Algebra and Discrete Mathematics
Volume **25** (2018). Number 2, pp. 303–310 RESEARCH ARTICLE
© Journal "Algebra and Discrete Mathematics"

The growth function of the adding machine

Volodymyr Skochko

Communicated by R. Grigorchuk

Abstract. We compute the growth function of the generalized adding machine and show that its generating function is not algebraic.

Introduction

Abstract automata are mathematical models of machines and computational processes. There are many classes of automata, and in this paper we consider (initial) automata-transducers, which generate an output string depending on an input string. Therefore, automata-transducers generate transformations of words over alphabet. The standard question is how to realize a given transformation by an automaton, and what is the minimal number of states required for such implementation.

Another problem is to find for a given automaton transformation f the minimal number of states required to implement composition $f^{(n)} = f \circ f \circ \ldots \circ f$ (n times). In order to solve this problem we have to understand the behavior of the growth function $\gamma_A(n)$ of an (initial) automaton A, which counts the number of states in the n-th iteration of A after its minimization. Note that here we should deal with automata with fixed initial state, while the theory of automaton groups deals with groups generated by all transformations obtained by changing the initial state

The author would like to thank his advisor Ievgen Bondarenko for his help, guidance and time spent during discussions and corrections of this article.
2010 MSC: 20M35, 68Q70.
Key words and phrases: automaton, growth function, adding machine.

of a given automaton. In this case, the growth function of an automaton counts the number of different elements of length n in the semigroup generated by this automaton. We have a connection with growth of groups which has essential influence in both group theory and automata theory. The most spectacular example is the automaton group of Grigorchuk [7], which was the first example of a group of intermediate growth between polynomial and exponential. Later, Bartholdi, Reznykov, and Sushchansky constructed the smallest automaton with intermediate growth function [1] and many examples of automata with polynomial growth of irrational degree [2]. The growth function of automata plays important role in decision problems around automaton group: see [3, 4] for applications to the word problem and [5] for the order and conjugacy problems.

In this paper we consider the growth function of initial automata, namely, the generalized adding machine. The standard adding machine (odometer) realizes addition of one to binary numbers. Therefore, its growth function $\gamma(n)$ counts the minimal number of states required to realize an automaton that adds n to binary numbers. We consider a generalized version of the adding machine and give an exact formula for its growth function. As a corollary, we obtain that the generating function of the growth function is algebraic only in the trivial cases.

1. Automata and their growth functions

Definition 1. An *automaton* A is a tuple (X, S, λ), where X is a finite set (alphabet) with at least two elements, S is the set of states, and $\lambda : S \times X \to X \times S$ is the output-transition map.

An automaton $A = (X, S, \lambda)$ is usually identified with the directed labeled graph with the vertex set S, where an arrow $s \to t$ with label $x|y$ exists if and only if $\lambda(s, x) = (y, t)$. We say that a state t is *reachable* from a state s if there is a directed path in A from s to t. If the labels $x_1|y_1$, $x_2|y_2$,$\dots$ $x_n|y_n$ are read along this path, then we use notation $t = s|_{x_1 x_2 \dots x_n}$. We also say that t is a (sub)state of s at the n-th level.

The *composition* of automata $A = (X, S_1, \lambda_1)$ and $B = (X, S_2, \lambda_2)$ is the automaton $A \circ B = (X, S_1 \times S_2, \lambda_3)$, where λ_3 is defined as follows. Let we have denoted $\lambda_2(s_2, x) = (z, t_2)$, $\lambda_1(s_1, z) = (y, t_1)$ then

$$\lambda_3((s_1, s_2), x) = (y, (t_1, t_2)).$$

Definition 2. An automaton A with fixed state $s \in S$ is called *initial* and is denoted by A_s.

Every initial automaton A_s defines a transformation of the space X^* of all finite words over X. The output $A_s(x_1x_2\ldots x_n)$ is defined recursively as follows:

$$A_s(x_1x_2\ldots x_n) = y_1y_2\ldots y_n$$

if $\lambda(s, x_1) = (y_1, t)$ and $A_t(x_2\ldots x_n) = y_2\ldots y_n$. Informally speaking, the initial automaton reads the input word letter by letter, generates an output letter depending on the current state, and changes its current state according to the transition map. Note that the terminal state of A_s after processing a word $x_1x_2\ldots x_n$ is $s|_{x_1x_2\ldots x_n}$.

The composition of two initial automata A_s and B_t over the alphabet X is the initial automaton $(A\circ B)_{(s,t)}$. It is easy to see that the composition of automata agrees with the composition of transformations:

$$(A_s \circ B_t)(x_1x_2\ldots x_n) = (A\circ B)_{(s,t)}(x_1x_2\ldots x_n) \text{ for all } x_i \in X,\ n\in\mathbb{N}.$$

Different states of an automaton may define the same transformation of X^*. The following concept eliminates this difficulty.

Definition 3. Two automata A and B over the same alphabet X are called equivalent if for every state s of A there exists a state t of B such that the transformations defined by A_s and B_t are equal, and vise versa.

The minimal automaton $\mathrm{Min}(A)$ is an automaton equivalent to A with the property that different states define different transformations.

For an initial automaton A_s, its minimal automaton $\mathrm{Min}(A_s)$ is a subautomaton of $\mathrm{Min}(A)$ with initial state t, where A_s and $\mathrm{Min}(A)_t$ define the same transformation, and every state of $\mathrm{Min}(A_s)$ is reachable from t.

Note that for finite automata the minimal automaton $\mathrm{Min}(A)$ has the least number of states required to realize all transformations defined by the states of an automaton A. The automaton $\mathrm{Min}(A_s)$ has the least number of states required to realize the transformation A_s.

Definition 4. The growth function of an initial automaton A_s is defined as the function which counts the number of states in the minimized n-th power of A_s, e.g.

$$\gamma_{A_s}(n) = \gamma_s(n) = \#\,\mathrm{States}(\mathrm{Min}(A_s^{(n)})),\ n\in\mathbb{N},$$

where $A_s^{(n)} = A_s\circ\ldots\circ A_s$ (n times).

In other words, if we take the automaton $\mathrm{Min}(A^{(n)})$ and its state $s^n = (s, \dots, s)$ (n times), which corresponds to n-th time iteration of A_s, then the growth function $\gamma_{A_s}(n)$ counts the number of all states $s^n|_v$ for $v \in X^*$ in $\mathrm{Min}(A^{(n)})$.

One of the classical examples of automata is the adding machine.

Definition 5. The *adding machine on d digits* is the initial automaton over the alphabet $X = \{0, 1, \dots, d-1\}$ with two states $S = \{e, a\}$, initial state a, where the output-transition map is defined by

$$\lambda(e, x) = (x, e) \quad \text{for all } x \in X,$$
$$\lambda(a, x) = \begin{cases} (0, a) & \text{if } x = d-1, \\ (x+1, e) & \text{otherwise.} \end{cases}$$

We denote the adding machine by its initial state a.

The state e defines the trivial transformation, while the transformation defined by the state a corresponds to the addition of 1 in the position numeral system with base d. In other words $a(x_1 x_2 \dots x_n) = y_1 y_2 \dots y_n$ if and only if

$$1 + x_1 + x_2 d + \dots + x_n d^{n-1} \equiv y_1 + y_2 d + \dots + y_n d^{n-1} \bmod d^n$$

for all $n \in \mathbb{N}$. Hence, the growth function $\gamma_a(n)$ gives us the minimal number of states required to construct the automaton that realizes the addition of n to numbers written in base d.

In this paper we consider the following generalization of the adding machine.

Definition 6. For every permutation π on the alphabet $X = \{0, \dots, d-1\}$ the *generalized adding machine* is defined as the initial automaton over X with two states $S = \{e, a_\pi\}$ and initial state a_π, where the output-transition map is defined by

$$\lambda(e, x) = (x, e) \quad \text{for all } x \in X,$$
$$\lambda(a_\pi, x) = \begin{cases} (\pi(d-1), a_\pi) & \text{if } x = d-1, \\ (\pi(x), e) & \text{otherwise.} \end{cases}$$

2. Main results

First we compute the growth function of the standard adding machine.

Theorem 1. *The growth function $\gamma(n)$ of the adding machine a on d digits can be computed as follows. Let $n = \varepsilon_0 + \varepsilon_1 d + \ldots + \varepsilon_m d^m$ be the expansion of n in base d and p be the first non-zero position.*

1) *If $d > 2$ then*

$$\gamma(n) = \begin{cases} 2m - p + 2 & \text{if } \varepsilon_m = 1, \\ 2m - p + 3 & \text{otherwise.} \end{cases}$$

2) *If $d = 2$ then*

$$\gamma(n) = \begin{cases} 2m - p + 2 & \text{if } \varepsilon_{m-1} = 1 \text{ or } p = m, \\ 2m - p + 1 & \text{otherwise.} \end{cases}$$

Proof. Each state of a^n is of the form a^i for some $0 \leqslant i \leqslant n$, and since the adding machine has infinite order, $a^i = a^j$ only when $i = j$. Let $A(n)$ be the set of all nonnegative integers i such that a^i is a state of a^n. Then $\gamma(n)$ counts the number of elements in $A(n)$. We show how to construct $A(n)$ iteratively and then conclude the result.

Let us divide n by d with reminder: $n = dq + r$, $0 \leqslant r < d$. Then the states of a^n on the first level are

$$a^n|_x = \begin{cases} a^{q+1} & \text{for } x = 0, \ldots, r-1, \\ a^q & \text{for } x = r, \ldots, d-1. \end{cases} \tag{1}$$

Notice that $q < q + 1 < n$ for all n and d, except for $n = d = 2$ when $q + 1 = n$. The above rule suggests an iterative construction of the set $A(n)$. Let $A_k(n)$ consists of all integers i such that $a^n|_v = a^i$ for some word $v \in X^k$; we have $A(n) = \cup_{k \geqslant 0} A_k(n)$. The equation (1) tells us that one can construct $A_{k+1}(n)$ from $A_k(n)$ as follows: for every number $y \in A_k(n)$, if d divides y, then put $\left[\frac{y}{d}\right]$ into $A_{k+1}(n)$; otherwise put two numbers $\left[\frac{y}{d}\right]$ and $\left[\frac{y}{d}\right] + 1$. Since each time we divide by d, it is direct to get the following properties of $A_k(n)$ by induction:

1) $A_k(n) = \left\{\left[\frac{n}{d^k}\right]\right\}$ for $k = 0, 1, \ldots, p$;
2) $A_k(n) = \left\{\left[\frac{n}{d^k}\right], \left[\frac{n}{d^k}\right] + 1\right\}$ for $k = p + 1, \ldots, m - 1$;
3) $A_k(n)$ are disjoint for $k = 0, 1, \ldots, m - 1$;
4) $A(n) = A_0(n) \cup A_1(n) \cup \ldots \cup A_{m+1}(n)$;

The last two sets in the union may have non-empty intersection and must be considered more carefully.

5) If $p = m$ then in this case $n = \varepsilon_m d^m$ and $\varepsilon_m \neq 0$. So we get $A_k(n) = \{\varepsilon_m d^{m-k}\}$ for $k = 0, 1, \ldots, m$ and $A_{m+1}(n) = \{0, 1\}$. Therefore, $A_m(n) \cup A_{m+1}(n) = \{0, 1, \varepsilon_m\}$ and its cardinality is equal to 2 or 3 depending on whether ε_m is equal to 1 or not.

6) If $p \leqslant m-1$ and $d > 2$, then

$$A_m(n) \cup A_{m+1}(n) = \{0, 1, \varepsilon_m, \varepsilon_m + 1\}$$

and this set is disjoint with $A_k(n)$ for $k < m$ (note that the cardinality of the union is 3 or 4 depending on whether ε_m is equal to 1 or not).

Indeed, in this case

$$A_{m-1}(n) = \begin{cases} \{[\frac{n}{d^{m-1}}]\} & \text{if } p = m-1, \\ \{[\frac{n}{d^{m-1}}], [\frac{n}{d^{m-1}}] + 1\} & \text{if } p < m-1. \end{cases}$$

and $\left[\frac{n}{d^{m-1}}\right] > \left[\frac{n}{d^m}\right] + 1$.

Therefore, $A_m(n) = \{[\frac{n}{d^m}], [\frac{n}{d^m}] + 1\} = \{\varepsilon_m, \varepsilon_m + 1\}$ and it is disjoint with $A_k(n)$ for $k < m$. But $1 \leqslant \varepsilon_m < \varepsilon_m + 1 \leqslant d$. Hence, $A_{m+1}(n) = \{0, 1\}$ by construction and we get $A_m(n) \cup A_{m+1}(n) = \{0, 1, \varepsilon_m, \varepsilon_m + 1\}$.

7) If $p \leqslant m-1$ and $d = 2$, then $A_m(n) \cup A_{m+1}(n) = \{0, 1, 2\}$. However, this set may have a non-empty intersection with $A_{m-1}(n)$; this happens exactly in the case $\varepsilon_{m-1} = 0$ when $2 \in A_{m-1}(n)$.

In this case $\varepsilon_m = 1$ and $[\frac{n}{2^{m-1}}] = 2\varepsilon_m + \varepsilon_{m-1} = 2 + \varepsilon_{m-1}$. Therefore,

$$A_{m-1}(n) = \begin{cases} \{3\} & \text{if } p = m-1, \\ \{3, 4\} & \text{if } \varepsilon_{m-1} = 1,\ p \neq m-1, \\ \{2, 3\} & \text{otherwise.} \end{cases}$$

In any case we have $A_m(n) = \{1, 2\}$ and $A_{m+1}(n) = \{0, 1\}$. So we get that $A_m(n) \cup A_{m+1}(n) = \{0, 1, 2\}$.

The value of the growth function $\gamma(n)$ immediately follows from items 1)-7). □

Corollary 1. *Let a_π be the generalized adding machine on d digits with $\pi \in \mathrm{Sym}(X)$.*

1) If $\pi(d-1) = d-1$, then a_π has finite order $|a_\pi| = |\pi|$ and its growth function is periodic.

2) If $\pi(d-1) \neq d-1$, then $\gamma_{a_\pi}(n)$ coincides with the growth function of the standard adding machine on l digits, where l is the length of the orbit of $d-1$ under π. More precisely, let $n = \varepsilon_0 + \varepsilon_1 l + \ldots + \varepsilon_m l^m$ be the expansion in base l of n and p be the first non-zero position. Then

(a) *if $l > 2$ then*

$$\gamma_{a_\pi}(n) = \begin{cases} 2m - p + 2 & \text{if } \varepsilon_m = 1, \\ 2m - p + 3 & \text{otherwise.} \end{cases}$$

(b) *if* $l = 2$ *then*

$$\gamma_{a_\pi}(n) = \begin{cases} 2m - p + 2 & \textit{if } \varepsilon_{m-1} = 1 \textit{ or } p{=}m, \\ 2m - p + 1 & \textit{otherwise.} \end{cases}$$

Proof. 1) If $\pi(d-1) = d-1$, then a_π changes only the first letter not equal to $d-1$ by π. Hence, $a_\pi^k = e$, where k is the order of π.

2) Without loss of generality we can suppose that the orbit of $d-1$ under π corresponds to the cycle $\tau = (d-l, \dots, d-1)$. Then the subtree $\{d-l, \dots, d-1\}^*$ of X^* is invariant under the action of a_π and the restricted action is exactly the standard adding machine on l letters. Therefore, a_π^n has the same states at words from $\{d-l, \dots, d-1\}^*$ as the standard adding machine. For a word v not in $\{d-l, \dots, d-1\}^*$ (here v contains a letter $x \notin \{d-l, \dots, d-1\}$), we have $a_\pi^n|_v = e$. The statement follows. □

Corollary 2. *The growth function of the generalized adding machine* a_π *on* d *digits for* $\pi(d-1) \neq d-1$ *satisfies*

$$\left[\frac{\log n}{\log l}\right] + 2 \leqslant \gamma(n) \leqslant 2\left[\frac{\log n}{\log l}\right] + c_d \textit{for all } n \geqslant 1,$$

where $c_d = 2$ *for* $d = 2$ *and* $c_d = 3$ *for* $d > 2$. *Moreover, the lower and the upper bounds are reached for infinitely many values of* n.

Let us recall that the *generating function* of a function $\gamma : \mathbb{N} \cup \{0\} \to \mathbb{N}$ is the formal power series $\Gamma(t) = \sum_{n \geqslant 0} \gamma(n) t^n$. A formal power series is called *algebraic* if it is algebraic over the field of rational functions.

Corollary 3. *Let* a_π *be the generalized adding machine on* d *digits. The generating function of* $\gamma_{a_\pi}(n)$ *is algebraic if and only if* $\pi(d-1) = d-1$*; moreover, in this case the generating function is rational.*

Proof. If $\pi(d-1) = d-1$, then the growth function of a_π is periodic and its generating function is rational.

The coefficients of an algebraic power series $\sum_{n \geqslant 0} c_n t^n$ have asymptotic of the type $c_n \sim C n^\alpha A^n$ (see theorem VII.8 in [6]) and cannot be of logarithmic growth as in Corollary 2. □

Corollary 4. *The growth function of the standard adding machine has non-algebraic generating function.*

References

[1] L. Bartholdi, I. I. Reznykov, V. I. Sushchansky, *The smallest Mealy automaton of intermediate growth*, J. Algebra 295 (2006), no. 2, 387–414.

[2] L. Bartholdi, I. I. Reznykov, *A Mealy machine with polynomial growth of irrational degree*, Internat. J. Algebra Comput. 18 (2008), no. 1, 59–82.

[3] I. Bondarenko, *Growth of Schreier graphs of automaton groups*, Mathematische Annalen 354 (2012), no. 2, 765–785.

[4] I. Bondarenko, *The word problem in Hanoi Towers groups*, Algebra and Discrete Mathematics 17 (2014), no. 2, 248–255.

[5] I. Bondarenko, N.Bondarenko, S.Sidki, F.Zapata, *On the conjugacy problem for finite-state automorphisms of regular rooted trees* (with an appendix by Raphael M. Jungers), Groups, Geometry, and Dynamics 7 (2013), no. 2, 323–355.

[6] Ph. Flajolet, R. Sedgewick, *Analytic combinatorics*, Cambridge University Press, 2009.

[7] R. I. Grigorchuk, *On the Milnor problem of group growth*, Dokl. Akad. Nauk SSSR 271 (1983), no. 1, 30-33.

[8] R.I. Grigorchuk, V.V. Nekrashevych, V.I. Sushchansky, Automata, dynamical systems and groups, *Proceedings of the Steklov Institute of Mathematics* **231** (2000), 128–203.

Contact information

V. Skochko

Department of Mechanics and Mathematics,
Kyiv National Taras Shevchenko Univ.,
Volodymyrska str., 64, 01033 Kyiv, Ukraine
E-Mail(s): vovaskochko@gmail.com

Received by the editors: 22.10.2016
and in final form 27.11.2016.