**Synthetic pseudo-random sequence**

**A A Tsatsin**

Moscow research and production complex "Avionika" named after O.V. Uspenskiy, 7 Obraztsova, Moscow 127055, Russia

sand_e@mail.ru

**Abstract.** The paper considers the basic information about a new class of pseudo-random sequences — the class of synthetic pseudo-random sequences. The main distinguishing feature of the sequences under consideration is the extended observation window. The proposed synthetic sequences are an extension of the area of existing pseudo-random sequences.

1. **Introduction**

Pseudo-random sequences (PRS) are widely used in modern communication systems, positioning systems, and instrumentation systems. Linear PRS: Gold sequences, Kasami sequences, M-sequences, and nonlinear PRS: de Bruijn sequences, GMW sequences and etc., are most widely used.

One application of pseudo-random sequences in instrumentation is the formation of digital encoder scales. The scales of binary single-track digital encoders, for example, based on the M-sequence [1], the de Bruijn sequence (T-sequence) [2], are based on one of the main properties of the PRS — the «window» of observation [3, 4]. The «window» property is that if a window from the number of neighboring characters, the width of which corresponds to the bit depth of the scale, is moved along the PSP period, then only unique combinations of numbers will be observed in this window [5].

This paper considers a new class of pseudo-random sequences with an extended observation window.

2. **Basic information**

To preserve the «window» property in full, i.e. to cover all possible unique combinations of codes, the maximum length of the numeric sequence \( S_N \) in the number system with base \( b \) for a given bit width \( m \) must be determined by the expression from combinatorics, as «placement with repetition»:

\[
S_N(b) = b^m.
\]

For parametric estimation of window introduces parameter extend the window of observation \( k_w \) — shift between adjacent assesses the elements of the observation window [6].

Existing classical pseudo-random sequences have a window of observation that evaluates neighboring quanta of the code scale (Figure 1). The extended observation window has the form (Figure 2).

One of the possible solutions to preserve the main "window" property is to synthesize special synthetic pseudo-random sequences with an extended observation window.
In [6], the concepts of aliquot and synthetic sequences are introduced and operations over them are described.

**Aliquot sequences** — a set of \( n \) cyclic sequences of length \( N_A \) with the observation window parameter \( k_w = 1 \), which correspond to \( n \) disjoint contours of the de Bruijn graph of order \( N_S = N_A \cdot n \), containing all the vertices of the graph.

**Synthetic sequence** — a pseudo-random sequence of length \( N_S \) with an observation window parameter \( k_w = n \), obtained by performing a merge operation on a set of \( n \) aliquot sequences of length \( N_A = N_S / n \).

Figure 3 shows an example of a de Bruijn graph (\( G_b \) graph) of order \( N_S = 8 \), corresponding to a given bit width \( m = 3 \) for \( b = 2 \) [7].

![Figure 3](image)

**Figure 3.** \( G_S \) — graph for \( b = 3, m = 3 \).

In the graph \( G_b \), two disjoint contours are highlighted in red and blue. For contours starting from vertices with numbers 1 and 3, we apply the division operation modulo 2 to the vertex numbers of the contours. We get two aliquot cyclic binary \( A \)-sequences:

\[
A_1^2 = \{1000\}, \quad A_2^2 = \{1101\}.
\]

After performing the merge operation [6] on the existing aliquot sequences, we get a synthetic pseudo-random sequence:

\[
S_2^2(3) = \left\{ A_1^2 A_2^2 \right\} = \{11010001\}.
\]

This synthetic pseudorandom sequence has the window extend parameter \( k_w = 2 \) (see Figure 2). If such an extended window is moved along the received PRS, then in accordance with expression (1), with the accepted parameter values \( (m=3, b=2) \), we will observe eight unique codes. This confirms that the properties of the "window" are preserved when it is extended.

The example also shows that the parameter \( k_w \) has a dual role. It is the aliquot coefficient, i.e. how many of \( A \)-sequences a synthetic \( S \)-sequence consists of.

Note that in accordance with the definitions of multiple and synthetic sequences introduced, pseudo-random de Bruijn sequences [7] must be considered as a special case of synthetic pseudorandom sequences. This position follows from the extended interpretation of the theory of pseudorandom sequences considered in [6] and the corresponding extension of the theory of the conceptual apparatus.

Synthetic pseudorandom sequences longer than \( N_S \geq 32 \) characters are of more interest (table 1).
Table 1. Examples of binary $A$- and $S$-sequences, $N_s = 32$.

| №  | $k_w$ | $A$-sequence | $S$-sequence |
|----|-------|--------------|--------------|
| 1  | 1     | 000001000110010011101011  | 00000100011001001110101111011111  |
|    |       | 111111       | 11           |
| 2  | 2     | 0000011000110011101011  | 00100010111100010111011110001001 |
|    |       | 0101110011111111     | 11           |
| 3  | 4     | 00011011       | 0001001111    |
|    |       | 00110111       | 10           |
|    |       | 11111010       |              |

* de Bruijn sequence.

Table 1 shows that for the same length, there are synthetic pseudo-random $S$-sequences that are based on sequences of different aliquot. In this case, all the given $S$-sequences are different, and they retain the "extended window" property.

Further research has shown that synthetic pseudo-random sequences can be obtained for other number systems (ternary, quaternary, etc.).

The most complete conceptual apparatus of open synthetic pseudorandom sequences is described in [6].

3. Summary

Thus, the article considers a new class of pseudorandom sequences — synthetic pseudorandom sequences. The main distinguishing feature of the sequences under consideration is the extended observation window. The discovery of sequences of this class significantly complements the theory of pseudorandom sequences, and allows us to expand scientific research in this area.

References

[1] Ozhiganov A A, Pribytkin P A, Pavlov V V et al Patent RF № 2510572 29.10.2012 Psevdosluchaynaya kodovaya shkala 27.03.2014 No 9
[2] Tsatsin A A 2017 Metod formirovaniya T-posledovateľnostey dlya odnokoordinatnykh tsifrovych datchikov peremeshcheniy Materialy IV nauchno-prakticheskoy konferentsii pamiati O V Uspenskogo (Moscow: Izdatel'skiy dom Akademii N Ye Zhukovskogo) p 54
[3] Fredricsson S A 1975 Pseudo-Randomness Properties of Binary Shift Register Sequences IEEE Trans. Inform. Theory 21 115–20
[4] Blackburn S A Note on Sequences with the Shift and Add Property 1996 Designs, Codes, and Crypt. 9 251–6
[5] MacWilliams J F and Sloane Neil J 1976 A Pseudo-Random Sequences and Arrays Proc. of The IEEE 64 12
[6] Tsatsin A A Sinteticheskiye psevdosluchayanye posledovateľnosti dlya datchikov polozheniya 2019 Pribyl 11 (233) 21–8
[7] de Bruijn N G 1946 A combinatorial problem (Koninklijke Nederlandse Akademie van Wetenschappen) 49 758–64