Complexity of Periodic Sequences

Wieb Bosma[1]

Radboud University Nijmegen, P.O. Box 9010,
6500 GL Nijmegen, the Netherlands, email: `w.bosma@math.ru.nl`

Abstract. Periodic sequences form the easiest sub-class of k-automatic sequences. Two characterizations of k-automatic sequences lead to two different complexity measures: the sizes of the minimal automaton with output generating the sequence on input either the k-representations of numbers or their reverses. In this note we analyze this exactly.

1 Introduction

By definition, an infinite k-automatic sequence $a = (a_n)_{n=0}^{\infty} = a_0a_1a_2a_3\cdots$ is the output of a deterministic finite automaton with output (DFAO) upon feeding the index n as input for a_n. In [2] two obvious complexity measure for such sequences are compared. The first, denoted $\|a\|_k$, is simply the size (that is, the number of states) of the smallest DFAO that produces a; the second, $\|a\|_k^R$ (the reversed size) is the size of the smallest DFAO that produces a when the input for n is the reverse of the k-ary representation of n. In general the two measures may differ, even exponentially, in size. In this note we attempt to analyze the exact values of both complexity measures for periodic sequences a. It turns out that in this case $\|a\|_k = O(n)$ and $\|a\|_k^R$ is $O(n^2)$; we will be more precise in the statement of the main theorems.

The main tool for the analysis is the basic result that $\|a\|_k^R$ is essentially equal to the size of the k-kernel $K_k(a)$; this kernel may be defined to be the smallest set of infinite sequences containing a as well as every $p_j(b)$ for any $b \in K_k(a)$ and any j with $0 \le j < k$, where $p_j(b) = (b_{j+n})_{n=0}^{\infty} = b_jb_{j+n}b_{j+2n}b_{j+3n}\cdots$. By [1], Theorem 6.6.2, a is k-automatic if and only if $K_k(a)$ is finite. For periodic sequences $\|a\|_k^R = |K_k(a)|$, see Theorem 4 in [2].

In this note we will mainly be concerned with the case of binary sequences and with $k = 2$; most result easily generalize (see also the Remarks).

2 Basic definitions

For any $k \ge 2$ and $\Sigma_k = \{0, 1, \ldots, k-1\}$ every natural number n has a unique representation $(n)_k \in \Sigma_k^*$, where $(0)_k = \epsilon$ and

$$(n)_k = a_0a_1\cdots a_r \iff n = a_0k^r + a_1k^{r-1} + \cdots + a_{r-1}k + a_r \wedge a_0 > 0$$

for $n > 0$. Conversely, every $u \in \Sigma_k^*$ represents a number $[u]_k$:

$$[a_0a_1\cdots a_r]_k \ = \ a_0k^r + a_1k^{r-1} + \cdots + a_{r-1}k + a_r.$$

For any Σ and any string $u \in \Sigma^*$ the reverse u^R of u is defined by $(u_1 u_2 \cdots u_n)^R = u_n u_{n-1} \cdots u_1$.

The set of infinite sequences $a = a_0 a_1 a_2 a_3 \cdots$ over a finite alphabet Γ is denoted by $\Gamma^{\mathbb{N}}$.

A deterministic finite automaton M with output (DFAO) is a tuple $M = (Q, \Sigma, \delta, q_0, \Gamma, \tau)$, of a finite set of states Q with $q_0 \in Q$ the initial state, a finite input alphabet Σ and finite output alphabet Γ, a transition function $\delta : Q \times \Sigma \to Q$, and output function $\tau : Q \to \Gamma$. We mainly focus on the case $\Sigma = \Gamma = \Sigma_2$.

The transition function δ extends to $\delta : Q \times \Sigma^* \to Q$, and a DFAO thus defines a function $f_M : \Sigma^* \to \Gamma$ defined by $f_M(u) = \tau(\delta(q_0, u))$.

An infinite sequence $a \in \Gamma^{\mathbb{N}}$ is called k-automatic if a k-DFAO exists such that $a_{[w]_k} = \tau(\delta(q_0, w)$ for all $w \in \Sigma_k^*$: the automaton produces a_n upon reading the k-ary representation of n. According to Theorem 5.2.3 from [1] a this is equivalent to the existence of a DFAO that produces a_n upon reading the reverse of the k-ary representation of n. As a matter of fact the latter automaton can be constructed directly from the k-kernel $K_k(a)$: its states Q correspond to the elements of $K_k(a)$ (with initial state a), and with input alphabet Σ_k the transition maps $\delta : K_k(a) \times \Sigma_k \to Q$ are given by $\delta(b, i) = p_i(b)$ for any $b \in K_k(a)$, while the output function $\tau : Q \to \Gamma$ is $\tau(b) = b_0$. Here p_i was defined in the previous section as the function that selects the subsequence with indices $i \bmod k$ from a given sequence.

3 Periodic sequences

We intend to analyze the complexity of periodic sequences. In this section m will be a positive integer. A sequence a will be called m-periodic if $a_{i+m} = a_i$ for every natural number i; the set of all m-periodic sequences is denoted P_m. Note that the *period* of a (by definition the least positive integer p for which a is p-periodic) will be a divisor of m, which may be, but is not necessarily, the same as m. For an m-periodic a we can write $a = (a_0 a_1 \cdots a_{m-1})^\omega$.

By $(\mathbb{Z}/m\mathbb{Z})^*$ we indicate the multiplicative group of integers modulo m, and by $\mathrm{ord}(a, m)$ we denote the multiplicative order of $a \bmod m$, the smallest positive integer k for which $a^k \equiv 1 \bmod m$, for any a coprime to m. Also, ϕ will be the Euler-phi function on the positive integers, that is, $\phi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$ is the order of the multiplicative group (and the number of integers less than m coprime to m).

The main result on the complexity is this.

Theorem 1. *Let m be the period of periodic sequence a, and write $m = 2^r \cdot s$, with s odd. Then $r + s \leq \|a\|_2 \leq m$.*

Corollary 2 *For any periodic sequence a of odd period m holds $\|a\|_2 = m$.*

Conjecture 3 *For any $m = 2^r s$ (with s odd) and any integer n such that $r + s \leq n \leq m$ there exists a periodic sequence a with $\|a\|_2 = n$.*

Proof. (Sketch) We first prove the upper bound. We construct a 2-DFAO M that will output the given m-periodic sequence a. The states of M will correspond to the residue classes modulo m, and the initial state corresponds to 0 mod m. The transition maps will be defined by $\delta(x, j) = k \cdot x + j \bmod m$, for any $x \in \mathbb{Z}/m\mathbb{Z}$ and $0 \leq j < 2$. The output function is given by $\tau(x) = a_{x \bmod m}$, which is well-defined as $a \in \Gamma^{\mathbb{N}}$ is m-periodic.

This automaton does what it should do, since reading a symbol j corresponds in the 2-ary representation to replacing the index n by $k \cdot n + j$. So this proves that $\|a\|_k \leq m$.

For the lower bound we first prove the result (stated separately in the Corollary) for the odd case $r = 0$, and then show that the sequence with period 10^{m-1} has complexity $r + s$, and then show that any other sequence has complexity at least as large. □

Remarks 4 There is compelling numerical evidence (for small r, s) that indeed every value in the range from $r + s$ to m is attained by $\|a\|_2$ for many sequences a. It is usually not difficult to exhibit an example a with given value for $\|a\|_2$ in this range. But we do not have a general proof for this statement.

4 The *k*-kernel

The purpose of this section is to establish the exact size of the kernel (and hence the 'reversed complexity') of periodic sequences. We will focus on the case where $k = 2$ (binary representation of natural numbers) and binary sequences (so the output alphabet is also $\Sigma_2 = \{0, 1\}$).

In this case we denote the operations p_0 (take the subsequence of even index) and p_1 (those of odd index) by even and odd. The main proofs of this section are given by looking at the action of these two operations on the set P_m of m-periodic sequences. First note the following properties of odd and even in their action on P_m:

(1) under composition, odd and even form a non-commutative *semigroup* $S = \langle \mathsf{odd}, \mathsf{even} \rangle$, with the empty product as 1;
(2) if m is odd, then $\mathsf{odd}^k = 1 = \mathsf{even}^k$ for $k = \mathrm{ord}(2, m)$, and this is the smallest positive integer with that property;
(3) hence, for odd m again, $\mathsf{odd}^{k-1} = \mathsf{odd}^{-1}$ and $\mathsf{even}^{k-1} = \mathsf{even}^{-1}$, and $S = \langle \mathsf{odd}, \mathsf{even} \rangle$ is a finite *group*;
(4) the element $m_2 = \mathsf{even}^{-1}$ in this group acts in on $a \in P_m$ by $a_j \mapsto a_{2j}$ with the index taken modulo m, so

$$m_2((a_0 a_1 a_2 \cdots a_{m-1})^\omega) = (a_0 a_{\frac{m+1}{2}} a_1 a_{\frac{m+3}{2}} a_2 \cdots a_{\frac{m-1}{2}})^\omega.$$

If $p_1, p_2, \ldots, p_w$, with $0 \leq w \leq m$ and $0 \leq p_1 < p_2 < \cdots < p_w < m$ are the positions in the period of a where a 1 occurs, then $m_2(a)$ is m-periodic with 1 exactly at the positions $2p_1, 2p_2, \ldots, 2p_w$ mod m.

(5) the shift operator tail, acting by $\mathsf{tail}(a_0a_1a_2\cdots) = a_1a_2\cdots$ is also in this group (for m odd): $\mathsf{tail} = \mathsf{even}^{-1} \circ \mathsf{odd} \in \langle \mathsf{odd}, \mathsf{even} \rangle$, and it satifies the additional properties:

(6) $\langle \mathsf{odd}, \mathsf{even} \rangle = S = \langle \mathsf{tail}, m_2 \rangle$;

(7) $\mathsf{tail}^2 \circ m_2 = m_2 \circ \mathsf{tail}$.

Theorem 5. *Let a be an m-periodic sequence for m odd; then $|K_2(a)|$ is at most $\mathrm{ord}(2, m) \cdot m$, which is a divisor of $\phi(m) \cdot m$. In particular*

$$\|a\|_2^R = |K_2(a)| \le (m-1) \cdot m.$$

Proof. By the above properties, for m odd, the semigroup S is a group, generated by m_2 and tail as well as by odd and even. Clearly, the order of m_2 equals $\mathrm{ord}(2, m)$, by Properties 4 and 2, and the order of tail and tail^2 equals m. Elements of the group can now be written as $m_2^x \circ \mathsf{tail}^y$, with $0 \le x < \mathrm{ord}(2, m)$ and $0 \le y < m$, while it follows from Property 4 that $m_2^x \notin \langle \mathsf{tail} \rangle$, unless $x = 0$. Hence the order of the group equals $\mathrm{ord}(2, m) \cdot m$.

For any element $a \in P_m$ it will be clear that the size of the orbit a^S is bounded by $|S|$, Since $K_2(a)$ is by definition equal to the orbit a^S, we obtain the inequality $|K_2(a)| \le \mathrm{ord}(2, m) \cdot m$. To obtain the final result, note that $\mathrm{ord}(2, m)$ is the order of the element 2 in the group $(\mathbb{Z}/m\mathbb{Z})^*$, hence divides the group order $\phi(m)$, which is at most $m - 1$. $\square$

The following theorem implies that for every odd $m > 7$ the upper bound $\mathrm{ord}(2, m) \cdot m$ on the size of the kernel is attained for some m-periodic sequence.

Theorem 6. *Let $m \ge 9$ be odd, and let c be the periodic sequence, of period length m, and period 10110^{m-4}, so $c = (10110^{m-4})^\omega$. Then the kernel $K_2(c)$ of c consists of $\mathrm{ord}(2, m) \cdot m$ elements.*

Proof. Let $c = (10110^{m-4})^\omega$ for some odd $m \ge 9$. We use the presentation $S = \langle m_2, \mathsf{tail} \rangle$ for the group S (Property 6 above) and keep track of the positions of the 1s in the sequence c under the action of elements of S. We will show that the orbit c^S contains $\mathrm{ord}(2, m) \cdot m$ different images, whence the theorem follows from the previous proposition.

In the period of c itself, there are only 1s in positions with index in $\{0, 2, 3\}$. Taking all positions modulo m, it is clear that for $0 \le j < m$ the periodic sequences $\mathsf{tail}^j(c)$ have 1s precisely in the positions $\{j, j + 2, j + 3\}$. And $m_2^i(c)$ has 1s in positions $\{0, 2^{i+1}, 3 \cdot 2^i\}$, by Property 4. It is then also obvious that $\mathsf{tail}^j \circ m_2^i(c)$ has 1s exactly in the positions $\{j, 2^{i+1} + j, 3 \cdot 2^i + j\}$.

Suppose that the positions of the 1s for $\mathsf{tail}^j \circ m_2^i(c)$ and $\mathsf{tail}^l \circ m_2^k(c)$ coincide, that is, the sets $\{j, 2^{i+1} + j, 3 \cdot 2^i + j\}$ and $\{l, 2^{k+1} + l, 3 \cdot 2^k + l\}$ are the same. Since these sets of positions (all taken modulo m) may be permutations of each other, we consider six cases:

(i) $j \equiv l$, $2^{i+1} + j \equiv 2^{k+1} + l$, and $3 \cdot 2^i + j \equiv 3 \cdot 2^k + l$;
from $j \equiv l$ it follows that $i \equiv k \bmod \mathrm{ord}(2, m)$.

(ii) $j \equiv l$, $2^{i+1} + j \equiv 3 \cdot 2^k + l$, and $3 \cdot 2^i + j \equiv 2^{k+1} + l$;
again $j \equiv l$ and we find $3 \cdot 2^i \equiv 2^{k+1}$ and $3 \cdot 2^k \equiv 2^{i+1}$. It follows that $3 \cdot 2^{i+1} \equiv 9 \cdot 2^k \equiv 2^{k+2}$ and so $5 \cdot 2^k \equiv 0 \bmod m$, which contradicts $m > 7$ odd.

(iii) $j \equiv 2^{k+1} + l$, $2^{i+1} + j \equiv l$, and $3 \cdot 2^i + j \equiv 3 \cdot 2^k + l$; the first two imply that $2^i + 2^k \equiv 0 \bmod m$, and substituting this and the first in the third equation gives $-3 \cdot 2^k + 2^{k+1} + l \equiv 3 \cdot 2^k + l$, so $4 \cdot 2^k \equiv 0 \bmod m$, which is impossible for odd $m > 1$.

(iv) $j \equiv 2^{k+1} + l$, $2^{i+1} + j \equiv 3 \cdot 2^k + l$, and $3 \cdot 2^i + j \equiv l$; in this case $2^{i+1} + 2^{k+1} \equiv 0$ and $3 \cdot 2^i + 2^{k+1} \equiv 3 \cdot 2^k$ imply that $4 \cdot 2^{i+1} \equiv 0 \bmod m$, which is impossible.

(v) $j \equiv 3 \cdot 2^k + l$, $2^{i+1} + j \equiv l$, and $3 \cdot 2^i + j \equiv 2^{k+1} + l$; now the first and second yield $2^{i+1} + 3 \cdot 2^k \equiv 0$, while second and third give $3 \cdot 2^i + 3 \cdot 2^k \equiv 2^{k+1}$; from this we find $7 \cdot 2^k \equiv 0 \bmod m$, which contradicts $m > 7$ odd.

(vi) $j \equiv 3 \cdot 2^k + l$, $2^{i+1} + j \equiv 2^{k+1} + l$, and $3 \cdot 2^i + j \equiv l$; first and third equation imply $3 \cdot 2^k + 3 \cdot 2^i \equiv 0$, while second and third combine to $2^{k+1} + 2^i \equiv 0 \bmod m$. Together this can only be if $3 \cdot 2^k \equiv 0 \bmod m$, contradicting $m > 7$ being odd.

We conclude that for odd $m > 7$ the positions can only coincide in the first case, and then only when $j \equiv l \bmod m$ and $i \equiv k \bmod \mathrm{ord}(2, m)$, and thus there are $\mathrm{ord}(2, m) \cdot m$ different images in c^S. □

Example 7 Here, for example is a scheme for the 54 images in the case $m = 9$:

{0, 2, 3}	{1, 3, 4}	{2, 4, 5}	{3, 5, 6}	{4, 6, 7}	{5, 7, 8}	{0, 6, 8}	{0, 1, 7}	{1, 2, 8}
{0, 4, 6}	{1, 5, 7}	{2, 6, 8}	{0, 3, 7}	{1, 4, 8}	{0, 2, 5}	{1, 3, 6}	{2, 4, 7}	{3, 5, 8}
{0, 3, 8}	{0, 1, 4}	{1, 2, 5}	{2, 3, 6}	{3, 4, 7}	{4, 5, 8}	{0, 5, 6}	{1, 6, 7}	{2, 7, 8}
{0, 6, 7}	{1, 7, 8}	{0, 2, 8}	{0, 1, 3}	{1, 2, 4}	{2, 3, 5}	{3, 4, 6}	{4, 5, 8}	{0, 5, 6}
{0, 3, 5}	{1, 4, 6}	{2, 5, 7}	{3, 6, 8}	{0, 4, 7}	{1, 5, 8}	{0, 2, 6}	,{1, 3, 7}	{2, 4, 8}
{0, 1, 6}	{1, 2, 7}	{2, 3, 8}	{0, 3, 4}	{1, 4, 5}	{2, 5, 6}	{3, 6, 7}	{4, 7, 8}	{0, 5, 8}

The positions of 1s in the period are given: the top left entry gives the initial sequence $c = (101100000)^\omega$ and to its right all of its shifts. Below it we find $m_2(c) = (100010100)^\omega$, below that $m_2^2(c) = (100100001)^\omega$ etc. Note that it is always the case that $m_2(a)$ for a sequence a in row i can be found in row $i + 1$, due to Property 7.

Remarks 8 The reason the cases $m = 3$ and $m = 5$ need to be excluded from Theorem 6 is that there are no periodic sequences in these two cases with $6 = \mathrm{ord}(2, 3) \cdot 3$, respectively $20 = \mathrm{ord}(2, 5) \cdot 5$ different images. However, for $m = 7$ there are such sequences, but the uniform sequence c given does not work in that case. The sequence $(1100000)^\omega$, for example, does have $\mathrm{ord}(2, 7) \cdot 7 = 21$ distinct images under the action of the group.

The upper bound $(m - 1)m$ in Theorem 6 can only be attained for prime values of m. Conjecturally, this happens for infinitely many primes, namely for the primes m for which 2 is a primitive root modulo m. The Artin conjecture states that this occurs infinitely often (and this is proven under assumption of a generalized Riemann hypothesis).

A similar proof works for period $(11010^{m-4})^\omega$ and for $(111010^{m-5})^\omega$ and several other cases.

Note also that for a larger output alphabet Σ_k (with $k > 2$) Theorem 5 also holds, and since the sequence c can also be represented as one defined over Σ_k, Theorem 6 also holds. In fact, it is easy in the case of larger output alphabet to show that the upper bound given will also be attained for certain sequences that are 3-, 5- or 7-periodic.

Theorem 9. *Let $m = 2^r s$ with $s > 7$ odd, and let a be an m-periodic binary sequence; then $|K_2(a)| \leq \mathrm{ord}(2, s) \cdot m + 2^r - 1$.*

Proof. We will assume that $r \geq 1$, as Theorem 6 dealt with the case $r = 0$. Note that the semigroup S is now not a group, and the operations odd and even will not be invertible. Also, for $a \in P_m$ we find that $\mathsf{odd}(a), \mathsf{even}(a) \in P_{\frac{m}{2}}$, so the images will be $\frac{m}{2}$-periodic. But this means that we can prove the result recursively! □

Remarks 10 It is no longer generally true that the upper bound in Theorem 9 can always be attained: for large r there may not be sufficiently many distinct elements in P_s.

A general strategy to create an element of $P_{2^r s}$ with maximal kernel size, is to start with 2^r 'different' elements of P_s and to use the zip operation repeatedly to create a single element of $P_{2^r s}$. The elements of P_s have to be sufficiently different to prevent any collisions under the action of S.

Example 11 Let a, b, c, d be the four 9-periodic binary sequences

$$a = (110100000)^\omega, b = (111010000)^\omega, c = (111101000)^\omega, d = (111110100)^\omega$$

from P_9; each of these have the maximum size 54 for the orbit under S, much like that in Example 7. Moreover, the weights of the periods of these sequences, as of all those in their orbits, are $3, 4, 5, 6$, respectively, which implies that all four orbits are disjoint. As a consequence, the orbits of the sequences $\mathsf{zip}(a, b)$ and $\mathsf{zip}(c, d)$ in P_{18} contain the maximum of 108 elements, and the orbit of $z = \mathsf{zip}(\mathsf{zip}(a, b), \mathsf{zip}(c, d))$ contains 218 different elements, namely the previous orbits as well as $\mathsf{zip}(a, b)$ and $\mathsf{zip}(c, d)$ themselves. Together with z itself this gives the maximum number of 219 elements in the kernel of z.

Here is a preliminary version of the accompanying result for a lower bound.

Conjecture 12 *Let $m = 2^r s$ with s odd, and let a be an m-periodic binary sequence; then $r + s + e \leq |K_2(a)|$, where $e = 1$ if $s = 1$, and $e = 0$ otherwise.*

Remarks 13 In this case only a few values in the range will be attained by $|K_2(a)|$.

It is not difficult to generalize Theorem 1, and Theorem 5 to the case of k-automatic sequences, $k \geq 2$, when m is coprime to k. In that case S is a group again, which is generated by tail and m_k, and $\mathrm{ord}(2, m)$ should be replaced by $\mathrm{ord}(k, m)$. Also Theorem 9 generalizes, with $m = k^r \cdot s$, for s coprime to k, and upper bound $\mathrm{ord}(k, s) \cdot m + k^r - 1$.

References

1. J.-P. Allouche and J. Shallit. *Automatic Sequences: Theory, Applications, Generalizations*. Cambridge University Press, 2003.
2. Hans Zantema. Complexity of automatic sequences. *submitted*, 2019.