Kybernetika

Ludvík Prouza

On a method of detection of nonperiodic pseudonoise binary sequences

Kybernetika, Vol. 20 (1984), No. 4, 314--321

Persistent URL: http://dml.cz/dmlcz/124828

KYBERNETIKA — VOLUME *20* (1984), NUMBER 4

ON A METHOD OF DETECTION OF NONPERIODIC PSEUDONOISE BINARY SEQUENCES

LUDVÍK PROUZA

A correlation method of rapid acquisition (and reception) of periodic pseudonoise (maximum length) binary sequences (PNBS) is modified for a single period of such sequences.

1. INTRODUCTION

In [2], [3], [4] variations of a general crosscorrelation method have been proposed for acquisition and reception of PNBS in communications application. The method is based on that a PNBS is generated by a shift register with binary feedback. Only so-called maximum length sequences have been investigated in cited references and also in the present article, where the concern is concentrated on modification of the method to the detection of a single period of PNBS.

A local replica of the received sequence which is to be crosscorrelated with it is, in this method, replaced by the output sequence of an "open" shift register (identical with the one used in the transmitter but without feedback).

This output sequence is crosscorrelated with the register input sequence. Since all cyclic permutations of a given shift-register PNBS can be generated (changing the initial conditions) by the same register, the behaviour of the method is dependent only on the register and not on the concrete generated sequence.

Thus the principal advantage of the method is that only the knowledge of the shift register generator and of the sequence rate are needed in the receiver, the transmitter and receiver clocks phase difference being resolved in obvious way by multiplexing.

2. THE DETECTION SCHEMA

A possible rudimentary detection schema, containing both the transmitter and the receiver, is given in the following figure, and is useful especially for Monte Carlo simulations.

In Fig. 1, the part on the left of the broken line represents the transmitter and all noise sources, the part on the right represents the receiver. TLSR and RLSR are resp. transmitter and receiver linear shift registers, NG is a noise generator, Σ is a summing block. Blocks T_1 and T_2 are arranged in the schema for convenience, performing the transforms described in what follows. The binary feedback of TLSR is only symbolically sketched. SGN means the usual signum operation, D is a decision block. There holds ($\oplus$ denotes addition modulo 2)

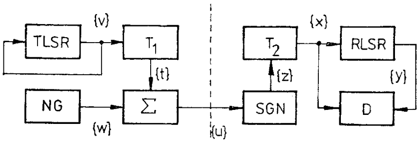

Fig. 1.

(1) $$v_i = v_{i-k} \oplus v_{i-l} \oplus \ldots \oplus v_{i-s}\,,$$
$$i > k, l, s > 1\,,$$

according to the generator schema used,

(2) $$t_i = 2v_i - 1$$

(3) $$u_i = t_i + w_i$$

where the noise sequence $\{w\}$ is white Gaussian $N(0, 1)$,

(4) $$z_i = \operatorname{sign} u_i\,,$$

(5) $$x_i = (z_i + 1)/2\,,$$

(6) $$y_i = x_{i-k} \oplus x_{i-l} \oplus \ldots \oplus x_{i-s}$$

(i, k, l, s the same as in (1)).

As decision rule only iterations of coincidences of x_i, y_i will be considered in what follows.

3. A SIMPLE CASE OF DETECTION

Suppose that both shift registers possess n stages, thus the sequence $\{v\}$ possesses $N = 2^n - 1$ terms.

Let at the beginning the whole schema be empty. Successively, the initial n bits are filled in TLSR, its output transformed in T_1 and added in Σ with noise, the s/n ratio being given by the magnitude K of the output of T_1. Thus

(7) $$\mathrm{s}/n = K^2\,.$$

From the schema there is clear that

$$(8) \qquad p(x_i = 1 \mid v_i = 1) = p(x_i = 0 \mid v_i = 0) = \Phi(K) = p\,,$$
$$p(x_i = 0 \mid v_i = 1) = p(x_i = 1 \mid v_i = 0) = 1 - \Phi(K) = q\,,$$

where Φ is the tabulated $N(0, 1)$ distribution function. Especially for $K = 0$, $p = q = \frac{1}{2}$.

Let in this simple case the following decision rule hold: in the decision block, the first n pairs (x_i, y_i) are not respected and the PNBS will be decided to be present if (and only if) the for following

$$(9) \qquad i = n + 1, n + 2, \ldots, N = 2^n - 1$$

the coincidence

$$(10) \qquad y_i = x_i$$

holds.

Theorem 1. For the above decision rule, the probability of the sequence detection is

$$(11) \qquad P_d = p^{(N-1)/2}(p^{(N+1)/2} + Nq^{(N+1)/2})\,.$$

Proof. a) There is clear that for given $\{v_1, \ldots, v_N\}$ the sequence $\{x_1, \ldots, x_N\}$ is a sequence of independent events, thus

$$(12) \qquad P(x_1, \ldots, x_N) = p(x_1) \ldots p(x_N)\,,$$

where from (8)

$$(13) \qquad \begin{aligned} p(x_i) &= p \quad \text{for} \quad x_i = v_i \\ &= q \quad \text{for} \quad x_i = 1 - v_i \\ &\quad (i = 1, \ldots, N)\,. \end{aligned}$$

Thus the probability in (12) is $p^r q^{N-r}$, where $0 \leqq r \leqq N$ is the number of coincidences $x_i = v_i$ $(i = 1, \ldots, N)$.

Being given $\{v_1, \ldots, v_N\}$, there are $\binom{N}{r}$ possibilities to arrange $\{x_1, \ldots, x_N\}$ so to get r coincidences $x_i = v_i$ and the sum probability is $\binom{N}{r} p^r q^{N-r}$, thus the probability distribution of coincidences is binomial, the total number of arrangements of $\{x_1, \ldots, x_N\}$ is 2^N and the total probability is 1.

b) The natural ordering of the set of 2^N N-places binary numbers according to their magnitude is divided in 2^n (n the register "lenght") subsets, in each the first n places $x_1, \ldots, x_n$ are not changing and only the remaining $N - n$ terms change, the number of changes being 2^{N-n} (and this is the number of numbers in the subset).

Now, one will seek in each subset all $\{x_1, \ldots, x_N\}$ for which (9), (10) hold. Finding it in all 2^n subsets and adding the probabilities thereof (in the original binary distribution), one gets P_d. The y_i are formed from $\{x_1, \ldots, x_N\}$ according to (6).

We will show that in each of the 2^n subsets, there exists precisely one $\{x_1, \ldots, x_N\}$ for which (9), (10) are fulfilled.

Let us suppose firstly that there were l ($l > 1$) such sequences

$$(14) \qquad \{x_1, \ldots, x_n, x_{n+1,j}, \ldots, x_{N,j}\}\,, \quad (j = 1, \ldots, l)$$

for which

$$(15) \qquad y_{i,j} = x_{i,j} \quad (i = n + 1, \ldots, N, \; j = 1, \ldots, l)\,.$$

Since $x_1, \ldots, x_n$ are not changing in the numbers of the subset, the relation (15) says that for more than one sequence with these initial terms, (1) (with all v's replaced by x's) is fulfilled. This is a contradiction, since, as is well known, the whole shift register sequence $\{x_1, \ldots, x_N\}$ is uniquely determined by the initial conditions $x_1, \ldots \ldots, x_n$. Thus, in each subset, there exists at most one sequence fulfilling (9), (10). That there exists actually such a sequence is clear, since in the numbers of each subset all possibilities of $x_{n+1}, \ldots, x_N$ occur, thus also the one given by $x_1, \ldots, x_n$ and (1) (with v's replaced by x's).

c) The transmitted sequence $\{v\}$ being given, there exists among the $2^n = N + 1$ subsets precisely one for which the probability of the unique sequence fulfilling (9), (10) is p^N. For the remaining N subsets the probability of the resp. unique sequence fulfilling (9), (10) is

$$(16) \qquad P = p^{(N-1)/2} q^{(N+1)/2}\,.$$

Indeed, in the subset for which $\{x_1, \ldots, x_n\} \equiv \{v_1, \ldots, v_n\}$, there is also $\{x_{n+1}, \ldots \ldots, x_N\} \equiv \{v_{n+1}, \ldots, v_N\}$ and according to (12), (13) the probability of this sequence is p^N. In the remaining subsets $\{x_1, \ldots, x_n\} \not\equiv (v_1, \ldots, v_n\}$. In these cases, as is well known, the sequences $\{x_1, \ldots, x_N\}$ are $\{0, \ldots, 0\}$ (in the first subset) and cyclic permutations of $\{v_1, \ldots, v_N\}$ (in the remaining N subsets). To say that the probability of $\{x_1, \ldots, x_N\}$ is (16) is the same as to say that comparing x_1 with $v_1, \ldots, x_N$ with v_N, one gets one more non-coincidence than is the number of coincidences. But this is well known. For the cyclic permutations, it is equivalent to the fact that all side peaks of the periodic autocorrelation sequence of a PNBS (with terms denoted by ± 1) equal to -1.

From a), b), c) there follows (11).

Especially for the noise alone, that is for $p = \frac{1}{2}$, the probability of false alarm is

$$(17) \qquad P_f = (N + 1)/2^N = 2^{-(2^n - n - 1)}\,.$$

4. COMPARISON WITH MATCHED FILTER COINCIDENCE DETECTION

Supposing that not only the transmitter linear shift register PNBS generator, but rather the transmitted PNBS itself is known at the receiver, the usual matched filter detection can be used. With the coincidence of all N terms of the sequence (that is now possible), there is

(18) $$P_d^* = p^N\,,$$
$$P_f^* = (\tfrac{1}{2})^N\,.$$

And from (16), (18)

(19) $$P_d/P_d^* = 1 + N(q/p)^{(N+1)/2}\,.$$

There follows

(20) $$\lim_{p\to 1} P_d/P_d^* = 1\,,$$

(21) $$P_f/P_f^* = N + 1\,.$$

Thus in the ideal case of Section 3, the detection method, being technically much simpler than that with the aid of a matched filter, is practically as good with respect to P_d for P_d not small, and gives a lower false alarm threshold, which is not a serious disadvantage and can be understood easily, because all sequences generated by the same generator are detected, not only a single one, and this gives greater chance also to noise to be accepted.

5. A REALISTIC DETECTION SCHEMA

There is clear that the detection schema of Section 3, based on neglection of the first n terms of the received sequence, is idealized and can be used only to roughly predict with the aid of Theorem 1 the behaviour of more complicated realistic schemas for which direct computing of detection probabilities can be practically inconvenient or perhaps impossible.

Such a schema will now be considered. Let us consider firstly the case of noise alone, that is $p = \frac{1}{2}$. Knowing that the signal sequence possesses $N = 2^n - 1$ terms, where n is the TLSR "length", one will seek r iterations of coincidences of x_i, y_i $(1 \leqq r \leqq N)$. If such event will occur, the signal will be declared as detected, the reception schema will be reset and a new signal seeking will be initiated and so on.

With this formulation, one has a classical problem of iterations [1], the number m of steps to reach decision is a random variable with ([1], Chpt. XIII, (1, 7))

(22) $$\mathsf{E}(m) = 2^{r+1} - 2\,,$$

(23) $$\sigma_m^2 = 2^{2(r+1)} - (2r + 1)\,2^{r+1} - 2\,,$$

so that for $r \to \infty$ there is asymptotically

(24) $$\mathsf{E}(m) \approx 2^{r+1}\,,$$

(25) $$\sigma_m \approx 2^{r+1}\,.$$

We define

(26) $$P_f = 1/\mathsf{E}(m) = 1/(2^{r+1} - 2)\,.$$

The formulae (22), (23) hold with the assumption of independence, thus, there must be shown that in the noise case the sequences $\{x\}$, $\{y\}$ are sequences of independent events and are also mutually independent.

Prior to show it, one may state that (24), (25) hold approximately for r not too great (say, practically, for $r > 25$).

From (26), one gets the following table.

Table 1.

P_f	r rounded	nearest "lenght' of usable PNBS
10^{-2}	6	7
10^{-4}	13	15
10^{-6}	19	31
10^{-7}	23	31
10^{-8}	26	31

Theorem 2. For noise alone, $\{x\}$ and $\{y\}$ are sequences of independent events and also x_i, y_i $(i = 1, 2, \ldots)$ are independent.

Proof. For noise alone, $\{x\}$ is evidently a sequence of independent events. For a given i, choose arbitrarily

$$(27) \qquad Y_i = \{y_i, y_{i-1}, \ldots, y_{i-t}\}\,,$$

t being also arbitrary. It is seen from (6) that the set $\mathcal{S}$ of all possible x's giving rise to Y_i in (27) is finite and uniquely determined. Forming now y_{i+1} with (6), the value y_{i+1} is determined as 0 or 1 with probabilities $\frac{1}{2}$, $\frac{1}{2}$ only by the new random variable x_{i-k+1} independently of $\mathcal{S}$ and thus of Y_i. That x_i, y_i are independent is clear since y_i is formed from x's with suffixes smaller than i.

It follows that the sequence of coincidences of x_i, y_i is also a sequence of independent events with probabilities $\frac{1}{4} + \frac{1}{4} = \frac{1}{2}$, and the results of [1] are applicable in the case of noise alone.

6. SOME RESULTS OF SIMULATION

For the case of signal plus noise one cannot apply the methods of [1], Chpt. XIII, Sec. 3, for $p \to 1$, moreover the signal sequence occurring irregularly in noise, the detection takes place in transient, not in stationary situation. Thus the signal detection process has been studied by computer Monte Carlo simulation.

Formula (11) has been checked for the simple case of 7-terms PNBS, generated by the TLSR (3,1,0) (in usual notation that means $v_4 = v_3 \oplus v_1$, $v_5 = v_4 \oplus v_2$, $\ldots$).

Initial conditions in the register were 1,1,1,1 in all experiments. The noise sequence was $N(0, 1)$. For each of the chosen values of s/n, 1000 random experiments have been made. Some results are given in the following table.

Table 2.

s/n (dB)	K (in (7))	P_d (in (11))	number of detections
6	2	0·868	868
3	1·41	0·558	560
0	1	0·298	307
-3	0·71	0·157	137
-6	0·5	0·096	98
$-\infty$	0	0·062	57

The agreement of the computed and simulated values is very good.

In all simulations, the beginning and end of each signal sequence are known, thus if the number of coincidence iterations is not sufficient to accept the hypothesis of signal presence at the signal end, the decision of signal miss is made in the experiment making it possible to measure P_d experimentally.

Some results will be shown for $r = 24$, PNBS-31 from the generator (5,2,0) and PNBS-63 from the generator (6,1,0), initial conditions being all 1's in both cases. After each decision, the register was filled by noise. Some results are shown in the following table each based on 500 random experiments.

Table 3.

s/n (dB)	K	P_d (PNBS-31)	P_d (PNBS-63)
9	2·83	0·98	1·00
6	2	0·57	0·87
3	1·41	0·10	0·34
0	1	0·01	0·05

7. CONCLUDING REMARKS

The method described may be useful with some radar configurations, or in the case of various nets where the detection of a given PNBS can initiate some control action.

As Ing. J. Beneš, CSc., has been pointed out, also other binary sequences than PNBS can be generated by a shift register (or some other type) generator of the length (defined by the memory places needed) substantially shorter than the number of sequence terms. This may be useful also in the periodic cases described in [2], [3], [4].

ACKNOWLEDGEMENT

For computer programs and simulations, and discussion of results, the author is indebted to Ing. J. Beneš, CSc.

(Received October 3, 1983.)

REFERENCES

[1] W. Feller: An Introduction to Probability Theory and Its Applications. Russian traпslation. Inoizdat, Moscow 1952.

[2] V. N. Botněv: Autocorrelation reception of pseudonoise signals (in Russian). Radiotechn. (USSR) *30* (1975), 6, 69–73.

[3] R. B. Ward and K. P. Yiu: Acquisition of pseudonoise signals by recursion-aided sequential estimation. IEEE Trans. Comm. COM-25 (1977), 8, 784–794.

[4] J. A. Ponnusamy and M. D. Srinath: Acquisition of pseudonoise codes in FH systems. IEEE Trans. Aerospace Electron. Systems AES-17 (1981), 3, 335–341.

Dr. Ludvík Prouza, DrSc., Tesla — Ústav pro výzkum radiotechniky (Institute of Radioengineering), Opočínek, 533 31 p. Lány na Důlku. Czechoslovakia.