Finding automatic sequences with few correlations

Vincent Jugé   Irène Marcovici

Univ Gustave Eiffel,   Université de Lorraine,
CNRS, LIGM   CNRS, Inria, IECL
F-77454 Marne-la-Vallée,   Nancy
France   France
`vincent.juge@univ-eiffel.fr`   `irene.marcovici@univ-lorraine.fr`

Abstract

Although automatic sequences are very simple algorithmically, some of them have pseudo-random properties. In particular, some automatic sequences such as the Golay–Shapiro sequence are known to be 2-uncorrelated, meaning that they have the same correlations of order 2 as a uniform random sequence. However, the existence of ℓ-uncorrelated automatic sequences (for $\ell \geqslant 3$) was left as an open question in a recent paper of Marcovici, Stoll and Tahay. We exhibit binary block-additive sequences that are 3-uncorrelated and, with the help of analytical results supplemented by an exhaustive search, we present a complete picture of the correlation properties of binary block-additive sequences of rank $r \leqslant 5$, and ternary sequences of rank $r \leqslant 3$.

1 Introduction

A *k-automatic sequence* is a sequence that can be computed by a finite automaton in the following way: the n-th term of the sequence is a function of the state reached by the automaton after reading the representation of the integer n in base k. Alternatively, a k-automatic sequence can also be described with the help of an infinite fixed point of a k-uniform morphism (we refer to the book of Allouche and Shallit [2] for a complete survey on automatic sequences).

It is known that some automatic sequences present pseudo-random properties. In particular, a succession of works [3, 6, 4] has shown that different generalisations of the Golay–Shapiro sequence have the same correlations of order 2 as a sequence of symbols chosen uniformly and independently at random. On the other hand, as the subword complexity of an automatic sequence is at most linear, it is clear that automatic sequences cannot look "too much" like random sequences. In this work, we continue to address the question of "how random" an automatic sequence can look.

As in the references cited above, we focus on *block-additive* automatic sequences. They are obtained by sliding the representation of the integer n in base k with a window of length r, and summing the *weights* of the subwords read, for a given weight function. In [4], the existence of a block-additive sequence being ℓ-*uncorrelated* for an integer $\ell \geqslant 3$ (i.e., having the same correlations of order ℓ as a uniform random sequence) was left as an open question. We prove that, when ℓ is even, a binary block-additive sequence is ℓ-uncorrelated if and only if it is $(\ell + 1)$-uncorrelated. As a consequence, all the binary sequences that are known to be 2-uncorrelated are also 3-uncorrelated. We also present a semi-decision algorithm providing a criterion for being

ℓ-*correlated.* With the help of this algorithm, an exhaustive search allows us to obtain a complete description of the correlation properties of binary block-additive sequences of rank $r \leqslant 5$, and ternary sequences of rank $r \leqslant 3$.

2 Definitions and presentation of the results

Below, let $\mathbb{N}$ denote the set of non-negative integers. For all integers $k \geqslant 0$, let Σ_k denote the set $\{0, 1, \ldots, k-1\}$ and let $\mathbb{Z}_k$ denote the set $\mathbb{Z}/k\mathbb{Z}$. For all finite sets $\mathscr{S}$, let $|\mathscr{S}|$ denote the cardinality of $\mathscr{S}$, i.e., the number of elements of $\mathscr{S}$.

   In general, let $\mathbf{0}$ (resp., $\mathbf{1}$) denote a tuple whose coordinates are all equal to 0 (resp., to 1), and let $\mathbf{1}_i$ denote a tuple whose i-th coordinate is 1 and the other coordinates are 0; the dimension of the tuple is left implicit. Moreover, given a sequence $(u_n)_{n \geqslant 0}$ and a tuple $\boldsymbol{\delta} = (\delta_1, \delta_2, \ldots, \delta_\ell)$ of non-negative integers, let $u_{n+\boldsymbol{\delta}}$ denote the tuples $(u_{n+\delta_1}, u_{n+\delta_2}, \ldots, u_{n+\delta_\ell})$. We also say that $\boldsymbol{\delta}$ is *increasing* if $\delta_1 < \delta_2 < \cdots < \delta_\ell$.

   Finally, for all integers $n \geqslant 0$ and $k \geqslant 1$, let $(n \bmod k)$ denote the unique element $x \in \Sigma_k$ such that k divides $n - x$. If $k \geqslant 2$, let also $\langle n \rangle_k$ denote the representation of n in base k, i.e., the unique sequence $(x_i)_{i \geqslant 0}$ with values in Σ_k such that

$$n = \sum_{i \geqslant 0} x_i k^i.$$

Definition 1. Let $k \geqslant 2$ and $r \geqslant 1$ be integers, and let $f \colon \Sigma_k^r \to \mathbb{Z}_k$ be a function such that $f(\mathbf{0}) = 0$. For all $n \geqslant 0$, let also u_n be the element of $\mathbb{Z}_k$ defined by

$$u_n = \sum_{i \geqslant 0} f(x_i, x_{i+1}, \ldots, x_{i+r-1}),$$

where $(x_i)_{i \geqslant 0} = \langle n \rangle_k$. The sequence $(u_n)_{n \geqslant 0}$ is said to be *block-additive* in base k with rank r, and we say that this sequence is *associated* with the function f.

   The block-additive sequence $(u_n)_{n \geqslant 0}$ associated with a function f also has the following characterisation.

Remark 2. Let $\mathscr{A}$ be the automaton over the alphabet Σ_k with state set $Q = \mathbb{Z}_k \times \Sigma_k^{r-1}$, initial state $q_0 = (0, \mathbf{0})$ and transition function $\Delta \colon Q \times \Sigma_k \to Q$ defined by

$$\Delta \colon ((v, (x_1, x_2, \ldots, x_{r-1})), i) \to (v + f(i, x_1, x_2, \ldots, x_{r-1}), (i, x_1, x_2, \ldots, x_{r-2})).$$

The value of u_n is obtained by letting the automaton $\mathscr{A}$ read *from right to left* the infinite word $(x_i)_{i \geqslant 0} = \langle n \rangle_k$: $\mathscr{A}$ goes through each tuple $(x_i, x_{i+1}, \ldots, x_{i+r-1})$, stores the first $r - 1$ coordinates $(x_i, x_{i+1}, \ldots, x_{i+r-2})$ of that tuple and accumulates, in the first component of each state, the values of $f(x_i, x_{i+1}, \ldots, x_{i+r-1})$ it encounters.

   Let $\phi \colon Q^* \to Q^*$ be the morphism of monoids that sends a state $s \in Q$ to the word $\phi(s) = \Delta(s, 0)\Delta(s, 1) \ldots \Delta(s, k-1) \in Q^k$. Projecting on their first component the letters of the infinite fixed-point $\phi^\omega(q_0) \in Q^{\mathbb{N}}$ provides us with the infinite word $u_0 u_1 u_2 \ldots$, which we identify with the sequence $(u_n)_{n \geqslant 0}$ itself. The automaton $\mathscr{A}$ is said to *generate* the sequence $(u_n)_{n \geqslant 0}$.

Definition 3. Let $\ell \geqslant 1$ be an integer and let $\mathscr{S}$ be a finite set. Given a sequence $\mathbf{u} = (u_n)_{n \geqslant 0}$ with values in $\mathscr{S}$, an increasing tuple $\boldsymbol{\delta} \in \mathbb{N}^\ell$ and a subset $\mathbf{S}$ of $\mathscr{S}^\ell$ called a *pattern*, let $\mathscr{D}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{S})$ denote the set $\{n \in \mathbb{N} \colon u_{n+\boldsymbol{\delta}} \in \mathbf{S}\}$.

We define the *frequency* of the pattern $\mathbf{S}$ in the sequence $(u_{n+\boldsymbol{\delta}})_{n \geqslant 0}$ as the real number

$$\mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{S}) = \lim_{N \to +\infty} \frac{|\mathscr{D}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{S}) \cap \Sigma_N|}{N},$$

when this limit exists.

Note that, if the automaton $\mathscr{A}$ that generates $\mathbf{u}$ is strongly connected, the sequence $\mathbf{u}$ is a morphic primitive sequence, which ensures that all the densities are well-defined.

We say that $\mathbf{u}$ is *ℓ-uncorrelated* if $\mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{S}) = |\mathbf{S}|/|\mathscr{S}|^\ell$ for all tuples $\boldsymbol{\delta}$ and all sets $\mathbf{S} \subseteq \mathscr{S}^\ell$. Otherwise, we say that $\mathbf{u}$ is *ℓ-correlated*.

A sequence whose terms are chosen independently and uniformly at random in $\mathbb{Z}_n$ is almost-surely ℓ-uncorrelated for every integer $\ell \geqslant 0$. However, no automatic sequence, and in particular no block-additive sequence, can be ℓ-uncorrelated for every $\ell \geqslant 0$, since this would in particular require the sequence to be normal, while the subword complexity of an automatic sequence is at most linear.

3 Correlations, block-additivity and base 2

It follows from Remark 2 that, if the automaton $\mathscr{A}$ that generates the block-additive sequence $\mathbf{u}$ is strongly connected, all the letters of Σ_k (i.e., patterns of length 1) have a well-defined frequency in $\mathbf{u}$. Furthermore, this frequency is equal to $1/k$. Indeed, each state in Q is the target of k edges from $\mathscr{A}$, so that the uniform probability measure on Q is the unique stationary measure of the Markov chain associated to $\mathscr{A}$, where each edge has weight $1/k$. We extend this argument to prove that this property still holds for the subsequences of $\mathbf{u}$ of the form $(u_{a+k^b n})_{n \geqslant 0}$, as stated in the lemma below.

Lemma 4. *Let $(u_n)_{n \geqslant 0}$ be a block-additive sequence in base $k \geqslant 2$ whose generating automaton is strongly connected. For all integers $a \geqslant 0$, $b \geqslant 0$ and all $s \in \mathbb{Z}_k$,*

$$\lim_{N \to +\infty} \frac{|\{n \in \Sigma_N \colon u_{a+k^b n} = s\}|}{N} = \frac{1}{k}.$$

We now use this lemma to provide the following characterisation of ℓ-uncorrelated block-automatic sequences.

Proposition 5. *Let $\mathbf{u} = (u_n)_{n \geqslant 0}$ be a block-additive sequence in base $k \geqslant 2$, and let $\ell \geqslant 2$ be an integer. The sequence $\mathbf{u}$ is ℓ-uncorrelated if and only if*

$$\mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{s} + \mathbb{Z}_k \mathbf{1}) = \frac{1}{k^{\ell-1}}$$

for all increasing tuples $\boldsymbol{\delta} \in \mathbb{N}^\ell$ such that $\delta_1 = 0$ and all tuples $\mathbf{s} \in \mathbb{Z}_k^\ell$, where $\mathbf{s} + \mathbb{Z}_k \mathbf{1}$ denotes the set $\{\mathbf{s} + x \mathbf{1} \colon x \in \mathbb{Z}_k\}$.

Sketch of the proof. The "only if" part is a direct consequence of Def. 3. Thus, we focus on the "if" part. Let $\mathbf{u}$ be a sequence that meets the requirements of Prop. 5. We wish to prove that $\mathbf{u}$ is ℓ-correlation free.

First, we prove that the automaton $\mathscr{A}$ that generates $\mathbf{u}$ is strongly connected. To do this, it is sufficient to show that, for all $x \in \mathbb{Z}_k$, the state $(x, \mathbf{0})$ is accessible from the initial state $q_0 = (0, \mathbf{0})$. Using the assumption that $\mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{s} + \mathbb{Z}_k \mathbf{1}) > 0$, with $\boldsymbol{\delta} = (0, k^r, 2k^r, \ldots, (\ell-1)k^r)$ and $\mathbf{s} = \mathbf{1}_1$, we obtain the desired result.

The rest of proof is based on the following idea. Let $\boldsymbol{\delta} = (\delta_1, \delta_2, \ldots, \delta_\ell) \in \mathbb{N}^\ell$ be an increasing tuple, let $\mathbf{s} = (s_1, s_2, \ldots, s_\ell)$ be an element of $\mathbb{Z}_k^\ell$, and r be the rank of $\mathbf{u}$. We aim at proving that $\mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\{s\}) = k^{-\ell}$. Since the sets $\mathscr{D}_{\boldsymbol{\delta}}^{\mathbf{u}}(\{s\})$ and $\mathscr{D}_{\boldsymbol{\delta} - \delta_1 \mathbf{1}}^{\mathbf{u}}(\{s\})$ are translated versions of each other, we assume without loss of generality that $\delta_1 = 0$. For each integer $n \in \mathbb{N}$ with representation $(x_i)_{i \geqslant 0} = \langle n \rangle_k$ in base k, the value of the tuple $u_{n+\boldsymbol{\delta}} - u_n \mathbf{1}$ depends only on the terms $x_0, x_1, \ldots, x_{m+r-1}$, where m is the least integer such that $\lfloor n/k^m \rfloor = \lfloor (n + \delta_\ell)/k^m \rfloor$, and is called the *carry distance* of n.

By assumption, if N is large enough, approximately $k^{N+r-\ell}$ integers $a \in \Sigma_{k^{N+r-1}}$ belong to $\mathscr{D}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{s} + \mathbb{Z}_k \mathbf{1})$. Very few of these integers have a carry distance larger than N; for each remaining integer a, Lemma 4 ensures that approximately $1/k$ of the integers $n \in \mathbb{N}$ that are such that $(n \bmod k^{N+r-1}) = a$ satisfy $u_n = s_1$. These integers n belong to $\mathscr{D}_{\boldsymbol{\delta}}^{\mathbf{u}}(\{s\})$, and thus $\mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\{s\}) \geqslant k^{-\ell}$. This inequality being valid for all $\mathbf{s}$, it is an equality, and we conclude that $\mathbf{u}$ is ℓ-uncorrelated. $\square$

Theorem 6. *Let ℓ be an even positive integer and let $(u_n)_{n \geqslant 0}$ be a block-additive sequence in base 2. This sequence is ℓ-uncorrelated if and only if it is $(\ell + 1)$-uncorrelated.*

Proof. First, every $(\ell + 1)$-uncorrelated sequence is clearly ℓ-uncorrelated. Conversely, let $\mathbf{u}$ be an ℓ-uncorrelated block-additive sequence in base 2, let $\boldsymbol{\delta} \in \mathbb{N}^{\ell+1}$ be an increasing tuple, and let $\mathbf{s}$ be an element of $\mathbb{Z}_2^{\ell+1}$. Let $|\mathbf{s}|_1$ denote the number of coordinates 1 in the tuple $\mathbf{s}$.

Since $\mathbf{u}$ is ℓ-uncorrelated, we know that $\mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{s}) + \mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{s} + \mathbf{1}_i) = 2^{-\ell}$ for all tuples $\mathbf{s}$ and all integers $i \leqslant \ell + 1$. Hence, and since $\ell + 1$ is odd, an immediate induction on $|\mathbf{s}|_1$ proves that $\mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\{\mathbf{s}\}) = \mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\{\mathbf{0}\})$ if $|\mathbf{s}|_1$ is even, and that $\mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\{\mathbf{s}\}) = \mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\{\mathbf{1}\})$ otherwise. It follows that

$$\mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{s} + \mathbb{Z}_2 \mathbf{1}) = \mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbb{Z}_2 \mathbf{1}) = 2^{-\ell}$$

for all $\mathbf{s} \in \mathbb{Z}_2^{\ell+1}$, and Prop. 5 then proves that $\mathbf{u}$ is $(\ell + 1)$-uncorrelated. $\square$

We prove now, by giving two examples, that the conclusions of Theorem 6 are no longer ensured if ℓ is odd or if $(u_n)_{n \geqslant 0}$ is block-additive in a base $k \geqslant 3$.

Example 7. Let $(u_n)_{n \geqslant 0} \in \Sigma_2^{\mathbb{N}}$ be the block-additive sequence associated with the function $f \colon \Sigma_2^2 \mapsto \mathbb{Z}_2$ defined by $f(x_1, x_2) = x_1 x_2$. This sequence is known as the *Golay–Shapiro sequence* (see [1] for precisions on the origin of this sequence). The sequence $(u_n)_{n \geqslant 0}$ is both 3-uncorrelated and 4-correlated.

Proof. It is known (see [5] and the subsequent generalisations [3, 6, 4]) that $(u_n)_{n \geqslant 0}$ is 2-uncorrelated, and thus Theorem 6 proves it is also 3-uncorrelated. Consider the

tuples $\boldsymbol{\delta} = (0,1,2,3) \in \mathbb{N}^4$ and $\mathbf{s} = (0,0,0,1) \in \mathbb{Z}_2^4$. Let $(x_i)_{i\geqslant 0} = \langle n \rangle_2$ be the representation of an integer n in base 2. If $n \in 8\mathbb{N}$, i.e., if $x_0 = x_1 = x_2 = 0$, one checks that

$$u_n = u_{n+1} = u_{n+2} = u_{n+3} - 1 = \sum_{i\geqslant 3} x_i x_{i+1}.$$

This shows that $u_{n+\boldsymbol{\delta}} = \mathbf{s} + u_n \mathbf{1}$, i.e., that $n \in \mathscr{D}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{s} + \mathbb{Z}_2 \mathbf{1})$. One checks similarly that $n \in \mathscr{D}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{s} + \mathbb{Z}_2 \mathbf{1})$ if $n \in 16\mathbb{N} + 11$. Hence, $\mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{u}}(\mathbf{s} + \mathbb{Z}_2 \mathbf{1}) \geqslant 3/16 > 2^{-3}$, so that $(u_n)_{n\geqslant 0}$ is 4-correlated. $\square$

Example 8. Let $(v_n)_{n\geqslant 0} \in \Sigma_3^{\mathbb{N}}$ be the block-additive sequence associated with the function $f \colon \Sigma_3^2 \mapsto \mathbb{Z}_3$ defined by $f(x_1, x_2) = x_1 x_2$. The sequence $(v_n)_{n\geqslant 0}$ is both 2-uncorrelated and 3-correlated.

Proof. It is known (same references as above) that $(v_n)_{n\geqslant 0}$ is 2-uncorrelated. Consider the tuple $\boldsymbol{\delta} = (0,1,2) \in \mathbb{N}^3$, and let $(x_i)_{i\geqslant 0} = \langle n \rangle_3$ be the representation of an integer n in base 3. If $n \in 9\mathbb{N}$, i.e., if $x_0 = x_1 = 0$, one checks that

$$u_n = u_{n+1} = u_{n+2} = \sum_{i\geqslant 2} x_i x_{i+1},$$

which proves that $n \in \mathscr{D}_{\boldsymbol{\delta}}^{\mathbf{v}}(\mathbb{Z}_3 \mathbf{1})$. One checks similarly that $n \in \mathscr{D}_{\boldsymbol{\delta}}^{\mathbf{v}}(\mathbb{Z}_3 \mathbf{1})$ if $n \in 27\mathbb{N} + 1$. Hence, $\mathsf{freq}_{\boldsymbol{\delta}}^{\mathbf{v}}(\mathbb{Z}_3 \mathbf{1}) \geqslant 4/27 > 3^{-2}$, so that $(v_n)_{n\geqslant 0}$ is 3-correlated. $\square$

4 Detecting correlations

In this section, we focus on the following problem. Given an integer $\ell \geqslant 1$ and a block-additive sequence $\mathbf{u} = (u_n)_{n\geqslant 0}$ in base $k \geqslant 2$, is $\mathbf{u}$ ℓ-correlated? We provide two partial results. First, we propose an algorithm for detecting ℓ-correlations, when they exist. This algorithm extends the method used for the sequences of Examples 7 and 8. Second, we propose a criterion that is sufficient for being 2- or 3-uncorrelated when $k = 2$.

Theorem 9. *Algorithm 1 is a semi-decision algorithm for deciding if a given block-additive sequence is ℓ-correlated. More precisely, when given integers $k \geqslant 2$, $r \geqslant 1$, $\ell \geqslant 1$ and a function $f \colon \Sigma_k^r \to \mathbb{Z}_k$ such that $f(\mathbf{0}) = 0$ as input, Algorithm 1 eventually returns **true** if the block-additive sequence $(u_n)_{n\geqslant 0}$ associated with f is ℓ-correlated, and runs forever otherwise.*

Conversely, a *difference condition*, sufficient for ensuring that a binary block-additive sequence of rank $r = 2$ is 2-uncorrelated, was developed in [4]. Below, we extend that condition, and make it both necessary and sufficient.

Theorem 10. *Let $k \geqslant 2$, $r \geqslant 1$ and $\ell \geqslant 1$ be integers, let $f \colon \Sigma_k^r \to \mathbb{Z}_k$ be a function such that $f(\mathbf{0}) = 0$, and let $\mathbf{u} = (u_n)_{n\geqslant 0}$ be the block-additive sequence associated with f.*

1. *If $k = 2$, $r = 3$ and $2 \leqslant \ell \leqslant 3$, the sequence $\mathbf{u}$ is ℓ-uncorrelated if and only if it satisfies one of the criteria C_1 or C_2 below.*

```
┌──────────────────────────────────────────────────────────────────────────┐
│ Algorithm 1: Detecting ℓ-correlations in block-additive sequences          │
├──────────────────────────────────────────────────────────────────────────┤
│   Input  : Integers k ⩾ 2, r ⩾ 1 and ℓ ⩾ 1.                                │
│             Function f : Σ_k^r → ℤ_k such that f(0) = 0.                    │
│   Result : true if the block-additive sequence (u_n)_{n⩾0} associated      │
│             with f is ℓ-correlated.                                         │
└──────────────────────────────────────────────────────────────────────────┘
```

Algorithm 1: Detecting ℓ-correlations in block-additive sequences

Input : Integers $k \geqslant 2$, $r \geqslant 1$ and $\ell \geqslant 1$.
Function $f \colon \Sigma_k^r \to \mathbb{Z}_k$ such that $f(\mathbf{0}) = 0$.

Result : **true** if the block-additive sequence $(u_n)_{n\geqslant 0}$ associated with f is ℓ-correlated.

1 **for** $m = 1, 2, 3, \ldots$:
2   **for** all increasing tuples $\boldsymbol{\delta} = (\delta_1, \ldots, \delta_\ell) \in \mathbb{N}^\ell$ such that $\delta_1 = 0$ and $\delta_\ell \leqslant m$:
3   **for** all ℓ-tuples $\mathbf{s} = (s_1, \ldots, s_\ell) \in \mathbb{Z}_k^\ell$ such that $s_1 = 0$:
4        $\mathsf{c}(\mathbf{s}) \leftarrow 0$
5   **for** $n = 0, 1, \ldots, k^{m+r} - 1$:
6   **if** $(n \bmod k^m) \in \Sigma_{k^m - m}$:
7          $\mathbf{s} \leftarrow u_{n+\boldsymbol{\delta}} - u_n \mathbf{1}$
8          $\mathsf{c}(\mathbf{s}) \leftarrow \mathsf{c}(\mathbf{s}) + 1$
9   **if** $\mathsf{c}(\mathbf{s}) > k^{m+r+1-\ell}$:
10   **return true**

C_1 $f(0,0,0) + f(1,0,0) + f(0,1,0) + f(1,1,0) = 1$ *and either*

- $f(a,b,c) = f(a,b,0)$ *for all* $(a,b,c) \in \mathbb{Z}_2^3$ *or*
- $f(a,b,c) = f(a,b,0) + c$ *for all* $(a,b,c) \in \mathbb{Z}_2^3$;

C_2 $f(0,b,0) + f(1,b,0) + f(0,b,1) + f(1,b,1) = 1$ *for all* $b \in \mathbb{Z}_2$.

2. *If* $k = 2$, $r \leqslant 5$ *and* $\ell \geqslant 4$, *the sequence* $\mathbf{u}$ *is* ℓ-*correlated.*

3. *If* $k = 3$, $r = 3$ *and* $\ell \geqslant 3$, *the sequence* $\mathbf{u}$ *is* ℓ-*correlated.*

Sketch of proof. Conditions C_1 and C_2 extend the difference condition of [4] to block-additive sequences of rank $r = 3$. Using the techniques developed in that article, we obtain that, under these conditions, the sequence is 2-uncorrelated (and, due to Theorem 6, also 3-uncorrelated). A priori, these conditions are only sufficient. But since there are only a finite number of functions $f \colon \Sigma_2^3 \to \mathbb{Z}_2$, we can use Algorithm 1 to exclude the other sequences. In practice, Algorithm 1 indeed allows us to show that all the sequences of rank 3 that do not satisfy Conditions C_1 and C_2 are 2-correlated, thereby proving point 1. In the same way, points 2. and 3. are proved experimentally using Algorithm 1. □

For the sake of simplicity, we have focused on one-dimensional automatic sequences. Note, however, that all our results extend to multi-dimensional block-additive sequences. In particular, Theorem 6 implies that the multi-dimensional binary block-additive sequences that are known to be 2-uncorrelated are also 3-uncorrelated.

Theorem 10 shows that block-additive binary sequences of relatively small rank are 4-correlated. We thus leave as an open question the existence of 4-uncorrelated automatic sequences. Also, Algorithm 1 is only a semi-decision algorithm for detecting if a given block-additive sequence is ℓ-correlated, and developing a proper decision algorithm to completely answer the question is still a challenge.

References

[1] Jean-Paul Allouche. On a Golay-Shapiro-like sequence. *Unif. Distrib. Theory*, 11(2):205–210, 2016.

[2] Jean-Paul Allouche and Jeffrey Shallit. *Automatic sequences.* Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations.

[3] Elyot Grant, Jeffrey Shallit, and Thomas Stoll. Bounds for the discrete correlation of infinite sequences on k symbols and generalized Rudin-Shapiro sequences. *Acta Arith.*, 140(4):345–368, 2009.

[4] Irène Marcovici, Thomas Stoll, and Pierre-Adrien Tahay. Discrete correlations of order 2 of generalized Golay-Shapiro sequences: a combinatorial approach. *Integers*, 21:paper a45, 21, 2021.

[5] Martine Queffélec. Une nouvelle propriété des suites de Rudin-Shapiro. *Ann. Inst. Fourier (Grenoble)*, 37(2):115–138, 1987.

[6] Pierre-Adrien Tahay. Discrete correlation of order 2 of generalized Rudin-Shapiro sequences on alphabets of arbitrary size. *Unif. Distrib. Theory*, 15(1):1–26, 2020.