#A31 INTEGERS 11 (2011)

COMPLETELY MULTIPLICATIVE AUTOMATIC FUNCTIONS

Jan-Christoph Schlage-Puchta
Department of Mathematics, Universiteit Gent, Gent, Belgium
jcsp@cage.ugent.be

Received: 3/11/10, Accepted: 1/16/11, Published: 5/18/11

Abstract

We show that a completely multiplicative automatic function, which does not have 0 as a value, is almost periodic.

1. Introduction and Results

A finite automaton consists of a finite set of states with a specified starting state s_0, an input alphabet $\mathcal{A}$, an output alphabet $\mathcal{B}$, and two functions $f : \mathcal{A} \times \mathcal{S} \to \mathcal{S}$, $g : \mathcal{S} \to \mathcal{B}$. Given a word w over $\mathcal{A}$, the output of the automaton is determined as follows. At first, the automaton is in s_0. Then the first letter a of w is read, and the new state of the automaton is changed to $s_1 = f(a, s_0)$. Then the next letter b of w is read, and the state of the automaton is changed to $s_2 = f(b, s_1)$. This is repeated untill all letters of w are read, and the procedure terminates. If the automaton ends in the state s, it returns the value $g(s)$.

Fix some integer $q \geq 2$. In our context, the alphabet $\mathcal{A}$ consists of the integers $0, 1, \dots, q-1$, and $\mathcal{B}$ consists of complex numbers. Every integer $n \geq 1$ can be written in the form $n = \sum e_i(n)q^i$ with $e_i(n) \in \{0, 1, \dots, q-1\}$, hence n can be viewed as a word over $\mathcal{A}$, and the automaton can be applied to this word. More precisely, write $n = \sum_{i=0}^{k} e_i q^i$ with $e_i \in \{0, 1, \dots, q-1\}$ and $e_k \neq 0$, and identify the integer n with the string $e_k e_{k-1} \dots e_1 e_0$. In this way, every automaton defines a sequence $(a_n)_{n\geq 0}$. A sequence is called automatic if there exists an integer q and a finite automaton, which defines this sequence.

Apart from its relation to computer science, the importance of automatic sequences stems from their natural interactions with many fields of mathematics, including algebra, dynamical systems, and in particular with number theory. For an overview of applications we refer the reader to [1].

A function $f : \mathbb{N} \to \mathbb{C}$ is called completely multiplicative if $f(nm) = f(n)f(m)$ holds true for all $n, m \in \mathbb{N}$. The question of which multiplicative functions are automatic has been dealt with by several authors, both for concrete examples (see,

e.g., [6], [5], [2]) and for classes of functions (see, e.g., [10] and [4]).

In the last two articles mentioned the set of integers n with $f(n) = 0$ played a crucial role, and therefore the condition that there are sufficiently many prime powers q for which $f(q) = 0$ comes in naturally. If f does not vanish, these approaches fail. The local behavior of multiplicative functions that do not vanish; that is, the question of how, for a fixed k, the set of patterns $\{(f(n), f(n+1), \dots, f(n+k) : n \in \mathbb{N}\}$ looks, appears to be completely mysterious. However, Ramsey theory implies that there is no total chaos; that is, no matter how difficult something looks, there is always a small region of order. It is the strategy of the present paper to exploit these small regions. We will prove the following.

Proposition 1 *Let $q \geq 2$ be an integer, and f be a completely multiplicative q-automatic function, which does not vanish. Then there exists an integer k, such that if n_1, n_2, ℓ are integers such that $(n_1, q^{\ell+1})|q^{\ell}$, and $n_1 \equiv n_2 \pmod{q^{k+\ell}}$, then $f(n_1) = f(n_2)$.*

Theorem 2 *Let f be a completely multiplicative automatic function, which does not vanish. Then f is almost periodic.*

Here a function is called almost periodic if there exists a sequence of periodic functions (f_i), such that the upper density of the set $\{n : f(n) \neq f_i(n)\}$ tends to 0 as i tends to ∞.

2. Some Lemmas

For the proof of the theorem we need the following two famous statements. The first is van der Waerden's theorem (see [8] for van der Waerden's proof or, for a more accessible proof, see [7]), the second the Wirsing-Halasz-Theorem (see [9], [3]).

Theorem 3 *Let N be an integer, S a finite set, $\chi : \mathbb{N} \to S$ a coloring. Then there exist a monochromatic arithmetic progression of length N, that is, there are integers a, D, such that $\chi(a) = \chi(a + D) = \chi(a + 2D) = \cdots = \chi(a + DN)$.*

For a function $f : \mathbb{N} \to \mathbb{C}$ we say that it has mean value $M(f)$, if the limit

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} f(n) = M(f)$$

exists.

Theorem 4 *Let f be a complex-valued multiplicative function such that $|f(n)| \leq 1$ for all n. Then there exists a real number t such that $n \mapsto n^{it} f(n)$ has a mean value. If for all $t \in \mathbb{R}$ the series $\sum_p \frac{\Re(1-p^{it} f(p))}{p}$ diverges, then the mean value of*

$n^{it}f(n)$ is 0 for all real t. If this series converges for some t, than for this t the mean value exists and is not zero.

The following simple observation is quite useful.

Lemma 5 *Let f be a completely multiplicative function, which takes only finitely many different values. Then each value of f is either 0 or a root of unity.*

Proof. Consider the sequence $f(n), f(n^2), f(n^3), \ldots$. Since f takes only finitely many different values, there must be indices $i \neq j$ with $f(n^i) = f(n^j)$. By complete multiplicativity this means $f(n)^i = f(n)^j$; hence, either $f(n) = 0$, or $f(n)^{j-i} = 1$. In both cases our claim follows. □

Lemma 6 *Let f be a completely multiplicative function which takes only finitely many different values. Then the restriction of f to any residue class has a mean value, that is, for each m and a the limit*

$$M(m,a) := \lim_{x\to\infty} \frac{m}{x} \sum_{\substack{n\leq x \\ n\equiv a \pmod m}} f(n)$$

exists. If there exist integers m, a, such that $|M(m,a) = 1|$, then we have $f(n) = 1$ for all $n \equiv 1 \pmod m$.

Proof. If f is completely multiplicative and takes only finitely many values, then all values of f are 0 or roots of unity. Hence, $|f(n)| \leq 1$ for all n, and we can apply the Wirsing-Halász theorem (Theorem 4) to find that there exists some t such that $n^{it}f(n)$ has a mean value. We claim that f itself has a mean value. To prove the claim, it suffices to show that $\sum_p \frac{\Re(1-p^{it}f(p))}{p}$ diverges for every $t \neq 0$. Let $t \neq 0$ be fixed, $R \subseteq \mathbb{C}$ be the range of f, and let $\epsilon > 0$ be small enough that $\bigcup_{z\in R} B_\epsilon(z)$ covers at most half of the boundary of the unit circle. Then from the prime number theorem it follows that $1 - p^{it}f(p) > \epsilon$ for a set of primes of positive relative lower density. Since $|f(p)| \in \{0, 1\}$, this implies that $\Re(1 - p^{it}f(p)) > \frac{\epsilon^2}{3}$, and hence, $\sum_p \frac{\Re(1-p^{it}f(p))}{p}$ diverges. Replacing f by χf for a Dirichlet-character χ, and taking linear combinations, we find that $M(m,a)$ exists whenever m and a are coprime. If $(a,m) = d$, we can use complete multiplicativity to see that $M(m,a)$ exists and equals $f(d)M(m/d, ad^{-1})$. Hence, in any case $M(m,a)$ exists.

Now suppose that $|M(m,a)| = 1$ for some integers m, a. Since f takes only finitely many values, and all values are in the unit circle, this implies that $f(n) = M(m,a)$ holds true for all $n \equiv a \pmod m$ with the possible exception of a set of density 0. Now let n_1 be an integer congruent to 1 modulo m, and suppose that $f(n_1) \neq 1$. Then for every integer $n \equiv a \pmod m$ we have that one of $f(n)$, $f(nn_1)$ is different from $M(m,a)$, while both n and nn_1 are congruent to 1 modulo m. Hence, the number of integers $n \leq x$ in the arithmetic progression $a \pmod m$

which do not satisfy $f(n) = M(m, a)$ is at least $\frac{x}{m(n_1+1)}$, contradicting the fact that $f(n) = M(m, a)$ holds true for almost all n congruent to a modulo m. Hence, no such n_1 exists, and we conclude that $f(n) = 1$ for all $n \equiv 1 \pmod{m}$. □

The following is probably folklore.

Lemma 7 *Let $\ell_1 \leq \cdots \leq \ell_m \in \mathbb{N}$ be positive integers, and $G \subseteq \mathbb{N}$ be the additive semigroup generated by these integers. If $n \geq \ell_1 \cdot \ell_m$, then $y \in G$ if and only if the greatest common divisor of $\ell_1, \ldots, \ell_m$ divides n.*

Proof. Necessity is clear. Let R_k be the set of residue classes modulo ℓ_1, which can be represented as $x_2\ell_2 + \cdots + x_m\ell_m$ with $x_i \geq 0$, $x_2 + \cdots + x_m \leq k$. The sequence $R_1 \subseteq R_2 \subseteq \ldots$ is strictly increasing until at some point it becomes stable. Since there are only ℓ_1 residue classes, this sequence has to stabilize after at most ℓ_1 steps, and we obtain $R_{\ell_1} + \ell_i = R_{\ell_i}$ for $i = 2, \ldots, m$. Choose $r_1, r_2 \in \mathbb{R}_{\ell_1}$. Then we can write $r_1 = \sum_{i=2}^{m} x_i\ell_i$, and obtain

$$r_1 + r_2 = r_2 + \underbrace{\ell_2 + \cdots + \ell_2}_{x_2} + \cdots + \underbrace{\ell_m + \cdots + \ell_m}_{x_m}$$
$$\in (\ldots(R_{\ell_1} \underbrace{+\ell_2) + \cdots + \ell_2)}_{x_2} + \ldots \underbrace{+\ell_m) + \cdots + \ell_m)}_{x_m} = R_{\ell_1}.$$

Hence, R_{ℓ_1} is the subgroup of the additive group of $\mathbb{Z}/\ell_1\mathbb{Z}$ generated by $\ell_2, \ell_3, \ldots, \ell_m$, which coincides with the subgroup generated by the greatest common divisor of $\ell_1, \ldots, \ell_m$. Hence, if $n > \ell_1\ell_m$ is an integer divisible by $(\ell_1, \ldots, \ell_m)$, then we can represent an integer $n' \equiv n \pmod{\ell_1}$, $n' \leq n$, as a non-negative linear combination using at most ℓ_1 summands, and obtain a representation of n as $n = n' + \frac{n-n'}{\ell_1}\ell_1$. □

3. Proof of the Theorem

Once we have proven Proposition 1, the theorem can be deduced as follows. Define $f_i(n) = f(n \bmod q^{k+i})$, where k is as in the proposition. Clearly, f_i is periodic, and $f_i(n) = f(n)$ unless $(n, q^i) \nmid q^i$. The upper density of integers n with the latter property tends to 0 as i tends to infinity. Hence, f is approximated by the periodic functions f_i, and therefore almost periodic.

The remainder of this section is devoted to the proof of Proposition 1.

Proof of Proposition 1. Let S be the state space of the automaton. Define a function $\chi : \mathbb{N} \to S$ by setting $\chi(n)$ to be the state the automaton is in after reading n. By van der Waerden's theorem there exist arbitrarily long χ-monochromatic arithmetic progressions. Set $N = 2q^{|S|!}$, and let a, D be integers, such that $a, a + D, a + 2D, \ldots, a + ND$ is a χ-monochromatic arithmetic progression. Then for every k

and every integer $b \in [0, q^k - 1]$ each element of the set $\{aq^k + b, (a + D)q^k + b, \ldots, (a + ND)q^k + b\}$ is mapped by f to the same element. We now choose k such that $q^k > D$, and b such that $aq^k + b \equiv 0 \pmod{D}$. Then all elements of the progression are divisible by D, and since f is completely multiplicative and does not vanish, we obtain that $\{\frac{aq^k+b}{D}, \frac{aq^k+b}{D} + q^k, \ldots, \frac{aq^k+b}{D} + Nq^k\}$ is an f-monochromatic progression with difference q^k. We write $a' := \frac{aq^k+b}{D} = uq^{k+|S|!} + vq^k + w$ where u, v, w are integers satisfying $0 \le v < q^{|S|!}$, $0 \le w < q^k$. By deleting an initial part of the arithmetic progression we may assume that $v = 0$, and in this way the length of the progression is reduced by less than $q^{|S|!}$.

Let s be the state the automaton is in after reading u, and let $X \subseteq S$ be the set of states which can be reached from s for some input string of length $|S|!$. S run of the automaton after reading some string can be described by a path in a directed graph with $|S|$ vertices. If there is a path of length $|S|!$ from s to s', then this path can be written as the union of a simple path of length ℓ_0, and disjoint minimal loops of length $\ell_1, \ldots, \ell_m$, which occur with multiplicity $x_1, \ldots, x_m$ in the path, such that $x_1\ell_1 + \cdots + x_m\ell_m = |S|! - \ell_0$ is solvable with non-negative integers x_i, and $\ell_0 + \cdots + \ell_m \le |S|$. Since $|S|!$ is divisible by every integer $\le |S|$, and therefore by the greatest common divisor d of $\ell_1, \ldots, \ell_m$, we find that ℓ_0 is divisible by d. Moreover, we have $\ell_1 \cdots \ell_m \le |S|! - \ell_0$. Hence, from Lemma 7 we conclude that the equation $x_1\ell_1 + \cdots + x_m\ell_m = y|S|! - \ell_0$ is solvable in non-negative integers x_i for every integer $y \ge 1$. Hence, every state which can be reached from s with $|S|!$ steps, can be reached with $y(|S|!)$ steps for every $y \ge 1$. Conversely, if a state can be reached with $y(|S|!)$ steps for some $y \ge 1$, then it can already be reached with $|S|!$ steps. Hence, for each y we have that the set X is equal to the set of all states reachable from s within $y(|S|!)$ steps.

For each $s' \in X$ we have that starting in s' and reading w, the automaton ends in a state which produces the value $f(a')$, since $\{a', a' + q^k, \ldots, a' + Nq^k\}$ is an f-monochromatic progression. Hence, we conclude that for every $y \ge 1$ and every integer v with $\le y(|S|!)$ digits we have $f(uq^{k+y|S|!} + vq^k + w) = f(a')$. This implies for all $y \ge 1$ that

$$\sum_{\substack{uq^{k+y|S|!} \le n < (u+1)q^{k+y|S|!} \\ n \equiv w \pmod{q^k}}} f(n) = q^{y|S|!} f(a').$$

On each fixed arithmetic progression a modulo m the function f has a mean value $M(m, a)$; in particular, we have

$$\sum_{\substack{uq^{k+y|S|!} \le n < (u+1)q^{k+y|S|!} \\ n \equiv w \pmod{q^k}}} f(n) = q^{y|S|!} M(q^k, w) + o(uq^{k+y|S|!}).$$

Since u and k are fixed, while y may tend to ∞, we can delete u and k in the error term. Hence, comparing the two expressions we conclude $M(q^k, w) = f(a')$. Since

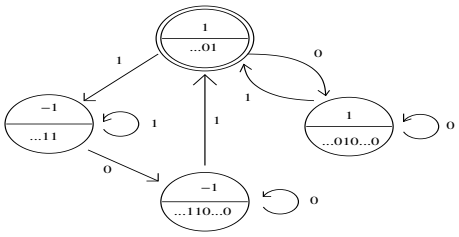

Figure 1: An automaton defining a completely multiplicative, non-vanishing function, which is not periodic. The upper number is the value returned by the automaton, the lower string describes strings leading to this state.

f takes only finitely many values, this implies that for all $n \equiv w \pmod{q^k}$ we have $f(n) = f(a')$ with the exception of a set of density 0.

Assume there exists an integer $n' \equiv 1 \pmod{q^k}$ satisying $f(n') \neq 1$. If n is an integer satisfying $n \equiv w \pmod{q^k}$, then one of $f(n)$, $f(nn')$ is different from $f(a')$. Hence, in the interval $[1, x]$ there are at least $\frac{x}{q^k n'}$ integers $n \equiv w \pmod{q^k}$ which do not satisfy $f(n) = f(a')$. But this means that the upper density of the set of integers n with $f(n) \neq f(a')$ and $n \equiv w \pmod{q^k}$ is at least $\frac{1}{n'q^k}$, which is impossible. Hence, we conclude that $f(n') = 1$ holds true for all $n' \equiv 1 \pmod{q^k}$.

Let n_1, n_2 be integers, coprime to q, and assume that $n_1 \equiv n_2 \pmod{q^k}$. Then n_1 is invertible modulo q^k, let $\overline{n_1}$ be a modular inverse. Then $n_1\overline{n_1} \equiv n_2\overline{n_2} \equiv 1 \pmod{q^k}$, hence, $f(n_1)f(\overline{n_1}) = f(n_2)f(\overline{n_1}) = 1$, and therefore $f(n_1) = f(n_2)$.

Let n_1, n_2 be integers, and assume that $n_1 \equiv n_2 \pmod{q^{k+\ell}}$, where ℓ is chosen in such a way that $(n_1, q^{\ell+1})|q^\ell$. Write $n_i = d_i t_i$, where $d_i = (n_i, q^{\ell+1})$. Then $d_1 = d_2$, and t_1, t_2 are coprime to q and congruent modulo q^k, and we obtain $f(t_1) = f(t_2)$, and therefore $f(n_1) = f(n_2)$. Hence, our claim follows in every case. □

4. An Example

Here we describe an example which shows that the parameter ℓ in Theorem 1 is really necessary. Consider an automaton over $\{0, 1\}$ that reads an integer n, deletes the last consecutive block of 0's to obtain a new integer n', and returns 1 if $n' = 1$ or the second to last digit of n' is 0, and returns -1 if the second to last digit of n' is 1. To compute this function we only have to remember whether the digit last read was 0 or 1, and, if we run through a streak of 0's, whether the two digits before were 01 or 11. Hence, one can easily construct an automaton computing this function (see Figure 1). The function computed by this automaton can be described arithmetically as dividing an integer by 2 as often as possible, and

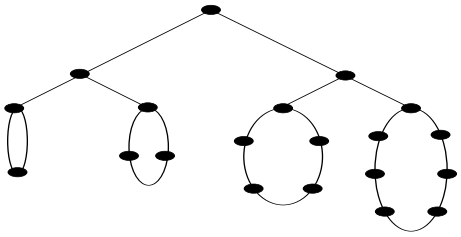

Figure 2: An automaton for which the set of states reachable within n steps determines n mod 210.

checking whether the remaining integer is 1 or 3 modulo 4. Hence, the automaton defines the completely multiplicative function f, which for a prime number p is defined as

$$f(p) = \begin{cases} 1, & p \equiv 1, 2 \pmod 4 \\ -1, & p \equiv 3 \pmod 4. \end{cases}$$

To determine $f(n)$ we have to know the digit before the last 1 in the binary expansion of n, that is, the statement of theorem 1 is optimal with $k = q = 2$. Similarly, if we put $f_i(n) = f(n \bmod 2^i)$, then $f_i(n) = f(n)$ unless n is divisible by 2^{i-2}. Hence, f is almost periodic, but it is easily seen that f is not periodic.

We next describe an automaton which shows that the set of states reachable within n steps can distinguish between many different values of n, that is, the choice of $|S|!$ is not exaggerated. We could have used the least common multiple of all integers up to n, which is $e^{(1+o(1))|S|}$, but the following example shows that we have to expect somewhat exponential behaviour. An example with 20 nodes, for which the set of states reachable within n steps determines n mod 210, is given in Figure 2.

The first part of the automaton consists of a binary tree of height k and with 2^k leaves and $2^{k+1} - 1$ nodes. Then to the ℓ-th leaf we attach a loop of length ℓ. If $n \geq k$, then a state reachable in n steps cannot be contained in the tree. In each loop there is precisely one reachable state, and the reachable state in the ℓ-th loop determines $n \pmod \ell$. Hence, the sets of states reachable within n_1 and n_2 steps coincide if and only if $n_1 \equiv n_2 \pmod \ell$ holds true for all $\ell \leq 2^k$, that is, we have to work with the least common multiple of all integers $\leq 2^k$, which is $e^{(1+o(1))2^k}$. Since the whole automaton has less than 2^{2k} states, we see that we cannot replace $|S|!$ by something smaller than $e^{(1+o(1))\sqrt{|S|}}$.

References

[1] J.-P. Allouche, J. Shallit, *Automatic Sequences*, Cambridge University Press, Cambridge, 2003.

[2] M. Coons, (Non)Automaticity of Number Theoretical Functions, *J. Théor. Nombres Bordeaux*, to appear, available via `http://arxiv.org/abs/0810.3709`

[3] G. Halász, Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen, *Acta Math. Acad. Sci. Hungar.***19** (1968) 365403.

[4] J.-C. Schlage-Puchta, A criterion for non-automaticity of sequences, *J. Integer Seq.* **6** (2003), Article 03.3.8.

[5] M. Minsky, S. Papert, Unrecognizable sets of numbers, *J. Assoc. Comput. Mach.* **13** (1966) 281–286.

[6] R. W. Ritchie, Finite automata and the set of squares, *J. Assoc. Comput. Mach.* **10** (1963) 528–531.

[7] T. Tao, V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, 105. Cambridge University Press, Cambridge, 2006

[8] B. L. van der Waerden, Beweis einer Baudetschen Vermutung, *Nieuw Arch. Wisk.* **15** (1927) 212–216

[9] E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen II, *Acta Math. Acad. Sci. Hungar.* **18** (1967) 411467.

[10] S. Yazdani, Multiplicative functions and k-automatic sequences, *J. Théor. Nombres Bordeaux* **13** (2001), 651–658.