Journal of Universal Computer Science, vol. 3, no. 10 (1997), 1085-1099
submitted: 30/3/97, accepted: 23/9/97, appeared: 28/10/97 © Springer Pub. Co.

Optimal description of automatic paperfolding sequences

Anton Černý
(Kuwait University
cerny@math-1.sci.kuniv.edu.kw)

Abstract: The class of 2-automatic paperfolding sequences corresponds to the class of ultimately periodic sequences of unfolding instructions. We first show that a paperfolding sequence is automatic iff it is 2-automatic. Then we provide families of minimal finite-state automata, minimal uniform tag sequences and minimal substitutions describing automatic paperfolding sequences, as well as a family of algebraic equations satisfied by automatic paperfolding sequences understood as formal power series.

Key Words: paperfolding sequence, automatic sequence, uniform tag system
Category: F.m, F 4.2, G 2.1

1 Introduction

Paperfolding sequences are patterns - sequences of folding edges ("peaks" and "valleys") - obtained by stepwise folding a stripe of paper. The stripe is always folded in its middle while its initial left-hand side part is kept in a fixed position. There are two different folding instructions possible: "up" – counterclockwise, and "down" – clockwise. The result of stepwise folding a stripe of paper following the sequence of instructions "up, down, down", as well as the pattern appearing on the unfolded stripe after each step, are depicted in Figure 1. The folding edges are denoted by black points, the fixed end of the stripe by a circle, the valleys are denoted by 0, the peaks by 1. The length of the folded stripe is not depicted proportionally.

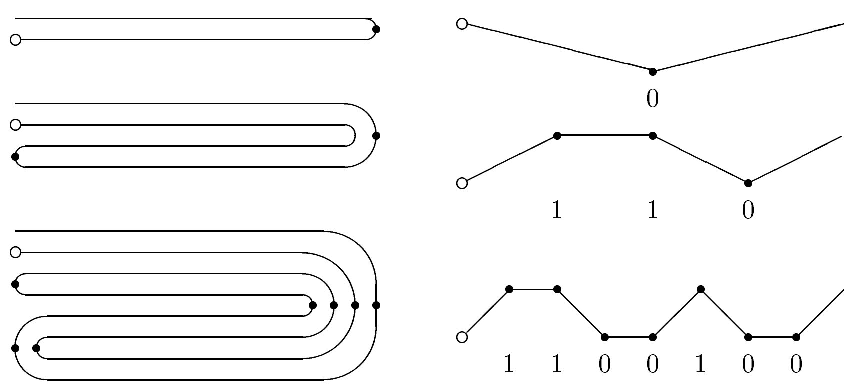

Figure 1: Figure 1: Folding up, down, and down

If we have two finite sequences of folding instructions, the first being a suffix of the second, then the first resulting pattern is a prefix of the second one. Therefore the folding instructions are usually considered in reversed order - as sequences of unfolding instructions. In the limit case an infinite sequence of unfolding instructions describes an infinite word - the paperfolding sequence.

Paperfolding sequences have been for several years a subject of investigations of many researchers (starting probably by [Davis and Knuth 70], more recently e.g. in [Allouche 92, Allouche and Bousquet-Mélou 94, Bercoff 95, Koskas 96, Lehr 92, Rodenhausen 95, Wen and Wen 92] and others). The areas of their applications include physics, number theory, harmonic analysis, fractal geometry (see e.g. [Wen and Wen 92] for references). A paperfolding sequence can be defined as a limit of a growing sequence of recurrently defined blocks, more details are provided in [Section 3]. The similarity to the description of the classical sequence of Thue-Morse ([Thue 06]) – a prototype of a 2-automatic sequence – naturally leads to the question of characterization of the subclass of automatic paperfolding sequences. In [Mendès-France and Shallit 89] the authors proved that a paperfolding sequence is 2-automatic iff the sequence of unfolding instructions is ultimately periodic. We will confirm here the intuitively expected fact that every automatic paperfolding sequence is 2-automatic. In [Bercoff 95] a family of uniform tag systems for such sequences was provided, based on the structure of Toeplitz word. We arrive here to the same family of tag systems by constructing the corresponding class of finite automata. We show that the tag systems from [Bercoff 95] are minimal, with an exception of the case when the shortest period of the unfolding sequence is a concatenation of two complementary words. Further we provide a family of minimal block-substitutions having automatic paperfolding sequences as fixed points and one possible algebraic characterization of automatic paperfolding sequences.

2 Preliminaries

2.1 Basic notions

We denote by $\mathbb{N}$, $\mathbb{Z}$ the sets of all natural numbers and of all integers, respectively. For $p \in \mathbb{N}$, we denote $\langle p\rangle = \{n \in \mathbb{N}; n < p\}$. By $i_{\langle p\rangle}$ we denote the notation in base p of $i \in \mathbb{N}$ starting by exactly two initial zeroes. The set $\langle p\rangle$ – besides being a set of numbers – will be also used as an alphabet. Together with $\langle p\rangle$ we will use the alphabets $\overline{\langle p\rangle} = \{\overline{n}; n < p\}$, $\widetilde{\langle p\rangle} = \langle p\rangle \cup \overline{\langle p\rangle}$, where we assume $\overline{\mathbb{N}} = \{\overline{n}\}_{n\in\mathbb{N}}$ to be a set consisting of pairwise different symbols, $\overline{\mathbb{N}} \cap \mathbb{N} = \emptyset$. We denote $\overline{\overline{n}} = n$.

We use the common terminology and notation from the formal languages theory, considering both finite words and one-way infinite words (sequences). In particular, the length of a finite word $\mathbf{w}$ is denoted by $|\mathbf{w}|$, the k-th power of $\mathbf{w}$ by $\mathbf{w}^k$, the sets of all finite words, words of length k, words of length being a multiple of k, and of all sequences on an alphabet Σ are denoted by Σ^*, Σ^k, $(\Sigma^k)^*$, and Σ^ω, respectively. Further we denote $\Sigma^\infty = \Sigma^* \cup \Sigma^\omega$.

The concatenation of $\mathbf{x} \in \Sigma^*$ and $\mathbf{y} \in \Sigma^\infty$ is the word $\mathbf{xy} \in \Sigma^\infty$. If $\mathbf{w} = \mathbf{xyz} \in \Sigma^\infty$, then $\mathbf{x}$ is a (*proper* if $|\mathbf{yz}| \geq \mathbf{1}$) *prefix*, $\mathbf{y}$ is a *factor*, and $\mathbf{z}$ is a *suffix* of $\mathbf{w}$. The symbol of $\mathbf{w}$ at the position i (the positions are numbered starting from 0) is denoted as $\mathbf{w}_i$, the factor $\mathbf{w}_i ... \mathbf{w}_{i+j-1}$ as $[\mathbf{w}]_i^j$. For a sequence of finite words $\{\mathbf{w}^{(k)}\}_{k=0}^{\infty}$, each $\mathbf{w}^{(k)}$ being a proper prefix of $\mathbf{w}^{(k+1)}$, the unique sequence having each $\mathbf{w}^{(k)}$ as a prefix will be denoted as $\lim\limits_{k\to\infty} \mathbf{w}^{(k)}$. In particular, for a finite non-empty word $\mathbf{w}$ we denote $\mathbf{w}^{\omega} = \lim\limits_{k\to\infty} \mathbf{w}^{k}$.

A sequence $\mathbf{s} \in \Sigma^{\omega}$ is *ultimately periodic* if $\mathbf{s} = \mathbf{x}\mathbf{y}^{\omega}$ for some words $\mathbf{x}, \mathbf{y} \in \Sigma^{\omega}$. The words $\mathbf{x}, \mathbf{y}$ are then called the *pre-period* and the *period* of $\mathbf{s}$, respectively. Some well-known properties of ultimately periodic sequences are summarized in Proposition 1. The unique decomposition described in part (iii) will be called *minimal.*

Proposition 1. *Let* $\mathbf{s}$ *be an ultimately periodic sequence.*
(i) If $\mathbf{s} = \mathbf{x}_1\mathbf{y}_1^{\omega}$ *then, for each pair of numbers* $m, n \in \mathbb{N}$ *such that* $m \geq |\mathbf{x}_1|$ *and* n *is a multiple of* $|\mathbf{y}_1|$*,* $\mathbf{s}$ *can be decomposed as* $\mathbf{s} = \mathbf{x}_2\mathbf{y}_2^{\omega}$ *where* $|\mathbf{x}_2| = m$ *and* $|\mathbf{y}_2| = n$.
(ii) If $\mathbf{s} = \mathbf{x}_1\mathbf{y}_1^{\omega}$ *and* $\mathbf{s} = \mathbf{x}_2\mathbf{y}_2^{\omega}$ *then* $\mathbf{s}$ *can be decomposed as* $\mathbf{s} = \mathbf{x}_3\mathbf{y}_3^{\omega}$ *where* $|\mathbf{y}_3| = \gcd(|\mathbf{y}_1|, |\mathbf{y}_2|)$.
(iii) There are unique words $\mathbf{x}$ *and* $\mathbf{y}$ *such that* $\mathbf{s} = \mathbf{x}\mathbf{y}^{\omega}$ *and if* $\mathbf{s} = \mathbf{x}_1\mathbf{y}_1^{\omega}$ *then* $|\mathbf{x}| \leq |\mathbf{x}_1|$ *and* $|\mathbf{y}| \leq |\mathbf{y}_1|$.

From (iii) and (i) we obtain the following Corollary 2 describing another unique decomposition of an ultimately periodic sequence - we will refer to it as *1-minimal decomposition.*

Corollary 2. *There are unique words* $\mathbf{x}$ *and* $\mathbf{y}$ *such that* $\mathbf{s} = \mathbf{x}\mathbf{y}^{\omega}$*,* $|\mathbf{x}| \geq 1$*, and if* $\mathbf{s} = \mathbf{x}_1\mathbf{y}_1^{\omega}$ *with* $|\mathbf{x}_1| \geq 1$ *then* $|\mathbf{x}| \leq |\mathbf{x}_1|$ *and* $|\mathbf{y}| \leq |\mathbf{y}_1|$.

A *morphism* is a mapping $\varphi : \Sigma^{\infty} \to \Gamma^{\infty}$, where Σ and Γ are alphabets, such that, for $\mathbf{x} \in \Sigma^{*}$, $\mathbf{y} \in \Sigma^{\infty}$, $\varphi(\mathbf{x})$ is finite and $\varphi(\mathbf{x}\mathbf{y}) = \varphi(\mathbf{x})\varphi(\mathbf{y})$. If $\varphi(\Sigma) \subseteq \Sigma^{k}$, for some $k \geq 0$, then φ is *k-uniform.* We will use substitutions as a generalization of uniform morphisms. An (r, s)*-substitution* ([Christol et al. 80]), for $r \geq 1$, $s \geq 0$, is a partial mapping $\sigma : \Sigma^{\infty} \to \Gamma^{\infty}$ defined for all words from $(\Sigma^{r})^{*} \cup \Sigma^{\omega}$, such that, for $\mathbf{x} \in (\Sigma^{r})^{*}$and $\mathbf{y} \in (\Sigma^{r})^{*} \cup \Sigma^{\omega}$, $|\sigma(\mathbf{x})| = s(|\mathbf{x}|/r)$ and $\sigma(\mathbf{x}\mathbf{y}) = \sigma(\mathbf{x})\sigma(\mathbf{y})$. Substitutions are fully determined by their values on Σ^{r}.

A *finite-state automaton* is a tuple (S, I, δ, q_0) where S is the *state alphabet,* I is the *input alphabet,* $q_0 \in S$ is the *initial state,* and $\delta : S \times I \to S$ is the *transition function.* We will use the usual extension $\delta : S \times I^{*} \to S$, as well.

Finally, for $\mathbf{w} \in \langle 2 \rangle^{\infty}$ we denote by $\widehat{\mathbf{w}}$ the word obtained from $\mathbf{w}$ by replacing zeroes by ones and vice versa, and for $\mathbf{w} \in \widetilde{\langle p \rangle}^{\infty}$ we denote by $\overline{\mathbf{w}}$ the word obtained from $\mathbf{w}$ by replacing each occurrence of each symbol s by $\overline{s}$.

2.2 Automatic sequences

Automatic sequences are infinite sequences described by finite state automata. We will provide three other characterizations of automatic sequences, as well, and then we will state the equivalence of the four ways of characterization in Proposition 3.

Let Σ and Γ be two alphabets and $p \geq 2$.

A sequence $\mathbf{s} \in \Gamma^{\omega}$ is *p-automatic* if there is an alphabet Σ, a finite-state automaton $(\Sigma, \langle p \rangle, \delta, a)$ satisfying $\delta(a, 0) = a$, and a 1-uniform morphism $\psi : \Sigma^{\infty} \to \Gamma^{\infty}$ such that, for each $i \geq 0$, $\mathbf{s}_i = \psi(\delta(a, i_{\langle p \rangle}))$. Since $\delta(a, 0) = a$, the number of leading zeroes in $i_{\langle p\rangle}$ is not important. We will say that $\mathbf{s}$ is *generated by the p-automaton* $(\Sigma, a, \delta, \Gamma, \psi)$. A p-automaton generating $\mathbf{s}$ will be called *minimal with respect to* $\mathbf{s}$ if the there is no p-automaton generating $\mathbf{s}$ with a state alphabet of a smaller size. It is a well-known fact from automata theory that a minimal automaton is unique up to renaming of symbols in the state alphabet.

Let $k \geq 1$ and $r \geq 2$, and let $\sigma : \Gamma^\infty \to \Gamma^\infty$ be a (k, kr)-substitution such that, for some $\mathbf{a} \in \Gamma^r$, $\mathbf{a}$ is a prefix of $\sigma(\mathbf{a})$ (i.e. σ is *expandable* in $\mathbf{a}$). Then $\sigma^n(\mathbf{a})$ is a proper prefix of $\sigma^{n+1}(\mathbf{a})$ for each $n \geq 0$ and the sequence $\mathbf{s} = \sigma^\omega(\mathbf{a}) = \lim_{n\to\infty} \sigma^n(\mathbf{a})$ is a fixed point of σ. We will say that the sequence $\mathbf{s} \in \Gamma^\omega$ is *generated by the substitution* σ. Since $r \geq 2$, it is easy to see that $\mathbf{s}$ is generated by σ if and only if $\mathbf{s}$ is a fixed point of σ. A (k, kr)-substitution generating $\mathbf{s}$ will be called *minimal with respect to* $\mathbf{s}$ if, whenever $\mathbf{s}$ is generated by some $(k_1, k_1 r_1)$-substitution, $k \leq k_1$ and $r \leq r_1$. Clearly, if $\mathbf{s}$ is a sequence generated by a substitution then there is a unique substitution minimal with respect to $\mathbf{s}$.

Now, let Γ be an alphabet. A sequence $\mathbf{s} \in \Gamma^\omega$ is a *p-uniform tag sequence* ([Cobham 72]), if there is an alphabet Σ (called *state alphabet*), a p-uniform morphism $\varphi : \Sigma^\infty \to \Sigma^\infty$ expandable in some $a \in \Sigma$, and a 1-uniform morphism $\psi : \Sigma^\infty \to \Gamma^\infty$ such that $\mathbf{s} = \psi(\lim_{n\to\infty} \varphi^n(a))$ $[= \lim_{n\to\infty} \psi(\varphi^n(a))]$. We will say that $\mathbf{s}$ is *generated by the p-uniform tag system* $(\Sigma, a, \varphi, \Gamma, \psi)$. A p-uniform tag system generating $\mathbf{s}$ will be called *minimal with respect to* $\mathbf{s}$ if there is no p-uniform tag system generating $\mathbf{s}$ with a state alphabet of a smaller size. Since uniform tag systems are closely related to automata (as we will see in Section 4) a minimal uniform tag system is unique up to renaming the symbols of the state alphabet.

If $\Gamma \subseteq \mathbb{F}$ where $\mathbb{F}$ is a finite field of characteristic p then a sequence $\mathbf{s} \in \Gamma^\omega$ may be identified with the formal power series $\sum_{i=0}^{\infty} \mathbf{s}_i X^i \in \mathbb{F}[[X]]$ and a finite word $\mathbf{w}$ with a polynomial $\sum_{i=0}^{|\mathbf{w}|-1} \mathbf{w}_i X^i \in \mathbb{F}[X]$.

Proposition 3. *Let* $\mathbf{s} \in \Gamma^\omega$ *be a sequence,* $p \geq 2$. *The following conditions (i), (ii), (iii) are equivalent. If* p *is a prime and* $\Gamma \subseteq \mathbb{F}$ *for a finite field* $\mathbb{F}$ *of characteristic* p *then the three conditions are equivalent to the condition (iv).*
(i) $\mathbf{s}$ *is a p-uniform tag sequence*
(ii) $\mathbf{s}$ *is a p-automatic sequence*
(iii) $\mathbf{s}$ *is a fixed point of some* (k, kp^m)*-substitution* $\sigma : \Gamma^\infty \to \Gamma^\infty$, k, $m \geq 1$
(iv) $\mathbf{s}$ *is algebraic over the field* $\mathbb{F}(X)$.

The proof of (i) $\equiv$ (ii) was given in [Cobham 72], the proof is based on the correspondence between the p-uniform tag system $(\Sigma, a, \varphi, \Gamma, \psi)$ and the p-automaton $(\Sigma, a, \delta, \Gamma, \psi)$ defined for $(b, i) \in \Sigma \times \langle p\rangle$ by the equality $\delta(b, i) = \varphi(b)_i$. The proof of (i) $\equiv$ (iii) can be found e.g. in [Černý and Gruska 86] (where it is provided for the 2-dimensional case), the idea of the proof (i) $\Rightarrow$ (iii) is used in [Section 5] of this paper. For the proof of (i) $\equiv$ (iv) see [Christol et al. 80].

3 Paperfolding sequences

Imagine the folding instructions denoted by 0 = "fold up" and 1 = "fold down", and the resulting edges denoted by 0 = "valley" and 1 = "peak". Let a stripe of paper be folded following a folding instruction sequence $\mathbf{u}_{i-1}...\mathbf{u}_0 \in \langle 2\rangle^*$ and subsequently unfolded following the reversed sequence $\mathbf{u}_0...\mathbf{u}_{i-1}$. The edge corresponding to the first folding instruction $\mathbf{u}_{i-1}$ appears in the middle of the created pattern, and the pattern in the right half of the paper is the result of the rotation of the pattern from the left half. Both these patterns appear as the result of application of the remaining part of the folding instruction sequence. Formally, the paperfolding word $\mathbf{p}_\mathbf{u}^{(i-1)} \in \langle 2\rangle^*$ corresponding to the finite sequence $\mathbf{u} = \mathbf{u}_0...\mathbf{u}_{i-1} \in \langle 2\rangle^*$of unfolding instructions is defined recurrently as

$$\mathbf{p}_\mathbf{u}^{(0)} = \mathbf{u}_0, \;\; \mathbf{p}_\mathbf{u}^{(n+1)} = \mathbf{p}_\mathbf{u}^{(n)}\mathbf{u}_n\widehat{\mathbf{p}_\mathbf{u}^{(n)}}^R$$

where $\mathbf{w}^R$ denotes the mirror image of $\mathbf{w}$. Obviously, $\mathbf{p}_\mathbf{u}^{(n)}$ is a proper prefix of $\mathbf{p}_\mathbf{u}^{(n+1)}$ for $n \geq 0$. We may extend this definition to an infinite sequence $\mathbf{u} \in \langle 2\rangle^\omega$ of unfolding instructions. The paperfolding sequence corresponding to $\mathbf{u}$ is then $\mathbf{p}_\mathbf{u} = \lim_{n\to\infty} \mathbf{p}_\mathbf{u}^{(n)}$.

Example 1. The following table describes the patterns obtained by a growing sequence of unfolding instructions.

folding sequence	unfolding sequence	pattern
1	1	1
11	11	110
011	110	1100100
1011	1101	110010011101100
11011	11011	1100100111011001110010001101100

Example 2. The following table contains four infinite sequences of unfolding instructions and the corresponding infinite paperfolding sequences. The n-th vertical line (placed between the (2^n-2)th and the (2^n-1)th position in the sequence $\mathbf{p}_\mathbf{u}$) denotes the end of the prefix $\mathbf{p}_\mathbf{u}^{(n-1)}$.

$\mathbf{u}$	$\mathbf{p}_\mathbf{u}$					
0^ω	0	01	0011	00011011	0001001110011011	...
$10(01)^\omega$	1	00	0110	11001110	0100011001001110	...
1001^ω	1	00	0110	11001110	1100011001001110	...
$0(110)^\omega$	0	11	1001	00110001	1011100110110001	...

The following position characterization of paperfolding sequences was proved in [Mendès-France and Shallit 89].

Proposition 4. *Let $n \geq 0$, $n+1 = 2^s(2k+1)$ with $s, k \geq 0$. If $k \equiv 0 \ (mod\ 2)$ then $(\mathbf{p}_\mathbf{u})_n = \mathbf{u}_s$, otherwise $(\mathbf{p}_\mathbf{u})_n = \overline{\mathbf{u}}_s$.*

One can easily observe that Proposition 4 can be reformulated as follows (there are two leading zeroes in $n_{\langle 2\rangle}$).

Proposition 5. *Let $n \geq 0$.*
If $n = r2^{s+2} + (2^s - 1)$ for some $r, s \geq 0$, i.e. $n_{\langle 2\rangle}$ ends with a suffix of the form 001^s, $s \geq 0$, then $\mathbf{p}_n = \mathbf{u}_s$.
If $n = r2^{s+2} + (2^{s+1} + 2^s - 1)$ for some $r, s \geq 0$, i.e. $n_{\langle 2\rangle}$ ends with a suffix of the form 101^s then $(\mathbf{p}_\mathbf{u})_n = \overline{\mathbf{u}}_s$.

We are interested in the optimal way of description of 2-automatic paperfolding sequences. First we will show the intuitively expected fact that a paperfolding sequence cannot be p-automatic for $p > 2$ unless p is a power of 2. In the proof, we will use the following property of the sequence $\mathbf{p_u}$.

Lemma 6. *For $j \geq 0, n \geq 1$*

$$[\mathbf{p_u}]_{j2^n}^{2^n-1} = [\mathbf{p_u}]_{(j+2)2^n}^{2^n-1}$$

Proof. By induction using the fact that $\mathbf{p_u}^{(n+2)} = \mathbf{p_u}^{(n)}\mathbf{u}_n\widehat{\mathbf{p_u}^{(n)}}^R, \mathbf{u}_{n+1}\mathbf{p_u}^{(n)}\overline{\mathbf{u}}_n\widehat{\mathbf{p_u}^{(n)}}^R$ and $|\mathbf{p_u}^{(n)}| = 2^n - 1$.

Theorem 7. *If $\mathbf{p_u}$ is a p-automatic sequence then p is a power of 2 and $\mathbf{p_u}$ is 2-automatic.*

Proof. Let $\mathbf{p_u}$ be a p-automatic sequence, $p \geq 2$. Due to [Cobham 72], if p is a power of 2 then $\mathbf{p_u}$ is 2-automatic. Assume p is not a power of 2. Then $p = 2^j(2i+1)$ for some $i \geq 1, j \geq 0$. According to (iii) of Proposition 3, $\mathbf{p_u}$ is a fixed point of some (k, kp^r)-substitution σ. Let $k = 2^c(2d+1)$ and $2^{z-1} \leq k < 2^z$ for some $c, d \geq 0$, $z \geq 1$. Denote $s = z + rj$ and $m = 2^{z+1}(2d+1)$. The number m is both a multiple of k and an even multiple of 2^z. By Lemma 6, the two subwords of length $2^z - 1$ of $\mathbf{p_u}$, one starting at the position 0 and one at the position m, are identical. Moreover, $kp^r = k2^{rj}(2i+1)^r \geq 2^{rj}(2i+1)^r 2^{z-1} > 2^s$ and $mp^r = 2^{z+rj+1}(2d+1)(2i+1)^r = 2^{s+2}i' + 2^{s+1}$ for some $i' \geq 1$, hence $mp^r + 2^s - 1 = 2^{s+2}i' + 2^{s+1} + 2^s - 1$. Using Proposition 5 we obtain

$$\begin{aligned}
\mathbf{u}_s &= (\mathbf{p_u})_{2^s-1} = ([\mathbf{p_u}]_0^{kp^r})_{2^s-1} = (\sigma([\mathbf{p_u}]_0^k))_{2^s-1} \\
&= (\sigma([[\mathbf{p_u}]_0^{2^z-1}]_0^k))_{2^s-1} = (\sigma([[\mathbf{p_u}]_m^{2^z-1}]_0^k))_{2^s-1} = (\sigma([\mathbf{p_u}]_m^k))_{2^s-1} \\
&= ([\mathbf{p_u}]_{mp^r}^{kp^r})_{2^s-1} = (\mathbf{p_u})_{mp^r+2^s-1} = \overline{\mathbf{u}}_s
\end{aligned}$$

yielding a contradiction.

Corollary 8. *The sequence $\mathbf{p_u}$ is automatic iff $\mathbf{u}$ is ultimately periodic.*

Proof. Follows from Theorem 7 and the fact ([Mendès-France and Shallit 89]) that $\mathbf{p_u}$ is 2-automatic if and only if $\mathbf{u}$ is ultimately periodic.

Starting from now, we will assume an arbitrary (but fixed) ultimately periodic unfolding sequence $\mathbf{u}$ and its 1-minimal decomposition (see Corollary 2) $\mathbf{u} = \mathbf{v}\mathbf{z}^\omega$ (hence $|\mathbf{v}| \geq 1$, $|\mathbf{z}| \geq 1$). We will denote $\mathbf{p} = \mathbf{p_u}$.

In the sequence $\mathbf{u}$, the symbol at position $s \in \mathbb{N}$ is denoted by $\mathbf{u}_s$. We will extend this notation to elements of $\overline{\mathbb{N}}$ by defining

$$\mathbf{u}_{\overline{s}} = \overline{\mathbf{u}}_s. \tag{1}$$

In our search for optimal ways of description of $\mathbf{p}$ we will distinguish two possible cases while keeping a common notation for both the cases.

Case **A** The word $\mathbf{z}$ cannot be decomposed as $\mathbf{z} = \mathbf{w}\overline{\mathbf{w}}$.
Case **B** The word $\mathbf{z}$ can be decomposed as $\mathbf{z} = \mathbf{w}\overline{\mathbf{w}}$.

In case **A** we will denote $\mathbf{w} = \mathbf{z}$. In both cases we will denote $p = |\mathbf{v}|$ and $q = |\mathbf{w}|$ and define a "periodic successor" function

$$\begin{array}{ll} \xi : \mathbb{N} \cup \overline{\mathbb{N}} \to \widetilde{\langle p+q \rangle} & \\ \xi(n) = n+1 & \text{for } 0 \le n < p+q-1 \\ \xi(n) = \xi(n-q) & \text{for } p+q \le n, \text{ case } \mathbf{A} \\ \xi(n) = \overline{\xi(n-q)} & \text{for } p+q \le n, \text{ case } \mathbf{B} \\ \xi(\overline{n}) = \overline{\xi(n)} & \text{for } n \ge 0. \end{array}$$

We will use the following properties of the function ξ.

Proposition 9. *For* $r,\ s \ge 0$.
(i) if $r+s \ge 1$ *then* $\xi^r(s) = \xi(r+s-1)$
(ii) if $r \ge p$ *then* $\xi^{r+q}(s) = \xi^r(s)$ *in case* **A**, *and* $\xi^{r+q}(s) = \overline{\xi^r(s)}$ *in case* **B**
(iii) $\mathbf{u}_{s+r} = \mathbf{u}_{\xi^r(s)}$ *(we are using the notation (1)).*

Let us note that, because of minimality of $\mathbf{v}$ and $\mathbf{z}$, in neither of the two cases $\mathbf{w}$ can be further decomposed as $\mathbf{w} = \mathbf{x}\overline{\mathbf{x}}$ and in case **A** the word $\mathbf{w}$ is primitive, i.e. $\mathbf{w}$ cannot be decomposed as $\mathbf{w} = \mathbf{x}^k$ for $k > 1$. Using the same notation in case **A** as in case **B**, we adopt the convention that all our further considerations and assertions, unless explicitly stated otherwise, apply to both the cases.

4 Description by automata and tag systems

We will first present a 2-automaton generating the sequence $\mathbf{p}$. The construction is simpler than the one provided in [Mendès-France and Shallit 89] and in case **A** corresponds directly to the uniform tag systems from [Bercoff 95] designed using Toeplitz description of the paperfolding sequence. The 2-automaton is defined as

$$\mathcal{A} = (\widetilde{\langle p+q \rangle}, 0, \delta, \langle 2 \rangle, \psi)$$

$\delta:$	$(0,0) \mapsto 0$	$(\overline{0},0) \mapsto 0$	
	$(s,0) \mapsto \overline{0}$	$(\overline{s},0) \mapsto \overline{0}$	for $1 \le s < p+q$
	$(s,1) \mapsto \xi(s)$	$(\overline{s},1) \mapsto \xi(\overline{s})$	for $0 \le s < p+q$
$\psi:$	$s \mapsto \mathbf{u}_s$	$\overline{s} \mapsto \overline{\mathbf{u}}_s$	for $0 \le s < p+q$

Let $\mathbf{w} \in 00\langle 2 \rangle^* \cup 10\langle 2 \rangle^*$. Then Proposition 9 implies that $\delta(0,\mathbf{w}) = b$ if and only if the following condition is satisfied for some $\mathbf{x} \in \langle 2 \rangle^*$:

$$\begin{array}{ll} \mathbf{w} = \mathbf{x}001^s & \text{if } b = s \in \underline{\langle p \rangle} \\ \mathbf{w} = \mathbf{x}101^s & \text{if } b = \overline{s} \in \underline{\langle p \rangle} \\ \text{case } \mathbf{A}: & \\ \mathbf{w} = \mathbf{x}001^{kq+s} & \text{if } b = s \in \underline{\langle p+q \rangle} - \underline{\langle p \rangle} \\ \mathbf{w} = \mathbf{x}101^{kq+s} & \text{if } b = \overline{s} \in \underline{\langle p+q \rangle} - \underline{\langle p \rangle} \\ \text{case } \mathbf{B}: & \\ \mathbf{w} = \mathbf{x}001^{2kq+s} \text{ or } \mathbf{w} = \mathbf{x}101^{2kq+q+s} & \text{if } b = s \in \underline{\langle p+q \rangle} - \underline{\langle p \rangle} \\ \mathbf{w} = \mathbf{x}101^{2kq+s} \text{ or } \mathbf{w} = \mathbf{x}001^{2kq+q+s} & \text{if } b = \overline{s} \in \underline{\langle p+q \rangle} - \underline{\langle p \rangle} \end{array}$$

The automaton $\mathcal{A}$ generates the sequence $\mathbf{p}$ as follows from Proposition 5.

The 2-uniform tag system corresponding to $\mathcal{A}$ (see [Cobham 72]) is

$$\mathcal{T} = (\widetilde{\langle p+q\rangle}, 0, \varphi, \langle 2\rangle, \psi)$$

$\varphi:$	$0 \mapsto 0\,1$	$\overline{0} \mapsto 0\,\overline{1}$	
	$s \mapsto \overline{0}\,\xi(s)$	$\overline{s} \mapsto \overline{0}\,\xi(\overline{s})$	for $1 \le s < p+q$
$\psi:$	$s \mapsto \mathbf{u}_s$	$\overline{s} \mapsto \overline{\mathbf{u}}_s$	for $0 \le s < p+q$

Proposition 10. *For* $s \in \widetilde{\langle p+q\rangle}$, $\psi(s) = \mathbf{u}_s$.

Applying the usual techniques of proving minimality of automata we obtain the following result.

Theorem 11. *The* 2*-automaton* $\mathcal{A}$ *is minimal with respect to* $\mathbf{p}$. *The* 2*-uniform tag system* $\mathcal{T}$ *is minimal with respect to* $\mathbf{p}$.

Proof. It is enough to prove the minimality of $\mathcal{A}$. Suppose that there is a 2-automaton generating $\mathbf{p}$ with a smaller number of states than $2(p+q)$. By the pigeonhole principle, the set $\{001^s, 101^s; s \in \langle p+q\rangle\}$ contains a pair of different words $\mathbf{b} = b01^{s_1}, \mathbf{c} = c01^{s_2}$, $b, c \in \langle 2\rangle$, $s_2 \ge s_1 \ge 0$, such that $\psi(\delta(0, \mathbf{bx})) = \psi(\delta(0, \mathbf{cx}))$ for each $\mathbf{x} \in \langle 2\rangle^*$. Let $\mathbf{b}$ and $\mathbf{c}$ be such that s_1 is minimal possible.

Obviously, $s_1 \ne s_2$, otherwise $\mathbf{b} = \mathbf{c}$ or $\mathbf{u}_{s_1} = \overline{\mathbf{u}}_{s_1}$. If $s_2 > s_1 = 0$ then $\mathbf{u}_0 = \psi(\delta(0, b00)) = \psi(\delta(0, c01^{s_2}0)) = \overline{\mathbf{u}}_0$ - a contradiction. Hence we may assume $s_2 > s_1 \ge 1$.

If $b = c = 0$ (the case $b = c = 1$ can be treated in a similar way) then for $k \ge s_1$

$$\mathbf{u}_{k+(s_2-s_1)} = \psi(\delta(0, \mathbf{c}1^{k-s_1})) = \psi(\delta(0, \mathbf{b}1^{k-s_1})) = \mathbf{u}_k.$$

If $s_1 < p$, we get a contradiction to the 1-minimality of $|\mathbf{v}|$, since $\mathbf{p}$ has a preperiod of length $1 \le s_1 \le |\mathbf{v}|$. If $s_1 \ge p$ we get a contradiction to the 1-minimality of $|\mathbf{z}|$, since $\mathbf{p}$ has a period of length $0 < s_2 - s_1 < (p+q) - p = q = |\mathbf{z}|$.

Let $b = \overline{c} = 0$ (the case $b = \overline{c} = 1$ can be treated in a similar way). Then for $k \ge s_2$ we obtain

$$\begin{aligned} \overline{\mathbf{u}}_k &= \psi(\delta(0, \mathbf{c}1^{k-s_2})) = \psi(\delta(0, \mathbf{b}1^{k-s_2})) = \mathbf{u}_{k-(s_2-s_1)} \\ \mathbf{u}_k &= \overline{\psi(\delta(0, \mathbf{c}1^{k-s_2}))} = \overline{\psi(\delta(0, \mathbf{b}1^{k-s_2}))} = \overline{\mathbf{u}}_{k-(s_2-s_1)} \end{aligned}$$

Hence $\mathbf{u}$ has a period of length $2(s_2 - s_1)$ starting from the position s_1. If $s_1 < p$, we get a contradiction to the minimality of $|\mathbf{v}|$. If $s_1 \ge p$ then, because of the minimality of q, $2(s_2 - s_1)$ is a multiple of $|\mathbf{z}|$. However, $s_2 - s_1 < |\mathbf{z}|$, therefore $s_2 - s_1 = |\mathbf{z}|/2$ yielding a contradiction in case **B.** If in case **A** $s_1 > p$ then for $\mathbf{x} \in \langle 2\rangle^*$

$$\begin{aligned} \psi(\delta(0, 001^{s_1-1}\mathbf{x})) &= \psi(\delta(0, 001^{s_1+|\mathbf{z}|-1}\mathbf{x})) = \psi(\delta(0, 001^{s_2+|\mathbf{z}|/2-1}\mathbf{x})) \\ &= \overline{\psi(\delta(0, 001^{s_2-1}\mathbf{x}))} = \psi(\delta(0, 101^{s_2-1}\mathbf{x})) \end{aligned}$$

- a contradiction to the minimality of s_1. The only remaining possibility in case **A** is $s_1 = p$, $s_2 = p + q/2$ implying $\mathbf{z} = \mathbf{w}\overline{\mathbf{w}}$ – a contradiction.

Example 3. Minimal tag systems for sequences from Example 2:

u	$\mathcal{T}$								
		0	$\overline{0}$	1	$\overline{1}$	2	$\overline{2}$	3	$\overline{3}$
00^ω	φ	01	$0\overline{1}$	$\overline{0}1$	$\overline{0}\overline{1}$				
	ψ	0	1	0	1				
$10(01)^\omega$	φ	01	$0\overline{1}$	$\overline{0}2$	$\overline{0}\overline{2}$	$\overline{0}\overline{2}$	$\overline{0}2$		
	ψ	1	0	0	1	0	1		
1001^ω	φ	01	$0\overline{1}$	$\overline{0}2$	$\overline{0}\overline{2}$	$\overline{0}3$	$\overline{0}\overline{3}$	$\overline{0}3$	$\overline{0}\overline{3}$
	ψ	1	0	0	1	0	1	1	0
$0(110)^\omega$	φ	01	$0\overline{1}$	$\overline{0}2$	$\overline{0}\overline{2}$	$\overline{0}3$	$\overline{0}\overline{3}$	$\overline{0}1$	$\overline{0}\overline{1}$
	ψ	0	1	1	0	1	0	0	1

5 Description by substitutions

In our next considerations we want to find a characterization of automatic paperfolding sequences according to (iii) of Proposition 3.

Let $\mathcal{T} = (\left\langle \widetilde{p+q} \right\rangle, 0, \varphi, \langle 2 \rangle, \psi)$ be the minimal 2-uniform tag system generating the sequence $\mathbf{p}$. We denote $\mathbf{p}^\varphi = \varphi^\omega(a) = \lim_{n\to\infty} \varphi^n(a)$. To learn about the internal structure of the sequence $\mathbf{p}$, we have to investigate the structure of $\mathbf{p}^\varphi$. We start with a technical lemma.

Lemma 12. *For each* $b \in \widetilde{\langle p+q \rangle} - \{0, \overline{0}\}$ *and* $i \geq 1$ *there is an odd number* $f(b,i)$ *such that* $\mathbf{p}^\varphi_{f(b,i)(2i+1)} = b$.

Proof. Let $s \in \langle p+q \rangle$. Since $\gcd(2i+1, 2^{s+2}) = 1$, there is $k \geq 0$ such that $(2k+1)(2i+1) \equiv 1 \pmod{2^{s+2}}$. If we chose $f(s,i) = (2^s - 1)(2k+1)$, $f(\overline{s}, i) = (2^{s+1} + 2^s - 1)(2k+1)$ then $f(s,i)(2i+1)$ends with the suffix 001^s, and $f(\overline{s},i)(2i+1)$ ends with 101^s.

The words of the form $\psi(\varphi^k(b))$, $k \geq 0$, $b \in \widetilde{\langle p+q \rangle}$, will be called k-blocks. If we decompose $\mathbf{p}$ to words of size 2^k, for a fixed $k \geq 0$, each of these words will be a k-block. Let $\{\equiv_k\}_{k=1}^\infty$ be a sequence of equivalence relations on $\widetilde{\langle p+q \rangle}$ defined by

$$b \equiv_k c \text{ iff } \psi(\varphi^k(b)) = \psi(\varphi^k(c)). \tag{2}$$

The equivalence relations $\equiv_k$ are closely related to substitutions for which $\mathbf{p}$ is a fixed point, as we will see in Lemma 16. The internal structure of k-blocks determining the relations $\equiv_k$ depends on the structure of the words $\varphi^k(b)$. This structure is described by the following lemma corresponding to Lemma 6. The lemma can be easily proved by induction.

Lemma 13. *Let* $k \geq 0$.
If $b \in \{0, \overline{0}\}$ *then* $\varphi^k(b) = \varphi^{k-1}(0)\varphi^{k-2}(\overline{0})\varphi^{k-3}(\overline{0})...\varphi^0(\overline{0})\xi^k(b)$.
If $b \notin \{0, \overline{0}\}$ *then* $\varphi^k(b) = \varphi^{k-1}(\overline{0})\varphi^{k-2}(\overline{0})\varphi^{k-3}(\overline{0})...\varphi^0(\overline{0})\xi^k(b)$.

Corollary 14. *For* $b, c \in \widetilde{\langle p+q \rangle} - \{0, \overline{0}\}$, $k \geq 1$
(i) $\psi(\varphi^k(b)) = \psi(\varphi^k(c))$ *if and only if* $\psi(\xi^k(b)) = \psi(\xi^k(c))$
(ii) $b \equiv_k c$ *if and only if* $\psi(\xi^k(b)) = \psi(\xi^k(c))$.

Lemma 15.
(i) If $\equiv_m = \equiv_0$ *then* $m = 0$.
(ii) Let $m, n \geq 1$. *If* $\psi(\varphi^m(b)) = \psi(\varphi^m(c))$ *implies* $\psi(\varphi^n(b)) = \psi(\varphi^n(c))$ *for all* $b, c \in \widetilde{\langle p+q \rangle} - \{0, \overline{0}\}$ *then* $\equiv_m = \equiv_n$.

Proof. (i) By Lemma 13 there are two different 0-blocks and for each $m \geq 1$ there are exactly four different m-blocks determining exactly four different equivalence classes of $\equiv_m$. Hence $m = 0$.

(ii) Let $\psi(\varphi^m(b)) = \psi(\varphi^m(c))$ imply $\psi(\varphi^n(b)) = \psi(\varphi^n(c))$. Let b_1 and c_1 be such that $\psi(\varphi^m(b_1)) \neq \psi(\varphi^m(c_1))$ and $\psi(\varphi^n(b_1)) = \psi(\varphi^n(c_1))$. Out of the four equivalence classes in both $\equiv_m$ and $\equiv_n$, two are the singleton sets $\{0\}$ and $\{\overline{0}\}$. Since any element from $\widetilde{\langle p+q \rangle} - \{0, \overline{0}\}$ is equivalent in $\equiv_m$ either to b_1 or to c_1, any two such elements must be equivalent in $\equiv_n$, thus $\equiv_n$ consists of three classes only – a contradiction.

Lemma 16. *The sequence* $\mathbf{p}$ *is a fixed point of a* $(2^r, 2^s)$*-substitution for some* $0 \leq r < s$, *if and only if* $\equiv_r = \equiv_s$.

Proof. Let $\equiv_r = \equiv_s$. The equality (2) allows us to define a $(2^r, 2^s)$-substitution $\sigma^{(r,s)} : \langle 2 \rangle^\infty \to \langle 2 \rangle^\infty$ by

$$\sigma^{(r,s)} : \ \psi(\varphi^r(b)) \mapsto \psi(\varphi^s(b)) \ \text{ for } b \in \Sigma$$

and arbitrarily for the remaining words from $\langle 2 \rangle^{2^r}$. Then $\mathbf{p}$ is a fixed point of $\sigma^{(r,s)}$. Indeed, for $k \geq 0$

$$\sigma^{(r,s)}([\mathbf{p}]_{k2^r}^{2^r}) = \sigma^{(r,s)}(\psi(\varphi^r(\mathbf{p}_k^\varphi))) = \psi(\varphi^s(\mathbf{p}_k^\varphi)) = [\mathbf{p}]_{k2^s}^{2^s}.$$

On the other hand, if $\mathbf{p}$ is a fixed point of a $(2^r, 2^s)$-substitution τ, then τ maps $\psi(\varphi^r(b))$ to $\psi(\varphi^s(b))$ and $\psi(\varphi^r(b)) = \psi(\varphi^r(c))$ implies $\psi(\varphi^s(b)) = \psi(\varphi^s(c))$ for $b, c \in \widetilde{\langle p+q \rangle}$. There are only two different 0-blocks, therefore $r \neq 0$, because $s > 0$ and there are four different s-blocks. By (ii) of Lemma 15, we get $\equiv_r = \equiv_s$.

Lemma 17.
(i) Let $\equiv_r = \equiv_s$ *for some* $s > r > 0$. *Then* $\equiv_{r+k} = \equiv_{s+k}$ *for* $k \geq 0$.
(ii) If $r \geq \max(1, p-1)$ *then* $\equiv_r = \equiv_{r+q}$
(iii) Let $\equiv_r = \equiv_{r+s}$ *for some* $r, s \geq 1$. *Then* $\equiv_p = \equiv_{p+\gcd(q,s)}$.

Proof. (i) By Lemma 16, $\sigma^{(r,s)}(\mathbf{p}) = \mathbf{p}$. We define a $(2^{r+k}, 2^{s+k})$-substitution τ by $\tau(\mathbf{x}^{(1)} ... \mathbf{x}^{(2^k)}) = \sigma^{(r,s)}(\mathbf{x}^{(1)}) ... \sigma^{(r,s)}(\mathbf{x}^{(2^k)})$ for $\mathbf{x}^{(i)} \in \langle 2 \rangle^{2^r}$. Then $\tau(\mathbf{p}) = \mathbf{p}$. Lemma 16 implies $\equiv_{r+k} = \equiv_{s+k}$.

(ii) It follows from Proposition 9, that $\psi(\xi^{r+q}(s)) = \psi(\xi^{r+1+q}(s-1))$ for $s \geq 1$. Therefore $\psi(\xi^{r+q}(s)) = \psi(\xi^{r+1}(s-1)) = \psi(\xi^r(s))$ in case $\mathbf{A}$, and $\psi(\xi^{r+q}(s)) = \psi(\overline{\xi^{r+1}(s-1)}) = \overline{\psi(\xi^r(s))}$ in case $\mathbf{B}$. Thus $\psi(\xi^{r+q}(b)) = \psi(\xi^{r+q}(c))$ implies

$\psi(\xi^r(b)) = \psi(\xi^r(c))$ for $b, c \in \widetilde{\langle p+q \rangle} - \{0, \overline{0}\}$. We may apply Corollary 14 and Lemma 15.

(iii) If $r < p$ then applying (i), with $k = (p-r)$, we obtain $\equiv_{r+(p-r)} = \equiv_{r+s+(p-r)}$. If $r \geq p$ then $r = p + mq + t$, where $m \geq 0$ and $q > t \geq 0$. Applying (i) with $k = (q-t)$, and then $(m+1)$ times (ii), we obtain $\equiv_{r+(q-t)-(m+1)q} = \equiv_{r+s+(q-t)-(m+1)q}$. In both cases $\equiv_p = \equiv_{p+s}$ and, by (ii), $\equiv_{p+q} = \equiv_p = \equiv_{p+s}$. Then (i) applied for $k = |q-s|$ yields $\equiv_{p+\min(q,s)} = \equiv_p = \equiv_{p+|q-s|}$. The assertion follows from application of Euclid's algorithm.

Corollary 18. $\equiv_p = \equiv_{p+q}$. *If* $p \geq 2$ *then* $\equiv_{p-1} = \equiv_{p-1+q}$.

Lemma 19. *Let* $\equiv_m = \equiv_n$ *for some* $n > m \geq 1$. *Then*
(i) $\psi(\xi^m(b)) = \psi(\xi^n(b))$ *for each* $b \in \widetilde{\langle p+q \rangle} - \{0, \overline{0}\}$ *or*
(ii) $\psi(\xi^m(b)) = \overline{\psi(\xi^n(b))}$ *for each* $b \in \widetilde{\langle p+q \rangle} - \{0, \overline{0}\}$.

Proof. Let $\equiv_m = \equiv_n$ and let, for some symbol $b \in \widetilde{\langle p+q \rangle} - \{0, \overline{0}\}$, $\psi(\xi^m(b)) = \psi(\xi^n(b))$. Let $c \in \widetilde{\langle p+q \rangle} - \{0, \overline{0}\}$. Then either $b \equiv_m c$ and $b \equiv_n c$, and $\psi(\xi^n(c)) = \psi(\xi^n(b)) = \psi(\xi^m(b)) = \psi(\xi^m(c))$, or $b \not\equiv_m c$ and $b \not{equiv}_n c$, and $\overline{\psi(\xi^n(c))} = \psi(\xi^n(b)) = \psi(\xi^m(b)) = \overline{\psi(\xi^m(c))}$. In the latter case $\psi(\xi^n(c)) = \psi(\xi^m(c))$ and (i) holds. If $\psi(\xi^m(b)) = \psi(\xi^n(b))$ is not true for any symbol $b \in \widetilde{\langle p+q \rangle} - \{0, \overline{0}\}$, then (ii) holds.

Lemma 20. *If* $\equiv_r = \equiv_{r+s}$ *for some* $r, s \geq 1$ *then* s *is a multiple of* q.

Proof. Assume that s is not a multiple of q. Denote $d = \gcd(s, q)$. Then $d < q$, i.e. $1 \leq d \leq q/2$, and $q \geq 2$. By Lemma 17, $\equiv_p = \equiv_{p+d}$. Lemma 19, applied for $m = p$ and $n = p + d$, implies some additional regularity on the structure of $\mathbf{u}$. If (i) of Lemma 19 is true then, for each $b \in \langle p+q \rangle - \{0\}$, $\mathbf{u}_{b+p} = \mathbf{u}_{b+p+d}$, as follows from Proposition 9 (iii) and Proposition 10. Let $k \geq 0$. The number k can be written as $k = k_1 q + k_2$, where $k_1 \geq 0$ and $q > k_2 \geq 0$. Then $1 \leq 1 + k_2 \leq p + k_2 < p + q$. We obtain $\mathbf{u}_{1+p+k+d} = \mathbf{u}_{1+p+k_1 q+k_2+d} = \mathbf{u}_{(1+k_2)+p+d} = \mathbf{u}_{(1+k_2)+p} = \mathbf{u}_{(1+k_2)+p+k_1 q} = \mathbf{u}_{1+p+k}$. Hence the sequence $\mathbf{u}$ has a period of length $d < q = |\mathbf{z}|$ – a contradiction to the minimality of the period $\mathbf{z}$.

In a similar way, if (ii) of Lemma 19 is true, then

$$\mathbf{u}_{b+p} = \overline{\mathbf{u}}_{b+p+d} \tag{3}$$

for each $b \in \langle p+q \rangle - \{0\}$. Then, for $0 < b < p+q-d$, $\mathbf{u}_{b+p} = \overline{\mathbf{u}}_{b+p+d} = \mathbf{u}_{b+p+2d}$.

If q/d is odd then $\mathbf{u}_{1+p} = \overline{\mathbf{u}}_{1+p+d} = \overline{\mathbf{u}}_{1+p+(q/d-1)d+d} = \overline{\mathbf{u}}_{1+p+(q/d)d} = \overline{\mathbf{u}}_{1+p+q}$ (since $0 < 1 + (q/d-1)d < q + p$) – a contradiction in case **A**. In case **B**, $\mathbf{u}_p = \overline{\mathbf{u}}_{p+q} = \overline{\mathbf{u}}_{p+(q-d)+d} = \overline{\mathbf{u}}_{p+(q/d-1)d+d} = \overline{\mathbf{u}}_{p+d}$. Hence (3) holds for $b = 0$, as well, and (3) implies that $\mathbf{w} = (\boldsymbol{\beta}\overline{\boldsymbol{\beta}})^{(q/d-1)/2}\boldsymbol{\beta}$ where $\boldsymbol{\beta}$ is the prefix of $\mathbf{w}$ of length d. Then $\mathbf{w}\overline{\mathbf{w}} = (\boldsymbol{\beta}\overline{\boldsymbol{\beta}})^{(q/d-1)/2}\boldsymbol{\beta}(\overline{\boldsymbol{\beta}}\boldsymbol{\beta})^{(q/d-1)/2}\overline{\boldsymbol{\beta}} = (\boldsymbol{\beta}\overline{\boldsymbol{\beta}})^{q/d}$ and $\boldsymbol{\beta}\overline{\boldsymbol{\beta}}$ is a period of $\mathbf{u}$ of length $2d < q$ – a contradiction to the minimality of the period $\mathbf{z}$.

Let q/d be even. Then, in case **A**, $\mathbf{u}_p = \mathbf{u}_{p+q} = \mathbf{u}_{p+(q/d-2)d+2d} = \mathbf{u}_{p+d+d} = \overline{\mathbf{u}}_{p+d}$ Hence (3) holds for $b = 0$ as well, and (3) implies that $\mathbf{w} = (\boldsymbol{\beta}\overline{\boldsymbol{\beta}})^{q/(2d)}$

where $\boldsymbol{\beta}$ is the prefix of $\mathbf{w}$ of length d. Then either $q/d > 2$ and $\boldsymbol{\beta}\overline{\boldsymbol{\beta}}$ is a period of $\mathbf{u}$ of length $2d < q$, or $q = 2d$ and $\mathbf{z}$ is decomposable as $\mathbf{z} = \boldsymbol{\beta}\overline{\boldsymbol{\beta}}$ – both cases yielding a contradiction. In case **B** (3) implies $\mathbf{u}_{1+p} = \mathbf{u}_{1+p+(q/2)2d} = \mathbf{u}_{1+p+q}$ (since $0 < 1 < 1 + (q/d-2)d < p + q - d$) – a contradiction.

Lemma 21. *Let* $\equiv_m = \equiv_{m+rq}$ *for some* $m \geq 1$ *and* $r \geq 1$. *Then* $m \geq p - 1$.

Proof. Assume to the contrary $m < p - 1$. In view of (ii) of Lemma 17 we may assume $p + q > m + rq$.

As in the proof of Lemma 20, for $b \in \langle p+q \rangle - \{0\}$ we obtain that $\mathbf{u}_{b+m} = \mathbf{u}_{b+m+rq}$ in case (i) of Lemma 19, and $\mathbf{u}_{b+m} = \overline{\mathbf{u}}_{b+m+rq}$ in case (ii) of the same Lemma. Case **A**. In case (i) of Lemma 19, by (i) of Proposition 1 we may choose for $\mathbf{u}$ a pre-period of length $p + q + m$ and a period of length rq. Then $\mathbf{u}_{b+m} = \mathbf{u}_{b+m+rq}$ for $b \geq p + q$, as well. Therefore $\mathbf{u}$ has a pre-period of length $1 \leq m + 1 < p$, which contradicts the minimality of p. In case (ii) of Lemma 19 we obtain $\mathbf{u}_{p+m} = \overline{\mathbf{u}}_{p+m+rq} = \overline{\mathbf{u}}_{p+m}$ – a contradiction.

Case **B**. In case (i) of Lemma 19, if r is even, we arrive to a contradiction in the same way as in the case **A** by showing that $\mathbf{u}$ has a pre-period of length $m + 1$. If r is odd then $\mathbf{u}_{p+m} = \mathbf{u}_{p+m+rq} = \overline{\mathbf{u}}_{p+m}$ – again a contradiction.

In case (ii) of Lemma 19, if r is odd, for $\max(m+1, p-q) \leq i < p$ we get $\mathbf{u}_i = \overline{\mathbf{u}}_{i+rq} = \overline{\mathbf{u}}_{i+(r-1)q+q} = \overline{\mathbf{u}}_{i+q}$. Since $\mathbf{u}_i = \overline{\mathbf{u}}_{i+q}$ for $i \geq p$, the sequence $\mathbf{u}$ has a non-empty pre-period of length $\max(m+1, p-q) < p$ – a contradiction to the minimality of p. If r is even then rq is a multiple of $2q$ and $\mathbf{u}_{p+m} = \overline{\mathbf{u}}_{p+m+rq} = \overline{\mathbf{u}}_{p+m}$ – a contradiction.

We are now ready to describe the minimal substitution having $\mathbf{p}$ as a fixed point.

Theorem 22. *The minimal substitution* σ *satisfying* $\sigma(\mathbf{p}) = \mathbf{p}$ *is* $\sigma = \sigma^{(p,p+q)}$ *if* $p = 1$, *and it is* $\sigma = \sigma^{(p-1,p-1+q)}$ *if* $p \geq 2$.

Proof. Let us use the common notation $\sigma^{(a,a+q)}$ where $a = p = 1$ or $p \geq 2$ and $a = p - 1$. The assertion $\sigma^{(a,a+q)}(\mathbf{p})=\mathbf{p}$ follows from Corollary 18 and Lemma 16.

If $\mathbf{p}$ is a fixed point of some (k, kr)-substitution, then according to Proposition 3 $\mathbf{p}$ is a r-automatic sequence. Since $\mathbf{p}$ is a 2-automatic sequence which is not ultimately periodic, due to the result of Cobham ([Cobham 69]) r is a power of 2.

Let $\mathbf{p}$ be a fixed point of some $(2^{a'}, 2^{a'+b'})$-substitution. Then by Lemma 20 $b' \geq q$ and by Lemma 21 $a' \geq a$.

Let $\mathbf{p}$ be a fixed point of some $(m, m2^k)$-substitution τ where either $k < q$, or $k \geq q$, $m < 2^a$ and m is not a power of 2. In either case, we may assume that $1 \leq 2^{r-1} < m < 2^r$. Then, in the former case by Lemma 20 and in the latter case (since $r - 1 < a$) by Lemma 21, $\equiv_{r-1} \neq \equiv_{r-1+k}$. Therefore there exist $b, c \in \langle p+q \rangle$ such that $\psi(\varphi^{r-1}(b)) = \psi(\varphi^{r-1}(c))$ and $\psi(\varphi^{r-1+k}(b)) \neq \psi(\varphi^{r-1+k}(c))$. The number m can be decomposed as $m = 2^j(2i+1)$, $0 \leq j < r - 1$, $i \geq 1$. Denote $n(d) = 2^{r-1}(2i+1)f(d,i)$ for $d \in \{b, c\}$, where $f(d,i)$ is the number from Lemma 12. Then $n(d)$ is a multiple of m and an odd multiple of 2^{r-1}, and, since

$2^{r-1+k} < m2^k$, we get

$$\begin{aligned}\psi(\varphi^{r-1+k}(d)) &= [\mathbf{p}]_{2^k n(d)}^{2^{r-1+k}} \\ &= [\tau([\mathbf{p}]_{n(d)}^{m})]_0^{2^{r-1+k}} \\ &= [\tau([\mathbf{p}]_{n(d)}^{2^{r-1}}[\mathbf{p}]_{n(d)+2^{r-1}}^{m-2^{r-1}})]_0^{2^{r-1+k}} \\ &= [\tau(\psi(\varphi^{r}(d))[\mathbf{p}]_{n(d)+2^{r-1}}^{m-2^{r-1}})]_0^{2^{r-1+k}}.\end{aligned} \tag{4}$$

Lemma 6 implies $[\mathbf{p}]_{n(b)+2^{r-1}}^{m-2^{r-1}} = [\mathbf{p}]_{n(c)+2^{r-1}}^{m-2^{r-1}}$. Therefore the last expression in (4) has the same value for b and c - a contradiction.

Example 4. The minimal substitutions for sequences from Example 2:

$\mathbf{u}$	σ
00^ω	$00 \mapsto 0010,\ 01 \mapsto 0011,\ 10 \mapsto 0110,\ 11 \mapsto 0111$
$10(01)^\omega$	$00 \mapsto 1101,\ 01 \mapsto 1100,\ 10 \mapsto 1000,\ 11 \mapsto 1001$
1001^ω	$1000 \mapsto 10001101,\ 1001 \mapsto 10001100$
	$1100 \mapsto 10011100,\ 1101 \mapsto 10011101$
$0(110)^\omega$	$00 \mapsto 0111001001100010$
	$01 \mapsto 0111001001100011$
	$10 \mapsto 0111001101100010$
	$11 \mapsto 0111001101100011$

6 Algebraic description

We conclude our considerations by providing an algebraic characterization of automatic paperfolding sequences. In this section the finite and infinite words are identified with finite and infinite power series over $\mathbb{Z}_2$, respectively.

Theorem 23. *Let for* $n \geq 1$

$$\begin{aligned}\mathbf{b}_{(n)} &= [\mathbf{p}]_0^{2^n-1}0[\mathbf{p}]_{2^n}^{2^n-1}0 \\ \overline{\mathbf{b}}_{(n)} &= [\mathbf{p}]_0^{2^n-1}1[\mathbf{p}]_{2^n}^{2^n-1}1\end{aligned}$$

Then the sequence $\mathbf{p}$ *satisfies the equation*

$$\begin{aligned}(1+X)^{2^{p+q+1}}(X^{2^q-1}\mathbf{p}^{2^q}+\mathbf{p}) + (X^{2^q-1}\mathbf{b}_{(p)}^{2^q}+\mathbf{b}_{(p+q)}) = 0 \quad \textit{in case } \mathbf{A} \\ (1+X)^{2^{p+q+1}}(X^{2^q-1}\mathbf{p}^{2^q}+\mathbf{p}) + (X^{2^q-1}\mathbf{b}_{(p)}^{2^q}+\overline{\mathbf{b}}_{(p+q)}) = 0 \quad \textit{in case } \mathbf{B}\end{aligned} \tag{5}$$

Proof. We will use the knowledge of the regularity of the internal structure of k-blocks in $\mathbf{p}$ from Lemmas 6 and 13. The sequences $\mathbf{b}_{(n)}^\omega$,$\overline{\mathbf{b}}_{(n)}^\omega$ and the corresponding formal series $\mathbf{c}_{(n)} = (1+X)^{-2^{n+1}}\mathbf{b}_{(n)}$, $\overline{\mathbf{c}}_{(n)} = (1+X)^{-2^{n+1}}\overline{\mathbf{b}}_{(n)}$ differ from $\mathbf{p}$ just in the sequence of positions $\{k2^n-1\}_{k\geq 0}$, where $\mathbf{c}_{(n)}$ contains the symbol 0 and $\mathbf{c}_{(n)}$ contains 1. Lemma 13 implies $\{\mathbf{p}_{k2^p-1}\}_{k\geq 0} = \{\mathbf{p}_{k2^{p+q}-1}\}_{k\geq 0}$ in case $\mathbf{A}$, and $\{\mathbf{p}_{k2^p-1}\}_{k\geq 0} = \{\overline{\mathbf{p}}_{k2^{p+q}-1}\}_{k\geq 0}$ in case $\mathbf{B}$. Therefore $\{((\mathbf{c}_{(p)}+\mathbf{p})^{2^q})_{k2^{p+q}-2^q}\}_{k\geq 0} = \{(\mathbf{c}_{(p+q)}+\mathbf{p})_{k2^{p+q}-1}\}_{k\geq 0}$ in case $\mathbf{A}$, and

$\{((\mathbf{c}_{(p)} + \mathbf{p})^{2^q})_{k2^{p+q}-2^q}\}_{k\geq 0} = \{(\overline{\mathbf{c}}_{(p+q)} + \mathbf{p})_{k2^{p+q}-1}\}_{k\geq 0}$ in case **B**, and we have the equation

$$X^{2^q-1}((1+X)^{-2^{p+1}}\mathbf{b}_{(p)} + \mathbf{p})^{2^q} = (1+X)^{-2^{p+q+1}}\mathbf{b}_{(p+q)} + \mathbf{p} \quad \text{in case } \mathbf{A}$$
$$X^{2^q-1}((1+X)^{-2^{p+1}}\mathbf{b}_{(p)} + \mathbf{p})^{2^q} = (1+X)^{-2^{p+q+1}}\overline{\mathbf{b}}_{(p+q)} + \mathbf{p} \quad \text{in case } \mathbf{B}$$

which can be transformed to 5.

We are not able to say anything about optimality of equation (5). Let us just note that the sequence $\overrightarrow{\mathbf{p}} = 0\mathbf{p}$ satisfies the equation

$$(1+X)^{2^{p+q+1}}(\overrightarrow{\mathbf{p}}^{2^q} + \overrightarrow{\mathbf{p}}) + (\overrightarrow{\mathbf{b}}_{(p)}^{2^q} + \overrightarrow{\mathbf{b}}_{(p+q)}) = 0 \quad \text{in case } \mathbf{A}$$
$$(1+X)^{2^{p+q+1}}(\overrightarrow{\mathbf{p}}^{2^q} + \overrightarrow{\mathbf{p}}) + (\overrightarrow{\mathbf{b}}_{(p)}^{2^q} + \overline{\overrightarrow{\mathbf{b}}}_{(p+q)}) = 0 \quad \text{in case } \mathbf{B}$$

where

$$\overrightarrow{\mathbf{b}}_{(n)} = 0[\overrightarrow{\mathbf{p}}]_1^{2^{n-1}} 0[\overrightarrow{\mathbf{p}}]_{2^n+1}^{2^n-1}$$
$$\overline{\overrightarrow{\mathbf{b}}}_{(n)} = 1[\overrightarrow{\mathbf{p}}]_1^{2^{n-1}} 1[\overrightarrow{\mathbf{p}}]_{2^n+1}^{2^n-1}.$$

Example 5. The algebraic equations for the sequences from Example 2:

u	equation (5)
00^ω	$(1+X)^8(X\mathbf{p}^2 + \mathbf{p}) + (X^6 + X^2) = 0$
$10(01)^\omega$	$(1+X)^8(X\mathbf{p}^2 + \mathbf{p}) + \sum_{i\in S} X^i = 0$
	$S = \{0, 1, 3, 4, 5, 7\}$
1001^ω	$(1+X)^{32}(X\mathbf{p}^2 + \mathbf{p}) + \sum_{i\in S} X^i$
	$S = \{0, 1, 4, 5, 7, 8, 9, 12, 13, 16, 17, 20, 21, 23, 24, 25, 28, 29\}$
$0(110)^\omega$	$(1+X)^{32}(X^7\mathbf{p}^8 + \mathbf{p}) + \sum_{i\in S} X^i$
	$S = \{1, 2, 3, 6, 9, 10, 14, 17, 18, 19, 22, 25, 26, 30\}$

References

[Allouche 92] Allouche, J.-P.: "The number of factors in a paperfolding sequence"; Bull. Austral. Math. Soc., 46, (1992), 23-32.

[Allouche and Bousquet-Mélou 94] Allouche, J.-P., Bousquet-Mélou, M.: "Canonical positions for the factors in paperfolding sequences"; TCS (Theoretical Computer Science), 129, (1994), 263-278.

[Bercoff 95] Bercoff, C.: "A family of tag systems for paperfolding sequences (preliminary version)", Proceedings STACS'95, Springer LNCS 900, Heidelberg / New York, (1995), 303-312.

[Černý and Gruska 86] Černý, A., Gruska, J.: Modular trellises, In: The Book of L., (Rozenberg., G., and Salomaa, A., eds.), Springer, Heidelberg / New York, (1986), 45-60.

[Christol et al. 80] Christol, G., Kamae, T., Mendès-France, M., Rauzy, G.: Suites algébriques, automates et substitutions, Bull. Soc. Math. France, 108, (1980), 401-419.

[Cobham 69] Cobham, A.: On the base dependence of sets of numbers recognizable by finite automata, Math. Syst. Theory, 3, (1969), 186-192.

[Cobham 72] Cobham, A.: Uniform tag sequences, Math. Syst. Theory, 6, (1972), 164-192.

[Davis and Knuth 70] Davis, C., D. E. Knuth: Number representations and dragon curves, I, II, Journal of Recreational Math., 3, (1970), 161-181, 133-149.

[Koskas 96] Koskas, M.: About the p-paperfolding words, TCS (Theoretical Computer Science), 158, (1996), 35-51.

[Lehr 92] Lehr, S.: A result about languages concerning paperfolding sequences, Mat. Syst. Theory, 25, (1992), 309-313.

[Mendès-France and Shallit 89] Mendès-France, M., Shallit, J. O.: Wire bending, Journal of Combinatorial Theory, Series A 50, (1989), 1-23.

[Rodenhausen 95] Rodenhausen, A. M.: Paperfolding, generalized Rudin-Shapiro sequences, and the Thue-Morse sequence, Fractals, 3, 4 (1995), 679-688.

[Thue 06] Thue, A.: Ueber unendliche Zeichenreihen, Videnskabs-Selskabets Skifter, Math. Naturv. Klasse, Kristiania, 7, (1906), 1-22.

[Wen and Wen 92] Wen, Z.-X., Wen, Z.-Y.: Some studies on the (p, q)-type sequences, TCS (Theoretical Computer Science), 94 (1992), 373-393.

Acknowledgments

This work was supported by the grant No. MSV SR 1/4315 of the Slovak Ministry of Education and Science.