w_i + a_d) w_{i+1} \dots w_{\ell-1}).$$

Example. "Fibonacci" $P(X) = X^2 - X - 1$, $\ell = 4$.

$$(1\,2\,3\,4) \approx_P (0\,1\,4\,4) \approx_P (4\,1\,0\,0) \approx_P (3\,0\,1\,0) \approx_P (2\,1\,1\,(-1))$$
$$\approx_P (2\,0\,0\,0) \approx_P (1\,0\,1\,1) \approx_P (0\,1\,1\,0) \approx_P (0\,0\,0\,1)$$

Given: $\ell \in \mathbb{N}^*$, $P(X) = \sum_{0 \le i \le d} a_i X^i \in \mathbb{Z}[X]$.

Let σ be the shift transformation defined by

$$\sigma((w_0 \dots w_{\ell-1})) = (w_1 \dots w_{\ell-1} w_0).$$

Let $A_\ell := (a_0 \dots a_i \dots a_d 0 \dots 0)$, if $\ell > d$, resp. $:= ((\sum_{j \equiv i \bmod \ell} a_j)_i)$ if $\ell \le d$, be the circular word associated to P.

Definition (Group of circular words with carry equivalence)

The carry equivalence $\approx_P$ defined by P on circular words of length ℓ is :
$W \approx_P W'$ if and only if there exists $(v_0, \dots, v_{\ell-1}) \in \mathbb{Z}^\ell$ such that

$$W = W' + \sum_{0 \le i \le \ell-1} v_i \sigma^{-i}(A_\ell).$$

Let $\mathcal{G}_{\ell,P}$ be the abelian quotient group of circular words of length ℓ by this carry equivalence.

Given: $\ell \in \mathbb{N}^*$, $P(X) = \sum_{0 \le i \le d} a_i X^i \in \mathbb{Z}[X]$.

Let σ be the shift transformation defined by

$$\sigma((w_0 \dots w_{\ell-1})) = (w_1 \dots w_{\ell-1} w_0).$$

Let $A_\ell := (a_0 \dots a_i \dots a_d 0 \dots 0)$, if $\ell > d$, resp. $:= ((\sum_{j \equiv i \bmod \ell} a_j)_i)$ if $\ell \le d$, be the circular word associated to P.

Definition (Group of circular words with carry equivalence)

The carry equivalence $\approx_P$ defined by P on circular words of length ℓ is :
$W \approx_P W'$ if and only if there exists $(v_0, \dots, v_{\ell-1}) \in \mathbb{Z}^\ell$ such that

$$W = W' + \sum_{0 \le i \le \ell-1} v_i \sigma^{-i}(A_\ell).$$

Let $\mathcal{G}_{\ell,P}$ be the abelian quotient group of circular words of length ℓ by this carry equivalence.

Examples.

- "Base 2": $P(X) = X - 2$, $\ell = 2$, $\mathcal{G}_{2,P} = \{(0\,0), (1\,0), (0\,1)\}$
- "Fibonacci": $P(X) = X^2 - X - 1$, $\ell = 4$,
  $\mathcal{G}_{4,P} = \{(0\,0\,0\,0), (1\,0\,0\,0), (0\,1\,0\,0), (0\,0\,1\,0), (0\,0\,0\,1)\}$.

The group of circular words of length ℓ with a carry P can be studied via algebraic isomorphisms between $\mathcal{G}_{\ell,P}$ and the:

1. Set of equivalent points on the action of the $\ell \times \ell$ circulant matrix whose first row is A_ℓ (or associated to P) on the lattice group $\mathbb{Z}^\ell$.
2. Abelian group (for $+$) of the quotient ring of integral polynomials $\mathbb{Z}[X]/(P(X), X^\ell - 1)$. The multiplication by X correspond to the inverse of the shift transformation.

The group of circular words of length ℓ with a carry P can be studied via algebraic isomorphisms between $\mathcal{G}_{\ell,P}$ and the:

1. Set of equivalent points on the action of the $\ell \times \ell$ circulant matrix whose first row is A_ℓ (or associated to P) on the lattice group $\mathbb{Z}^\ell$.
2. Abelian group (for $+$) of the quotient ring of integral polynomials $\mathbb{Z}[X]/(P(X), X^\ell - 1)$. The multiplication by X correspond to the inverse of the shift transformation.

Proposition (Finite group)

$\mathcal{G}_{\ell,P}$ is a finite abelian group if and only if P has no ℓ-th roots of unity

From now on:
Assumption: P has no roots of unity.

The group of circular words of length ℓ with a carry P can be studied via algebraic isomorphisms between $\mathcal{G}_{\ell,P}$ and the:

1. Set of equivalent points on the action of the $\ell \times \ell$ circulant matrix whose first row is A_ℓ (or associated to P) on the lattice group $\mathbb{Z}^\ell$.
2. Abelian group (for $+$) of the quotient ring of integral polynomials $\mathbb{Z}[X]/(P(X), X^\ell - 1)$. The multiplication by X correspond to the inverse of the shift transformation.

Proposition (Finite group)

$\mathcal{G}_{\ell,P}$ is a finite abelian group if and only if P has no ℓ-th roots of unity

From now on:

Assumption: P has no roots of unity.

Links with other topics:

- dynamical systems : periodic points for toral endomorphisms
- cyclic resultants, for producing large primes
- ...

Let $g_{\ell,P}$ be the order of the group $\mathcal{G}_{\ell,P}$. We have:

Proposition (Properties of the order of the group)

(i) $g_{\ell,P} = |\mathrm{Resultant}(P(X), X^\ell - 1)| = |\prod_{0\leq k<\ell} P(e^{2i\pi k/\ell})|$.

(ii) $(g_{\ell,P})_\ell$ *is a divisibility sequence.*

(iii) $\text{Exponential growth}: \lim_{\ell\to+\infty} \ln g_{\ell,P}/\ell = \ln M(P)$, *where $M(P)$ is the Mahler measure of P.*

(iv) $\text{Apparition of primitive prime factors}:$ *If P is monic and irreducible, there are infinite primitive prime factors in the sequence $(g_{\ell,P})_\ell$ (and more finer results).*

Let $g_{\ell,P}$ be the order of the group $\mathcal{G}_{\ell,P}$. We have:

Proposition (Properties of the order of the group)

(i) $g_{\ell,P} = |\mathrm{Resultant}(P(X), X^\ell - 1)| = |\prod_{0\leq k<\ell} P(e^{2i\pi k/\ell})|$.

(ii) $(g_{\ell,P})_\ell$ *is a divisibility sequence.*

(iii) Exponential growth : $\lim_{\ell\to+\infty} \ln g_{\ell,P}/\ell = \ln M(P)$, *where $M(P)$ is the Mahler measure of P.*

(iv) Apparition of primitive prime factors : *If P is monic and irreducible, there are infinite primitive prime factors in the sequence $(g_{\ell,P})_\ell$ (and more finer results).*

Example. Fibonacci case, $(g_{\ell,X^2-X-1})_\ell$=sequence A001350 "Associated Mersenne numbers". First primitive prime factors: 2, 5, 11, 13, 29, 3, 19, 199, 521, 31, 7, 3571....

Open questions.

Find more generalized/deeper results on primitive prime factors.

Case of P not monic ?

From now, we omit the dependance on P.

Let $B^{(\ell)}(X) = \sum_{0 \leq i < \ell} b_i^{(\ell)} X^i$ be the integral polynomial such that

$$g_\ell = P(X)B^{(\ell)}(X) + (X^\ell - 1) \sum_{0 \leq i \leq d-1} v_i^{(\ell)} X^i.$$

Proposition (Structure of the group)

(i) *The word $G_\ell := (10^{\ell-1})$ is an element of maximal order.*

(ii) *The exponent of the group $\mathcal{G}_\ell$ is equal to $g_\ell / \gcd((b_i^{(\ell)}), (v_j^{(\ell)}))$.*

(iii) *The group $\mathcal{G}_\ell$ is cyclic generated by G_ℓ if and only if $\gcd(b_i^{(\ell)}, g_\ell) = 1$ for some (or any) i. In this case, the sequence $(b_i^{(\ell)} \pmod{g_\ell})_i$ is geometric, and the inverse of its common ratio, is a root of the polynomial P and a ℓ-th root of unity in $\mathbb{Z}/g_\ell\mathbb{Z}$.*

From now, we omit the dependance on P.

Let $B^{(\ell)}(X) = \sum_{0 \le i < \ell} b_i^{(\ell)} X^i$ be the integral polynomial such that

$$g_\ell = P(X)B^{(\ell)}(X) + (X^\ell - 1) \sum_{0 \le i \le d-1} v_i^{(\ell)} X^i.$$

Proposition (Structure of the group)

(i) *The word $G_\ell := (10^{\ell-1})$ is an element of maximal order.*

(ii) *The exponent of the group $\mathcal{G}_\ell$ is equal to $g_\ell / \gcd((b_i^{(\ell)}), (v_j^{(\ell)}))$.*

(iii) *The group $\mathcal{G}_\ell$ is cyclic generated by G_ℓ if and only if $\gcd(b_i^{(\ell)}, g_\ell) = 1$ for some (or any) i. In this case, the sequence $(b_i^{(\ell)} \pmod{g_\ell})_i$ is geometric, and the inverse of its common ratio, is a root of the polynomial P and a ℓ-th root of unity in $\mathbb{Z}/g_\ell\mathbb{Z}$.*

Examples.

- "Base b": ($b \ge 2$): $P(X) = X - b$, $g_\ell = b^\ell - 1$, $b_i^{(\ell)} = b^{\ell-1-i}$, $\mathcal{G}_\ell = \langle (10^{\ell-1}) \rangle \simeq \mathbb{Z}/(b^\ell - 1)\mathbb{Z}$.
- "Rational base": $P(X) = pX - q$ ($q > p$ coprime), $g_\ell = q^\ell - p^\ell$, $b_i^{(\ell)} = p^i q^{\ell-1-i}$, $\mathcal{G}_\ell = \langle (10^{\ell-1}) \rangle \simeq \mathbb{Z}/(q^\ell - p^\ell)\mathbb{Z}$.

In order to describe more precisely the structure of any group $\mathcal{G}_\ell$, we have to use more algebraic tools.
A simple tool is to use Bezout's relations between P and $X^\ell - 1$ (as for the previous proposition). But it is difficult to obtain general results for certain classes of polynomials.

Example. "Quadratic case, generalizing Fibonacci"
Let $P(X) = X^2 - kX - 1$, with $k \in \mathbb{N}^*$. Then we have:

- If ℓ is odd, then $\mathcal{G}_\ell \simeq \mathbb{Z}/g_\ell\mathbb{Z}$, except for $\ell \in 3\mathbb{N}$ and k odd, where $\mathcal{G}_\ell \simeq \mathbb{Z}/g_\ell/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- If $\ell \equiv 2 \bmod 4$, then $\mathcal{G}_\ell \simeq \mathbb{Z}/\sqrt{g_\ell}\mathbb{Z} \times \mathbb{Z}/\sqrt{g_\ell}\mathbb{Z}$.
- If $\ell \equiv 0 \bmod 4$, then $\mathcal{G}_\ell \simeq \mathbb{Z}/\sqrt{\Delta g_\ell}\mathbb{Z} \times \mathbb{Z}/\sqrt{g_\ell/\Delta}\mathbb{Z}$ (case k odd), or $\mathcal{G}_\ell \simeq \mathbb{Z}/\sqrt{\Delta g_\ell/4}\mathbb{Z} \times \mathbb{Z}/\sqrt{4g_\ell/\Delta}\mathbb{Z}$ (case k even).
  (Δ is the discriminant of P)

(small improvement of previous results of Benoît Rittaud)

Remark. We can give "explicit" generators corresponding to these decompositions.

Other Example. "Quadratic case, generalizing more Fibonacci".
Let $P(X) = X^2 - qX + p$, with $p, q \in \mathbb{Z}^*$ (+ conditions). Let $\ell \geq 1$.
Then:

- $\pm g_\ell = p^\ell - L_\ell + 1$
- for $0 \leq i < \ell$, $b_i^{(\ell)} = p^{\ell-1-i}(F_i - F_{i-\ell})$
- $\mathcal{G}_\ell \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, with $n|m$ (m is the exponent of the group). It can be cyclic if $n = 1$.

where
$(L_n)_{n\in\mathbb{Z}}$ is a Lucas-type sequence : $L_0 = 2$, $L_1 = q$, $L_{n+2} = qL_{n+1} - pL_n$,
$(F_n)_{n\in\mathbb{Z}}$ is a Fibonacci-type sequence : $F_0 = 1$, $F_1 = q$,
$F_{n+2} = qF_{n+1} - pF_n$.

Other Example. "Quadratic case, generalizing more Fibonacci".
Let $P(X) = X^2 - qX + p$, with $p, q \in \mathbb{Z}^*$ (+ conditions). Let $\ell \geq 1$.
Then:

- $\pm g_\ell = p^\ell - L_\ell + 1$
- for $0 \leq i < \ell$, $b_i^{(\ell)} = p^{\ell-1-i}(F_i - F_{i-\ell})$
- $\mathcal{G}_\ell \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, with $n|m$ (m is the exponent of the group). It can be cyclic if $n = 1$.

where
$(L_n)_{n\in\mathbb{Z}}$ is a Lucas-type sequence : $L_0 = 2$, $L_1 = q$, $L_{n+2} = qL_{n+1} - pL_n$,
$(F_n)_{n\in\mathbb{Z}}$ is a Fibonacci-type sequence : $F_0 = 1$, $F_1 = q$,
$F_{n+2} = qF_{n+1} - pF_n$.

Open questions

- Studying more precisely this case.
- Studying cases where P is not monic.
- Find more suitable algebraic/computationable tools.

Recall that $(g_\ell)_\ell$ is divisibility sequence: $g_\ell | g_{\ell\ell'}$.

Theorem (Subgroups)

Let ℓ and ℓ' be integers ≥ 1.

The map $\begin{array}{ccc} \mathcal{G}_\ell & \longrightarrow & \mathcal{G}_{\ell\ell'} \\ W & \longmapsto & W^{\ell'} = (W \dots W) \ \ (\ell' \ times) \end{array}$

is an injective morphism of $\mathcal{G}_\ell$ into $\mathcal{G}_{\ell\ell'}$. So is $\mathcal{G}_{\ell'}$ into $\mathcal{G}_{\ell\ell'}$ by $W \mapsto W^\ell$. Considering $\mathcal{G}_\ell$ and $\mathcal{G}_{\ell'}$ as subgroups of $\mathcal{G}_{\ell\ell'}$, their intersection is equal to $\mathcal{G}_{gcd(\ell,\ell')}$:

$$\mathcal{G}_{gcd(\ell,\ell')} = \mathcal{G}_\ell \cap \mathcal{G}_{\ell'} \subset \mathcal{G}_\ell(\mathcal{G}_{\ell'}) \subset \mathcal{G}_{\ell\ell'}.$$

Recall that $(g_\ell)_\ell$ is divisibility sequence: $g_\ell | g_{\ell\ell'}$.

Theorem (Subgroups)

Let ℓ and ℓ' be integers ≥ 1.

The map $\begin{array}{ccc} \mathcal{G}_\ell & \longrightarrow & \mathcal{G}_{\ell\ell'} \\ W & \longmapsto & W^{\ell'} = (W \ldots W) \ \ (\ell' \text{ times}) \end{array}$

is an injective morphism of $\mathcal{G}_\ell$ into $\mathcal{G}_{\ell\ell'}$. So is $\mathcal{G}_{\ell'}$ into $\mathcal{G}_{\ell\ell'}$ by $W \mapsto W^\ell$. Considering $\mathcal{G}_\ell$ and $\mathcal{G}_{\ell'}$ as subgroups of $\mathcal{G}_{\ell\ell'}$, their intersection is equal to $\mathcal{G}_{gcd(\ell,\ell')}$:

$$\mathcal{G}_{gcd(\ell,\ell')} = \mathcal{G}_\ell \cap \mathcal{G}_{\ell'} \subset \mathcal{G}_\ell(\mathcal{G}_{\ell'}) \subset \mathcal{G}_{\ell\ell'}.$$

We use the same type of algebraic tools as previous, and in particular the morphism of abelian groups:

$$N_\ell \ : \ \begin{array}{ccc} \mathcal{G}_\ell & \longrightarrow & \mathbb{Z}/g_\ell\mathbb{Z} \\ (w_0 \ldots w_{\ell-1}) & \longmapsto & \sum_{0 \leq i < \ell} w_i b_{\ell-i}^{(\ell)} \pmod{g_\ell}. \end{array}$$

It can be considered as a numeration system on the abelian finite group $\mathcal{G}_\ell$. When $\mathcal{G}_\ell$ is cyclic, it is an isomorphism.

Definition (Whole group of circular words)

We can define $\mathcal{G} = \varinjlim \mathcal{G}_\ell$ the inductive limit of the groups $\mathcal{G}_\ell$ with respect to the morphisms $\begin{array}{l} \mathcal{G}_\ell \longrightarrow \mathcal{G}_m \\ W \longmapsto W^{m/\ell} \end{array}$, whenever ℓ divides m.

Addition of two circular words of different lengths.

Example:

Let $W = (w_0 w_1 w_2)$ and $W' = (w'_0 w'_1)$, then
$W + W' = (w_0 w_1 w_2 w_0 w_1 w_2) + (w'_0 w'_1 w'_0 w'_1 w'_0 w'_1)$.

More generally:

If W (resp. W') is a circular word of length ℓ (resp. ℓ'), then
$W + W' = W^{n/\ell} + W'^{n/\ell'} \in \mathcal{G}_n$, with $n = \operatorname{lcm}(\ell, \ell')$.

The morphisms N_ℓ behaves well and we have:

Proposition (Numeration system on $\mathcal{G}$)

The morphism $N : \mathcal{G} \to [0,1[$, such that for all $W \in \mathcal{G}_\ell$,

$$N(W) = \{\frac{1}{g_\ell} N_\ell(W)\} = \{\frac{1}{g_\ell} \sum_{0 \leq i < \ell} w_i b^{(\ell)}_{\ell-i}\},$$

where $\{x\}$ is the fractional part of x, is well defined.

This gives us a representation of some rationals in $[0,1[$ by a circular word, compatible with the addition and the carry equivalence defined by P.

Examples.

- "Base b": $(b \geq 2)$: $P(X) = X - b$, $g_\ell = b^\ell - 1$, $b_i^{(\ell)} = b^{\ell-1-i}$, $\mathcal{G}_\ell \simeq \mathbb{Z}/(b^\ell - 1)\mathbb{Z}$. Then we have:
$$N((w_0 \dots w_{\ell-1})) = \{\frac{1}{b^\ell - 1} \sum_{0 \leq i < \ell} w_i b^{i-1}\} \in [0,1[$$

Examples.

- "Base b": $(b \geq 2)$: $P(X) = X - b$, $g_\ell = b^\ell - 1$, $b_i^{(\ell)} = b^{\ell-1-i}$, $\mathcal{G}_\ell \simeq \mathbb{Z}/(b^\ell - 1)\mathbb{Z}$. Then we have:

$$N((w_0 \ldots w_{\ell-1})) = \{\frac{1}{b^\ell - 1} \sum_{0 \leq i < \ell} w_i b^{i-1}\} \in [0,1[$$

It is similar to the expression we find when we consider the usual periodic expansion in base b:

$$0.\overline{w_0 \cdots w_{\ell-1}} = \sum_{0 \leq i < \ell} w_i \sum_{k \geq 0} \frac{1}{b^{k\ell+i+1}} = \frac{1}{b^\ell - 1} \sum_{0 \leq i < \ell} w_i b^{\ell-i-1}.$$

We can then obtain all the rational numbers with denominators of the form $b^\ell - 1$.

Examples.

- "Base b": $(b \geq 2)$: $P(X) = X - b$, $g_\ell = b^\ell - 1$, $b_i^{(\ell)} = b^{\ell-1-i}$, $\mathcal{G}_\ell \simeq \mathbb{Z}/(b^\ell - 1)\mathbb{Z}$. Then we have:

$$N((w_0 \dots w_{\ell-1})) = \{\frac{1}{b^\ell - 1} \sum_{0 \leq i < \ell} w_i b^{i-1}\} \in [0,1[$$

It is similar to the expression we find when we consider the usual periodic expansion in base b:

$$0.\overline{w_0 \cdots w_{\ell-1}} = \sum_{0 \leq i < \ell} w_i \sum_{k \geq 0} \frac{1}{b^{k\ell+i+1}} = \frac{1}{b^\ell - 1} \sum_{0 \leq i < \ell} w_i b^{\ell-i-1}.$$

We can then obtain all the rational numbers with denominators of the form $b^\ell - 1$.

For example, in base 10, we have an isomorphism of abelian groups:

$$\begin{array}{ccll} \mathcal{G} & \longrightarrow & E = & \{n \in [0,1[, n = a/99 \cdots 9,\ a \in \mathbb{N}\} \\ W & \longmapsto & N(W) & \end{array}$$

E is the set of the rationals which are not decimal in $[0,1[$ (except 0).

Examples.

- "Rational base": $P(X) = pX - q$ ($q > p$ coprime), $g_\ell = q^\ell - p^\ell$, $b_i^{(\ell)} = p^i q^{\ell-1-i}$, $\mathcal{G}_\ell \simeq \mathbb{Z}/(q^\ell - p^\ell)\mathbb{Z}$. Then we have:
$$N((w_0 \dots w_{\ell-1})) = \{\frac{1}{q^\ell - p^\ell} \cdot \frac{1}{q} \sum_{0 \le i < \ell} w_i p^{\ell-i} q^i\} \in [0, 1[$$

Examples.

- "Rational base": $P(X) = pX - q$ ($q > p$ coprime), $g_\ell = q^\ell - p^\ell$, $b_i^{(\ell)} = p^i q^{\ell-1-i}$, $\mathcal{G}_\ell \simeq \mathbb{Z}/(q^\ell - p^\ell)\mathbb{Z}$. Then we have:

$$N((w_0 \dots w_{\ell-1})) = \{\frac{1}{q^\ell - p^\ell} \cdot \frac{1}{q} \sum_{0 \le i < \ell} w_i p^{\ell-i} q^i\} \in [0,1[$$

It is similar to the expression we find when we consider periodic expansion in "base p/q":

$$0.\overline{w_0 \cdots w_{\ell-1}} = \sum_{0 \le i < \ell} w_i \sum_{k \ge 0} \frac{p^{k\ell+i}}{q^{k\ell+i+1}} = \frac{1}{q^\ell - p^\ell} \cdot \frac{1}{q} \sum_{0 \le i < \ell} w_i p^i q^{\ell-i}.$$

So, we can represent all the rational numbers of $[0,1[$, whose denominators (irreducible form) are coprime with p and q, by a circular word of finite length.

Examples.

- "Rational base": $P(X) = pX - q$ ($q > p$ coprime), $g_\ell = q^\ell - p^\ell$, $b_i^{(\ell)} = p^i q^{\ell-1-i}$, $\mathcal{G}_\ell \simeq \mathbb{Z}/(q^\ell - p^\ell)\mathbb{Z}$. Then we have:
$$N((w_0 \dots w_{\ell-1})) = \{\frac{1}{q^\ell - p^\ell} \cdot \frac{1}{q} \sum_{0 \le i < \ell} w_i p^{\ell-i} q^i\} \in [0,1[$$
It is similar to the expression we find when we consider periodic expansion in "base p/q":
$$0.\overline{w_0 \cdots w_{\ell-1}} = \sum_{0 \le i < \ell} w_i \sum_{k \ge 0} \frac{p^{k\ell+i}}{q^{k\ell+i+1}} = \frac{1}{q^\ell - p^\ell} \cdot \frac{1}{q} \sum_{0 \le i < \ell} w_i p^i q^{\ell-i}.$$
So, we can represent all the rational numbers of $[0,1[$, whose denominators (irreducible form) are coprime with p and q, by a circular word of finite length.
Numerical example: Consider $P(X) = 2X - 3$.
For $a = 2/35$: $\ell = 6$, $g_6 = 665 = 35 * 19$, $a = N((2\,0\,1\,0\,2\,1))$.
For $b = 1/5$: $\ell = 2$, $g_2 = 5$, $b = N((0\,2)) = N((0\,2\,0\,2\,0\,2))$.
Then $a + b = 9/35 = N((2\,2\,1\,2\,2\,3)) = N((1\,1\,0\,1\,1\,2))$.

Examples.

- "Fibonacci": $P(X) = X^2 - X - 1$.
  With the Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, $f_{n+2} = f_{n+1} + f_n$, we obtain: $g_\ell = f_{\ell-1} + f_{\ell+1} - 1 + (-1)^{\ell+1}$ and

$$N((w_0 \dots w_{\ell-1})) = \{\frac{1}{g_\ell} \sum_{0 \leq i < \ell} w_i \left[f_i + (-1)^i f_{\ell-i}\right]\}$$
$$= \{\frac{1}{g_\ell} \sum_{0 \leq i < \ell} w_i \left[f_i + (-1)^{\ell+1} f_{-\ell+i}\right]\} \in [0,1[$$

Examples.

- "Fibonacci": $P(X) = X^2 - X - 1$.
  With the Fibonacci sequence: $f_0 = 0$, $f_1 = 1$, $f_{n+2} = f_{n+1} + f_n$, we obtain: $g_\ell = f_{\ell-1} + f_{\ell+1} - 1 + (-1)^{\ell+1}$ and

$$N((w_0 \dots w_{\ell-1})) = \{\frac{1}{g_\ell} \sum_{0 \le i < \ell} w_i \left[f_i + (-1)^i f_{\ell-i}\right]\}$$

$$= \{\frac{1}{g_\ell} \sum_{0 \le i < \ell} w_i \left[f_i + (-1)^{\ell+1} f_{-\ell+i}\right]\} \in [0,1[$$

Links with usual Fibonacci numeration system ?

Numerical example: $\ell = 5$, $g_5 = 11$,
$N((1\,0\,0\,0\,0)) = 5/11$, $N((0\,1\,0\,0\,0)) = 9/11$, $N((0\,0\,1\,0\,0)) = 3/11$,
$N((0\,0\,0\,1\,0)) = 1/11$, $N((0\,0\,0\,0\,1)) = 4/11$, $N((1\,0\,1\,0\,0)) = 8/11$,
$N((1\,0\,0\,1\,0)) = 6/11$, $N((0\,1\,0\,1\,0)) = 10/11$, $N((0\,1\,0\,0\,1)) = 2/11$,
$N((0\,0\,1\,0\,1)) = 7/11$

Work in progress - Open questions. For a fixed polynomial P (or a family of polynomials):

- Describe the rationals which are in $N(\mathcal{G})$, determine the smallest integer ℓ such that $a \in N(\mathcal{G}_\ell)$.
- For $a \in N(\mathcal{G}_\ell)$, give an efficient algorithm to find the circular word corresponding to a. Greedy-style algorithm ?
- For a real x in $[0, 1[$, can we find a sequence of circular words whose values converge towards x ? Study the convergence of the values of some sequences of words.
- What are the canonical representations of a circular word in terms of conditions on the digits ?
  (already made for the cases $X - b$, $pX - q$, $X^2 - kX - 1$)
- When p is a primitive prime factor of g_ℓ, there is a subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z}$, not being a $\mathcal{G}_n$. What is his interpretation ?
- When the $\mathcal{G}_\ell$ are not cyclic, for example are isomorphic to $E = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, each element of E as a unique representation by a circular word.
  Representation by a word of a couple $(a, b) \in [0, 1[^2$: interpretation ?

Work in progress - Open questions.

- Other questions...
- And of course more connections to usual topics in numeration.... ?

Thank you !

Benoît RITTAUD, "Structure of Classes of Circular Words defined by a Quadratic Equivalence", *RIMS Kôkyûroku Bessatsu*, **B 46**, 231-239 (2014-06).

Benoît RITTAUD & Laurent VIVIER, "Circular words and three applications: factors of the Fibonacci word, $\mathcal{F}$-adic numbers, and the sequence 1, 5, 16, 45, 121, 320,...", *Functiones et Approximatio* **47**, n°2, 207-231 (2012).