ISSN 1392 – 1215 ELEKTRONIKA IR ELEKTROTECHNIKA, 2005. Nr. 6(62)

T 121 SIGNALŲ TECHNOLOGIJA

Identification of Pseudo-Random Noise Generator Structure

E. Lossmann, A. Meister, U. Madar
Department of Radio and Communication Engineering, Tallinn University of Technology,
Ehitajate tee 5, EE-19086 Tallinn, Estonia, e-mail: umadar@lr.ttu.ee

Introduction

Pseudorandom sequence of maximal length is such pseudorandom sequence of the elements of Galois field GF(2) that consists of approximately equal number of zeros and ones, has an autocorrelation function similar to that of white noise and has almost flat power spectral density. Pseudorandom sequences can be generated using algebraic methods and generating matrix for cyclic simplex code:

$$1;\beta^1;\beta^2;\beta^3;.....\beta^{m-1};\beta^m;.....\beta^{2^m-3};\beta^{2^m-2}; \quad (1)$$

where β is an element of finite extended array $GF\left(2^m\right)$ and also holds

$$\beta^i = \beta^{i-1}(\times)_{\mathrm{mod}\, G_m(z)}\beta, \quad (2)$$

where

$$G_m(z) = g_m z^m + g_{m-1}z^{m-1} + .. + g_1 z^1 + g_0, g_0 = 1.$$

If a primitive element β and its minimal polynomial $G_\beta(z) = M_\beta(z)$ is used to generate a pseudorandom sequence, then the sequence period is of maximum length $T_m = 2^m - 1$. Extended finite array $GF\left(2^m\right)$ can consist of several primitive elements, but each primitive element has its respective minimal polynomial [1].

Both direct m-sequence and its cyclically shifted variants are in use. Cyclical shifting does preserve the optimal features of a m-sequence.

Identification of a m-sequence reduces in fact to generating the m-sequence or a part of it. It is a well-known fact [2] that generating polynomial of a m-sequence is fully identifiable if we know sequence of symbols during one period

$$x_1; x_2; x_3;.....; x_{2m-2}; x_{2m-1}; x_{2m};..... ..; x_{2^m-1}. \quad (3)$$

Pseudorandom sequences can be generated using large extended finite arrays $GF\left(2^m\right)$, where m = 20, 21,..., making the analysis of the m-sequence over the period $T_m = 2^m - 1$ computationally extensive. Identification of generating polynomial implies *a priori* uncertainty when m and coefficients of the minimal polynomial are unknown. Identification can be done using partial sequences of the m-sequence, containing information about the generating minimal polynomial.

Identification problem

The problem of m-sequence identification can be divided into two parts using common methods for solving problems involving *a priori* uncertainty:

1. identify the coefficients of minimal polynomial $G_\beta(z) = M_\beta(z)$;

2. generate an identical sequence to the given m-sequence.

Identification of the coefficients of minimal polynomial $G_\beta(z)$

It is sufficient to know the sequence of 2m symbols in order to identify the coefficients of generating minimal polynomial of the m-sequence [3]:

$$\overline{x = [i = 1, m]} = x_1; x_2; x_3;.....; x_{2m-2}; x_{2m-1}; x_{2m}, \quad (4)$$

where m determines the necessary length of the m-sequence and i = 1 refers to the first symbol in the m-sequence as the first symbol in the known sequence to be analyzed.

m-sequence satisfies an equation

$$\|X\| \cdot \bar{g} = \overline{x[m+1, 2m]}, \quad (5)$$

where

$$\|X\| = \begin{Vmatrix} x_1 & x_2 & .. & x_m \\ x_2 & x_3 & .. & x_{m+1} \\ .. & .. & .. & .. \\ x_m & x_{m+1} & .. & x_{2m-1} \end{Vmatrix}; \bar{x} = \begin{vmatrix} x_{m+1} \\ x_{m+2} \\ .. \\ x_{2m} \end{vmatrix}; \bar{g} = \begin{vmatrix} g_1 \\ g_2 \\ .. \\ g_m \end{vmatrix}.$$

Coefficients $g_m; g_{m-1};.....g_2; g_1; g_o = 1$ of the generating minimal polynomial can be found as solution to the equation (5):

$$\bar{g} = \|X\|^{-1} \overline{x[m+1,2m]}, \quad (6)$$

where

$$\begin{vmatrix} g_1 \\ g_2 \\ .. \\ g_m \end{vmatrix} = \begin{Vmatrix} x_1 & x_2 & .. & x_m \\ x_2 & x_3 & .. & x_{m+1} \\ .. & .. & .. & .. \\ x_m & x_{m+1} & .. & x_{2m-1} \end{Vmatrix}^{-1} \begin{vmatrix} x_{m+1} \\ x_{m+2} \\ .. \\ x_{2m} \end{vmatrix}.$$

There exists a solution to the system of equations (6) if

$$\det\|X\| \neq 0 . \quad (7)$$

Let us consider two different *a priori* possibilities.

1. Identification of coefficients $g_m; g_{m-1};.....g_2; g_1;$ of minimal polynomial $G_\beta(z) = M_\beta(z)$when the value of *m* is known.

2. Identification of coefficients of $G_\beta(z) = M_\beta(z)$ when *m* is unknown.

Computer experiments

A computer program has been compiled using MATLAB 6.5 software package to identify m-sequences. The program has the following options:

1. to generate m-sequences of different length ($m < 33$);

2. to extract a sequence of length $2k$ from the generated sequence, starting from the i-th symbol:

$$\overline{x[i,k]} = x_i; x_{i+1}; x_{i+2}; .....; x_{i+2k-1}; x_{i+2k};$$

$$i = 1;.....;2^m - 2k - 2; \quad (8)$$

3. to distort the generated m-sequence using modulo-2 summation

$$\overline{x[i,k]} \oplus \overline{n[i,k]};$$

4. to calculate the coefficients of the generating minimal polynomial

$$g_m; g_{m-1};.....g_2; g_1.$$

The task of m-sequence identification can be solved in the following order as mentioned above:

1. identify the length *m* and coefficients $g_m; g_{m-1};.....g_2; g_1;$ of generating minimal polynomial;

2. generate an identical sequence to the given m-sequence

Conclusions

The results of the computer experiments led to the following conclusions:

1. If we know the value of *m* then the coefficients of the generating polynomial $G_\beta(z) = M_\beta(z)$ are $g_m; g_{m-1};.....g_2; g_1;$

- the system of equations has unique solution for arbitrary $m < 33$;
- the algorithm is invariant with respect to value of *i* for the set $\overline{x[i,k]}$;
- the algorithm is stable even if there exist small distortions in the sum $\overline{x[i,k]} \oplus \overline{n[i,k]}$.

2. Identification of coefficients $g_m; g_{m-1};.....g_2; g_1;$ of generating minimal polynomial $G_\beta(z) = M_\beta(z)$ when m is unknown:

- the algorithm allows for searching the value of *m* based on the m-sequence $\overline{x[i,k]}$, using sequence $\overline{x[i,d]}$ and:

a. the value of parameter *d* approaches to the value of *m*: $d + j \le m < k; j = 1;2...;$

b. choosing initial value of *d* larger than *m* and again the value of *d* approaches to *m*: $d \ge m;$ $m \le d - j < k; j = 1;2...;$

- the algorithm is invariant to the choice of *i* for the sequence $\overline{x[i,k]}$;
- the algorithm is stable even when there exist small distortions in the sum $\overline{x[i,k]} \oplus \overline{n[i,k]}$;
- there exists no unique solution for the coefficients of minimal polynomial if the length of extracted sequence $\overline{x[i,k]}$ is shorter than $2m$, i.e. $2k < 2m$.

3. The final identification of m-sequence takes place after we have identified the values of *m* and the coefficients of generating minimal polynomial; the final identification can be done if the extracted sequence $\overline{x[i,k]}$ is long enough.

One possible solution to generate the identical partial m-sequence is to generate the partial m-sequences of length $2m$ if we know the value of *m*. The value of *i* for the partial sequence $\overline{x[i,k]}$ should be chosen according to the maximum of non-periodic correlation coefficients.

References

1. **Madar U., Puusemp P.** Kodeerimine. – Tallinn: TTÜ, 2000 (*in Estonian*).**Pless V. S., Huffman W. C.** Handbook of Coding Theory. // Vol. 1, 2. – Elsevier, 1998.
3. **Sklar B.** Digital Communications: Fundamentals and Applications. – B. NJ, 1988.

Pateikta spaudai 2005 05 18

E. Lossmann, A. Meister, U. Madar. Pseudoatsitiktinių triukšmų generatoriaus struktūros atpažinimas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2005. – Nr. 6(62). – P. 13–15.

Maksimalaus ilgio pseudoatsitiktinės sekos (*m* sekos), taikomos telekomunikacijose, gali būti generuojamos taikant algebrinį metodą ar generavimo matricą ištęstai baigtinei Galois erdvei $GF(2^m)$. Jei žinosime vieno periodo simbolių seką, *m* sekos generavimo polinomas bus visiškai atpažįstamas. Atpažinimo užduotis analizuojama toliau: 1) identifikuojant minimalaus polinomo $G_\beta(z) = M_\beta(z)$ koeficientus ir 2) generuojant identišką duotajai *m* seką. Norint atpažinti *m* sekos koeficientus, pakanka žinoti 2*m* sekos simbolius. Šioms užduotims atlikti buvo sudarytos ir išanalizuotos MATLAB programos. Vienas iš galimų sprendimų generuojant identišką dalinę *m* seką yra 2*m* ilgio dalinių *m* sekų generavimas, jei yra žinoma *m* vertė. Dalinės sekos $\overline{x[i,k]}$ vertė *i* turi būti parenkama pagal maksimalius neperiodinės koreliacijos koeficientus. Bibl. 3 (anglų kalba; santraukos lietuvių, anglų ir rusų k.).

E. Lossmann, A. Meister, U. Madar. Identification of Pseudo-Random Noise Generator Structure // Electronics and Electrical Engineering. – Kaunas: Technologija, 2005. – No. 6(62). – P. 13–15.

Pseudorandom sequences of maximal length (*m*-sequences) needed in many telecommunication applications can be generated using algebraic methods and generating matrix for large extended Galois' finite array $GF(2^m)$. If we know the sequence of symbols during one period the generating polynomial of a *m*-sequence is fully identifiable. The task of identification is further analyzed in two parts: identification of the coefficients of minimal polynomial $G_\beta(z) = M_\beta(z)$, and generation of identical sequence to the given m-sequence. To identify the coefficients of generating minimal polynomial of the *m*-sequence it is sufficient to know the sequence of 2*m* symbols. MATLAB programs for both tasks have been compiled and investigated. One possible solution to generate the identical partial m-sequence is to generate the partial m-sequences of length 2*m* if we know the value of *m*. The value of *i* for the partial sequence $\overline{x[i,k]}$ should be chosen according to the maximum of non-periodic correlation coefficients. Bibl. 3 (in English; summaries in Lithuanian, English and Russian).

Э. Лоссман, А. Мейстер, У. Мадар. Опознание структуры генератора псевдо-случайных шумов // Электроника и электротехника.– Каунас: Технология, 2005. – № 6(62). – С. 13–15.

Псевдослучайные последовательности максимальной длины (*m*-последовательности), которые применяются в телекоммуникациях, могут генерироваться с помощью алгебраического метода или матрицу генерирования для растянутой ограниченной Galois среды. Зная последовательность символов одного периода, полином генерирования *m*-последовательности полностью опознаваем. Задача анализа производится далее при помощи: 1) идентификации коэффициентов минимального полинома $G_\beta(z) = M_\beta(z)$ и 2) генерирования последовательности *m*. Чтобы опознать коэффициенты последовательности *m*, достаточно знать символы последовательности 2*m*. Для этой цели были созданы и исследованы программы MATLAB. Одним из возможных решений генерируя идентичную частичную последовательность *m* является генерирование частичных последовательностей *m*, длина которых - 2*m*, при условии, что *m* значение известно. Значения *i* частичных последовательностей $\overline{x[i,k]}$ должны быть подобраны по максимальным коэффициентам непериодичной корреляции. Библ. 3 (на английском языке; рефераты на литовском, английском и русском яз.).

DOI: 10.5755/j02.eie.10460