Numeration systems for circular words and applications to arithmetics

Benoît Rittaud*

April 2014

Abstract

We investigate some properties of finite abelian groups defined by equivalence relations on circular words. In particular, we show how the formalism of circular words gives rise naturally to the notion of numeration systems for finite abelian groups. We also give some consequences of our results, concerning the "gcd-property" of some linear recurrence sequences and a generalization of Fermat's little theorem.

Most numeration systems are intended to provide a codage of natural numbers and/or real numbers [2]. Here, we wish to provide a codage of elements of some finite abelian groups. Our basic structure is the notion of *(dotted) circular words*, introduced in the algebraic context in [7]. A dotted circular word (or, simply, a circular word) of length ℓ is a finite word made of ℓ letters of a given alphabet $\mathcal{A}$, indexed by $\mathbb{Z}/\ell\mathbb{Z}$ instead of $\{0,\dots,\ell-1\}$. (Note that we must have $\ell \geq 1$, i.e. the empty word $\varnothing$ does not give rise to a circular word $\widetilde{\varnothing}$.) We write $\widetilde{W}$ such a circular word, to distinguish from the usual finite word $W = w_0 \dots w_{\ell-1}$. When the dotted circular word is lengthy like $\widetilde{w_0 \dots w_{\ell-1}}$, we also write $\widetilde{\mathrm{cw}}(w_0 \dots w_{\ell-1})$ instead.

If the alphabet $\mathcal{A}$ is a group (in the sequel, we will consider only the case $\mathcal{A} = \mathbb{Z}$), then it is possible to equip naturally the set $\widetilde{\mathcal{A}^\ell}$ of circular words of length ℓ with a binary operation defined by the summation component by component, together with some equivalence relation $\approx$ that defines a "carry". A toy example is given by $\mathcal{A} = \mathbb{Z}$ embedded with the natural addition, and the "carry" defined by the combinatorics of base-2 numeration system, that is: for any i, we set

$$\widetilde{\mathrm{cw}}(w_0 \dots w_{i-2} w_{i-1} w_i w_{i+1} \dots w_{\ell-1}) \approx \widetilde{\mathrm{cw}}(w_0 \dots w_{i-2} (w_{i-1} - 2)(w_i + 1) w_{i+1} \dots w_{\ell-1}).$$

It is then easy to see that the quotient $\mathcal{G}_\ell := \widetilde{\mathbb{Z}^\ell}/\approx$ is isomorphic to the group $\mathbb{Z}/(2^\ell - 1)\mathbb{Z}$. A way to prove it consists in defining the function N on $\widetilde{\mathbb{Z}^\ell}$ by $N(\widetilde{\mathrm{cw}}(w_0 \dots w_{\ell-1})) := \sum_{i=0}^{\ell-1} w_i \cdot 2^i \bmod (2^\ell - 1)$, to show that two equivalent circular words have the same image under N, and that the quotient function is an isomorphism of groups. A straightforward generalization gives that base-b numeration systems for integer b together with circular words provide numeration systems for groups of the form $\mathbb{Z}/(b^\ell - 1)\mathbb{Z}$, that is: an ordered set of ℓ integers n_i (here: 1, b, b^2, ..., $b^{\ell-1}$) such that the function $N : \widetilde{\mathcal{A}^\ell} \longrightarrow \mathbb{Z}/(b^\ell - 1)\mathbb{Z}$ defined by $N(\widetilde{\mathrm{cw}}(w_0 \dots w_{\ell-1})) := \sum_{i=0}^{\ell-1} w_i n_i$ provides a one-to-one correspondence between the equivalence classes of $\widetilde{\mathcal{A}^\ell}$ and the elements of $\mathbb{Z}/(b^\ell - 1)\mathbb{Z}$. Since a real number is rational iff its b-expansion is periodic (with $b \in \mathbb{N}$, b> 1), what precedes can be used to construct the set $\mathbb{Q}$ of rational numbers (see [8]); it can be regarded as a way to construct the set $\mathbb{Q}_b$ of rational b-adic numbers as well.

*Université Paris-13, Sorbonne Paris Cité, LAGA, CNRS, UMR 7539, F-93430 Villetaneuse, France. rittaud@math.univ-paris13.fr

Our aim is to investigate some generalizations of these basic facts to other possible definitions of the carry, extending previous results on the field that were limited to the Fibonacci numeration system [7], [6] and quadratic cases of the form $X^2 = kX + 1$ with $k \in \mathbb{N}^*$ [5]. We will emphasize on these cases as well as on the case of a very nice numeration system introduced by Shigeki Akiyama *et al.* [1], namely the rational base number systems. Eventually, we provide arithmetical consequences of the theory (natural generalizations of Fermat's little theorem and the property $\gcd(F_m, F_n) = F_{\gcd(m,n)}$ for the Fibonacci sequence $(F_n)_n$), and conclude by some remarks about representatives of equivalence classes that can be recognized by some natural language.

1 General algebraic structures on circular words

For a given alphabet $\mathcal{A}$, we put $\widetilde{\mathcal{A}^*} := \cup_{\ell \geq 1} \widetilde{\mathcal{A}^\ell}$, and write $|\widetilde{W}|$ for the length of $\widetilde{W} \in \widetilde{\mathcal{A}^*}$. Let $\widetilde{W'}$ be also in $\widetilde{\mathcal{A}^*}$. Then, $\widetilde{W}\widetilde{W'} = \widetilde{WW'}$ stands for the circular word defined by the concatenation of W and W'. We also define $\widetilde{W}^1 := \widetilde{W}$ and $\widetilde{W}^n = \widetilde{W}\widetilde{W}^{n-1}$ for any $n \geq 2$. The *power equivalence* $\approx_p$ on $\widetilde{\mathcal{A}^*}$ identifies $\widetilde{W}$ with all of its powers.

Assume that a binary operation $+$ is defined on $\mathcal{A}$. For $|\widetilde{W}| = |\widetilde{W'}|$, the sum of $\widetilde{W}$ and $\widetilde{W'}$ is defined letter by letter. Since for any $\widetilde{W}$ and $\widetilde{W'} \in \widetilde{\mathcal{A}^*}$ we have $|\widetilde{W}^{|W'|}| = |\widetilde{W'}^{|W|}|$, it is easy to check that the previous addition extends to an addition on $\widetilde{\mathcal{A}^*}/\approx_p$, and that if $(\mathcal{A}, +)$ is a group (resp. an abelian group, a monoid), then so is $(\widetilde{\mathcal{A}^*}/\approx_p, +)$.

Let $d \geq 1$ be fixed. We choose $d+1$ elements of $\mathcal{A}$, denoted by $a_0, \ldots, a_d$, satisfying that $a_0 \neq 0$ and $a_d \neq 0$. It can be shown that it is of no inconvenience to assume $\gcd(a_0, \ldots, a_d) = 1$. Define, for any $\ell \geq 1$ and any integer $0 \leq i \leq d$, the circular word $\widetilde{A_{\ell,i}} \in \widetilde{\mathcal{A}^\ell}$ whose letters are all equal to 0 but the one indexed by $i \mod \ell$, equal to a_i. We put $\widetilde{A_\ell} := \sum_{0 \leq i \leq d} \widetilde{A_{\ell,i}}$. We set the *carry equivalence relation* $\approx$ between circular words of same length ℓ by: $\widetilde{W} \approx \widetilde{W'}$ iff there exists integers $v_0, \ldots, v_{\ell-1}$ such that $\widetilde{W} = \widetilde{W'} + \sum_{1 \leq i \leq k} v_i \sigma^{-i}(\widetilde{A_\ell})$, where σ is the *shift* transformation defined by $\sigma(\widetilde{\mathrm{cw}}(w_0 \ldots w_{\ell-1})) := \widetilde{\mathrm{cw}}(w_1 \ldots w_{\ell-1} w_0)$. Again, it is easy to see that if $\mathcal{A}$ is a group (resp. an abelian group, a monoid), then so is $\mathcal{G}_\ell := \widetilde{\mathcal{A}^\ell}/\approx$.

A $\ell \times \ell$-*circulant matrix* is an array of elements $m_{i,j}$ of $\mathcal{A}$, indexed by $(\mathbb{Z}/\ell\mathbb{Z})^2$ and such that, for any i and j, $m_{i+1,j+1} = m_{i,j}$. Any such matrix can be described by its first row, written on the form of a dotted circular word $\widetilde{A}$, the next rows being equal to $\sigma^{-1}(\widetilde{A})$, $\sigma^{-2}(\widetilde{A})$, $\ldots$, $\sigma^{-(\ell-1)}(\widetilde{A})$. For any $\widetilde{A}$, we write $C_{\widetilde{A}}$ for the corresponding circulant matrix. Let $\ell \geq 1$ be given. With the notation of the previous section, we have the following

Proposition 1. *For $\mathcal{A} = \mathbb{Z}$, if the polynomial $P(X) := a_d X^d + \cdots + a_1 X + a_0$ does not admits any ℓ-th root of unity as a root, then $c_\ell := \mathrm{card}(\mathcal{G}_\ell) = |\det(C_{\widetilde{A_\ell}})|$.*

The assumption on P is made to ensure that $C_{\widetilde{A_\ell}}$ is invertible, a necessary and sufficient condition to have that $\mathcal{G}_\ell$ is finite.

Theorem 1. *For $\mathcal{A} = \mathbb{Z}$, let $E = (e_{i,j})_{i,j} \in \mathcal{M}_d(\mathbb{Z})$ with $e_{1,j} = -a_j/a_0$ for all j and $e_{i+1,i} = 1$ for all $1 \leq i < d$. For any $\ell \geq 1$, we have*

$$c_\ell = a_0^\ell \cdot |\det(E^\ell - I)|.$$

The proof is a simple Gaussian reduction. Some more algebra gives then:

Proposition 2. *Let Λ^+ be the set of roots of P bigger than 1 in modulus (each of these roots being written according to its order of multiplicity). We have*

$$\lim_{\ell\to+\infty}\left(\frac{c_{\ell+1}}{c_\ell}\right) = \exp\left(\int_{\mathbb{U}} \log(|P(z)|)\mathrm{d}z\right) = \left|a_0 \prod_{\lambda\in\Lambda^+} \lambda\right|.$$

Proposition 2 implies that, for any choice of P, the sequence $(c_\ell)_\ell$ is growing exponentially with ℓ. Nevertheless, it is worth mentioning that we may not have $c_{\ell+1} > c_\ell$ for all ℓ. Indeed, for $P(X) = X^3 - X^2 - X - 1$ (the Tribonacci numeration), the first terms of $(c_\ell)_\ell$ are 2, 4, 2, 16, 22, 28, 86...

2 Numeration system on $\mathcal{G}_\ell$ and structure of $\mathcal{G}_\ell$

From now, we work within the assumptions of Proposition 1, and assume $\gcd(a_0, \ldots, a_d) = 1$. Let $\widetilde{B_\ell} := \widetilde{\mathrm{cw}}(b_0 \ldots b_{\ell-1})$ be the circular word for which $(1/c_\ell)\cdot C_{\widetilde{B_\ell}} = (C_{\widetilde{A_\ell}})^{-1}$: by Proposition 1, we have $\widetilde{B_\ell} \in \widetilde{\mathbb{Z}^\ell}$. The circular word $\widetilde{B_\ell}$ defines our *numeration system* on $\mathcal{G}_\ell$ by the way of the function

$$\begin{array}{rccc} N : & \mathcal{G}_\ell & \longrightarrow & \mathbb{Z}/c_\ell\mathbb{Z} \\ & \widetilde{\mathrm{cw}}(w_0 \ldots w_{\ell-1})) & \longmapsto & \displaystyle\sum_{0\le i<\ell} w_i b_i \pmod{c_\ell}. \end{array}$$

As recalled in introduction, in the classical case of base b numeration, we have $b_i = b^i$, and the application N characterizes the equivalent classes of circular words by the property: $\widetilde{W} \approx \widetilde{W'}$ iff $N(\widetilde{W}) = N(\widetilde{W'})$. Here is what this result becomes in the general case:

Theorem 2. *Assume a_d or a_0 be prime to c_ℓ. For any $\widetilde{W}$, $\widetilde{W'} \in \widetilde{\mathcal{A}^\ell}$, we have*

$$\widetilde{W} \approx \widetilde{W'} \iff N(\sigma^n(\widetilde{W})) = N(\sigma^n(\widetilde{W'})) \text{ for any } 0 \le n < d.$$

There are various cases in which the hypothesis $\gcd(a_d, c_\ell) = 1$ (or $\gcd(a_0, c_\ell) = 1$) is true for any ℓ. The simplest one is, of course, the one in which $a_d = 1$ (or $a_0 = 1$). Another case which is worth mentioning is the case $d = 1$ with a_0 and a_1 mutually prime (we will deal with this case more extensively in section 4).

Theorem 3. *Assume a_d or a_0 be prime to c_ℓ. Let $\widetilde{W} \in \widetilde{\mathcal{A}^\ell}$ such that, for some integer m, we have $\widetilde{W} \approx \sigma^m(\widetilde{W})$. Then, $\widetilde{W} \in \mathcal{G}_{\gcd(m,\ell)}$ (i.e. we can find $\widetilde{X} \in \widetilde{\mathcal{A}^d}$ such that $\widetilde{W} \approx \widetilde{X^{\ell/d}}$, where $d = \gcd(m, \ell)$).*

Corollary 1. *For any ℓ and ℓ' such that a_0 and a_d are prime to c_ℓ and $c_{\ell'}$, we have $\mathcal{G}_\ell \cap \mathcal{G}_{\ell'} = \mathcal{G}_{\gcd(\ell,\ell')}$.*

All of this allows to describe in a complete manner the structure of the finite abelian groups $\mathcal{G}_\ell$. For brievety, we only mention here one result simple to state: for a_d or a_0 prime to c_ℓ, $\mathcal{G}_\ell$ is monogenetic iff $\gcd(b_i, c_\ell) = 1$ for some i.

3 Applications

3.1 The Tetris number

Definition 1. *For any $\ell \geq 1$, let us call the ℓ-th* Tetris number *of $(a_i)_{0\leq i\leq d}$ the smallest positive integer t such that $\widetilde{t^\ell} \approx \widetilde{0^\ell}$.*

The name comes from the fact that we can consider the problem in the framework of the well-known video game Tetris. Our "playing field" is of width ℓ (and is embedded within a toral structure) and the famous rigid tetraminoes are replaced by a unique model of piece, which cannot be rotated but whose $d+1$ columns can slide along each other. The i-th column of the piece contains a_i blocks (possibly of negative value), and the aim of the game is to let pieces fall down the playing field until they constitutes a rectangle of width ℓ and height t.

Proposition 3. *For any ℓ, $t_\ell = c_1 = |\sum_i a_i|$.*

3.2 Fermat's little theorem

Proposition 4. ("Fermat's little Theorem") *For any prime number p, we have*

$$c_p \equiv |\sum_i a_i| \pmod p.$$

The original Fermat's little Theorem corresponds to the special case of numeration in base b (i.e. $d = 1$, $a_0 = -b$ and $a_1 = 1$), in which we have $c_p = b^p - 1$ and $c_1 = b - 1$. Another example of interest is the case of $P(X) = aX - b$ with $0 < a < b$ and a and b mutually prime (see also section 4), for which Proposition 4 writes $b^p - a^p \equiv b - a \pmod p$. A third interesting case is given by $P(X) = X^2 - X - 1$. In this case, we have that, for any odd value of ℓ, $c_\ell = L_\ell$, where $(L_\ell)_\ell$ is the *Lucas sequence*, defined by $L_1 = 1$, $L_2 = 3$ and $L_\ell = L_{\ell-1} + L_{\ell-2}$ for $\ell \geq 3$. Therefore, Proposition 4 proves that, for any prime number p, we have $L_p \equiv 1 \pmod p$.

3.3 The gcd property

More than a century ago, Édouard Lucas [4] (see also [3]) made the observation than, for the Fibonacci sequence $(F_n)_n$ defined by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$, we have what we could call the *gcd-property*: for any integers m and n, we have $\gcd(F_m, F_n) = F_{\gcd(m,n)}$. The following result can be regarded as a way to generalize this observation.

Theorem 4. *For any ℓ and ℓ', $c_{\gcd(\ell,\ell')} = \gcd(c_\ell, c_{\ell'})$.*

As an example, it is proved in [7] that, in the case $P(X) = X^2 - X - 1$, we have $c_{4\ell} = 5F_{2\ell}^2$. Therefore, Theorem 4 proves Lucas's observation for all even indices m and n. We will not complete the proof here for other indices, but only mention that the value $5F_{2\ell+1}^2$ is the cardinality of the quotient $\mathcal{G}_{4(2\ell+1)}/\mathcal{G}_{2(2\ell+1)}$.

4 The question of canonical representatives in some particular cases

When applied to the elementary case of base b numeration system, Theorem 1 gives that $c_\ell = b^\ell - 1$. This value is exactly equal to the cardinality of the set of circular words of length ℓ

on the alphabet $\{0, 1, \ldots, b-1\}$, where the classical identification $\widetilde{(b-1)^\ell} = \widetilde{0^\ell}$ is made. In [7] as well as in [5], where the cases $P(X) = X^2 - kX - 1$ are investigated, the cardinality of the groups $\mathcal{G}_\ell$ is obtained by the natural generalization of *admissible forms*. The idea is there to define a language $\mathcal{L}$ such that each equivalence class has a unique representative recognized by $\mathcal{L}$. Counting the nomber of circular words of length ℓ recognized by $\mathcal{L}$ therefore provided the value of c_ℓ. For $k \geq 1$, a suitable language is defined by the alphabet $\{0, 1, \ldots, k\}$ and the condition $w_i = k \implies w_{i+1} = 0$. The only exception occurs in the case $\ell = 2m$, in which the null class has exactly three representatives recognized by the language: $\widetilde{\mathrm{cw}}(0^\ell)$, $\widetilde{\mathrm{cw}}((0k)^m)$ and $\widetilde{\mathrm{cw}}((k0)^m)$. (Note also that, in that case, the group $\mathcal{G}_\ell$ is not monogenetic for all values of ℓ. For example, for $k = 1$, it is monogenetic iff ℓ is odd, otherwise it is generated by two elements.)

Another case which is worth mentioning is the Tribonacci case, defined by the polynomial $P(X) = X^3 - X^2 - X - 1$. It provides an example in which what could appear as the natural language to define canonical representation (the language on $\{0, 1\}$ excluding factors of the form 111) is not convenient as it is for the case $X^2 - kX - 1$. Indeed, not only the cardinality of circular words of length ℓ recognized by this language is not equal to c_ℓ, but it is also sometimes *less* than it. Indeed, a standard analysis shows that the number of such circular words is equal to $2u_{\ell-4} + u_{\ell-3} + u_{\ell-1}$, where $(u_n)_n$ is the sequence defined by $u_0 = 1$, $u_1 = 2$, $u_2 = 4$ and $u_n = u_{n-1} + u_{n-2} + u_{n-3}$ for any $n \geq 3$. Hence, we get that $u_\ell < c_\ell$ for example for $\ell = 4, 5, 7, 10, 13, 16, 19, \ldots$ We do not have a full explanation right now of this phenomenon, but it seems probable that what precedes could be a useful step to understand it better.

Finally, let us consider in some details the case of a very interesting numeration system introduced by Shigeki Akiyama *et al.* [1], here corresponding to the polynomial $P(X) = aX - b$ with $0 < a < b$.

Proposition 5. *For $P(X) = aX - b$ with $0 < a < b$, any element of $\mathcal{G}_\ell$ has a unique representative of the form $\widetilde{\mathrm{cw}}(w_0 \ldots w_{\ell-1})$ such that all the w_is belong to $\{0, 1, \ldots, b-1\}$ and such that at least one w_i satisfies $w_i \leq b - a$.*

Note that, in the classical case $P(X) = X - 10$ of decimal numeration system, the latter condition consists in forbidding the writing $\widetilde{99 \ldots 99}$ for the neutral element $\widetilde{00 \ldots 00}$.

In the case $P(X) = aX - b$, some complementary informations of an arithmetical nature can be easily given. Without loss of generality, assume $\gcd(a, b) = 1$. It is then easy to prove that, for any q prime to both a and b, there exists ℓ such that q divides $c_\ell = b^\ell - a^\ell$ (consider k and k' such that $a^k \equiv 1 \pmod{q}$ and $b^{k'} \equiv 1 \pmod{q}$, then take $\ell = \mathrm{lcm}(k, k')$). By Corollary 1, and since all the $\mathcal{G}_\ell$ are monogenetic (hence isomorphic to $\mathbb{Z}/c_\ell\mathbb{Z}$), we get that the subgroup $\mathcal{P}_q$ made of all elements of $\widetilde{\mathcal{A}^*}$ of order q is isomorphic to $\mathbb{Z}/q\mathbb{Z}$. This remark provides an alternative way of expanding fractions in this numeration system, which is equivalent neither to the one provided by the greedy algorithm nor to the one given by the modified Euclidean algorithm of [1]. Contrarily to these expansions, we get here rational numbers for which, as in the usual base b numeration system, the expansion is ultimately periodic. For example, in the case $P(X) = 2X - 3$, the denominator $q = 5$ can be obtained with $\ell = 2$ (since we have $c_2 = 3^2 - 2^2 = 5$). The set $\mathcal{G}_2$ is equal to $\{\widetilde{00}, \widetilde{01}, \widetilde{02}, \widetilde{20}, \widetilde{10}\}$, and the expresssions $0.\overline{01}$, $0.\overline{02}$, $0.\overline{20}$ and $0.\overline{10}$ are respectively equal to $4/5$, $8/5$, $12/5$ and $6/5$. Nevertheless, not only the fractions with denominator q not prime to a and b are excluded of the process (for any ℓ, the value $c_\ell = b^\ell - a^\ell$ is prime to both b and a, hence no $\mathcal{G}_\ell$ has $\mathbb{Z}/a\mathbb{Z}$ or $\mathbb{Z}/b\mathbb{Z}$ as a subgroup), but also, for a given denominator q, not all numerators p provide a fraction p/q for which a ultimately periodic expansion can be obtained. To stay in the case $P(X) = 2X - 3$ and $q = 5$, it is easy to show that no ultimately periodic expression (on the allowed language on the alphabet $\{0, 1, 2\}$), even with a periodic part in $\mathcal{G}_2$, is equal to $1/5$.

References

[1] S. Akiyama, Christiane Frougny & Jacques Sakarovitch, *Powers of rationals modulo 1 and rational base number systems*, Israel Journal of Mathematics **168**, 53-91, 2008.

[2] Ch. Frougny, *Numeration systems*, in Lothaire, *Algebraic Combinatorics on Words*, Cambridge University Press, 2002.

[3] G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1960.

[4] É. Lucas, *Recherches sur plusieurs ouvrages de Léonard de Pise et sur diverses questions d'arithmétique supérieure*, Imprimerie des sciences mathématiques et physiques, Rome, 1877.

[5] B. Rittaud, *Structure of Classes of Circular Words defined by a Quadratic Equivalence*, RIMS Kôkyûroku Bessatsu (to appear).

[6] B. Rittaud and L. Vivier, *Circular words and applications*, Proceedings 8th International Conference Words 2011, Prague, 31-36, 2011.

[7] B. Rittaud and L. 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.

[8] B. Rittaud and L. Vivier, *The Field $\mathbb{Q}$ and the Equality* $0.999\ldots = 1$ *from the Standpoint of Circular Words and History* (submitted).