ANALYSIS OF METHODS FOR CALCULATING REFERENCE SIGNATURES IN DIGITAL DEVICES

R. Kh. Djurayev
Candidate of Technical Sciences, Associate Professor of Tashkent University of Information Technologies named after Muhammad al Khorezmi,
Sh.Yu. Jabborov
Candidate of Technical Sciences, Associate Professor of Tashkent University of Information Technologies named after Muhammad al Khorezmi,
I. I. Omonov is assistant at Urgench brench Tashkent University of Information Technologies named after Mahammad al Khorezmi

ABSTRACT

In this report the modern methodology of identifying the faults and the estimation of control reability by means of compact testing are considered. Comparative analysis of considered methods is provided. The need to create methods for calculating signatures is associated, firstly, with the need to automate the production of dictionaries (tables) of reference signatures, since their creation by measuring signatures is quite time consuming, and secondly, with the assessment of the reliability of the signature analyzers themselves. Therefore, the main document of signature analysis is the dictionary of reference signatures, which defines the troubleshooting algorithm.

Key words: *binary, polynomial, register, input polynomial, Simplified signature, inverse polynomial.*

АННОТАЦИЯ

В этом отчете рассмотрена современная методика выявления неисправностей и оценки достоверности управления с помощью компактного тестирования. Приведен сравнительный анализ рассмотренных методов. Необходимость создания методов вычисления подписей связана, во-первых, с необходимостью автоматизации создания словарей (таблиц) эталонных подписей, поскольку их создание путем измерения подписей достаточно трудоемко, во-вторых, с оценкой достоверности сами анализаторы сигнатур. Поэтому основным документом сигнатурного анализа является словарь эталонных сигнатур, который определяет алгоритм устранения неполадок.

Ключевые слова: *двоичный, полином, регистр, входной полином, упрощенная подпись, обратный полином.*

INTRODUCTION

The transition to the widespread use of microprocessor kits in modern telecommunications equipment has created a number of serious problems associated with diagnostic processes. One of the most powerful external diagnostic tools for microprocessor systems is a signature analyzer (SA) [1,2]. An important parameter of a signature analyzer is a set (dictionary) of reference signatures, which is predetermined for a working digital device. The need to create methods for calculating signatures is associated, firstly, with the need to automate the production of dictionaries (tables) of reference signatures, since their creation by measuring signatures is quite time consuming, and secondly, with the assessment of the reliability of the signature analyzers themselves. Therefore, the main document of signature analysis is the dictionary of reference signatures, which defines the troubleshooting algorithm.

At present, various theoretical methods are known that make it possible to calculate reference signatures [1-4].

DISCUSSION AND RESULTS

A method for calculating signatures based on modeling the operation of a CA As you know, the essence of CA lies in the fact that data sequences from a node of a correctly functioning circuit in test mode are set in accordance with a certain signature. During the subsequent verification of this circuit, the operator, using the analyzer, measures the signatures at various points in the circuit of the digital device and compares them with the reference signatures recorded in the documentation. The principle of operation of the CA is based on the method of signature analysis, that is, the compression of long sequences into four-digit hexadecimal signatures. Physically, this method is implemented on a linear shift register with feedback, the signals of which are summed modulo two with the input sequence. An irreducible polynomial is used as a polynomial

$$P(X)=x^{16}+x^{12}+x^{9}+x^{7}+1$$

Signatures are usually reproduced in an alphabet consisting of ten numbers and six letters: 0,1,2,3,4,5,6,7,8,9, A, C, F, H, P, U. Each binary sequence has its own signature

0000 - “0”	0100 - “4”	1000 - “8”	1100 - “F”
0001 - “1”	0101 - “5”	1001 - “9”	1101 - “H”
0010 - “2”	0110 - “6”	1010 - “A”	1110 - “P”
0011 - “3”	0111 - “7”	1011 - “C”	1111 - “U”

Figure 1 shows a diagram explaining the principle of compression of the input sequence [1,2].

The signature is generated using a logic feedback shift register

$P(X)=x^{16} + x^{12} + x^{9} + x^{7} +1$, at the input of which there is an adder modulo two. Suppose that during the connection of the CA probe to any control point, a 20-bit sequence of ones and zeros appeared in it, which looks like:

11111100000111111111.

This input sequence is added modulo 2 with the contents of cells 7,9,12 and 16 of the shift register. After 20 clock cycles of the circuit, the register will contain a 16-bit combination 1101100101010011, which, as a result of division into four four-bit combinations, corresponds to the alphanumeric signature H953.

Method for calculating signatures based on nested polynomials

Consider the scheme of a pseudo-random sequence generator on an n-bit shift register, with feedbacks taken from n, m, l, k bits, which are fed into the adder modulo 2 (Fig. 1)[1,3].

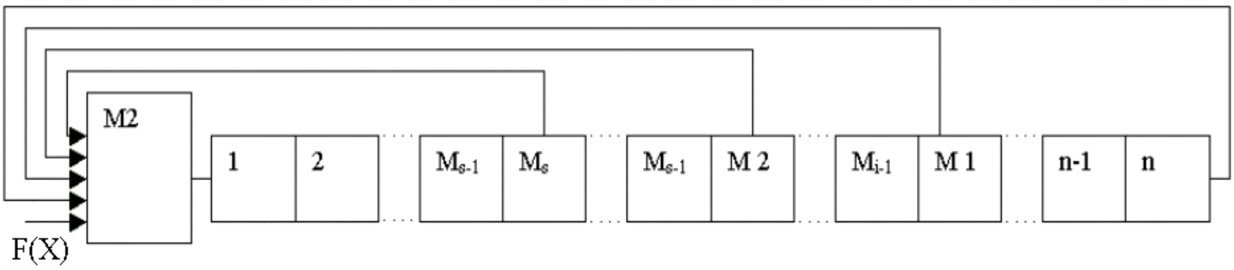

Fig. 1. Scheme of a pseudo-random sequence generator (PRSP) based on a shift register with a length of n bit

Then

$$F(X) = g(X) P_n(X) + r(X)$$

where F (X) is the input polynomial;

g (X) - quotient of division;

Pn (X) - inverse of the feedback polynomial for a register of length n-discharges;

r (X) is the remainder.

In [3], the shift register is considered as a set of n, m, l, k-bit shift registers nested one into the other. Obviously, each register performs its own division (transformation) of the input polynomial. If the degree of the input polynomial is greater than the degree (width) of the shift register, then the influence of nested registers is taken into account in the feedback polynomial of the shift register of greater length. If the degree of the input polynomial does not exceed the degree of the register, then the input polynomial is divided by the inverse of the feedback polynomial of the shift register of a shorter length. Since the degree r (X) is less than the degree P (X), then to obtain the real remainder, it is necessary to divide r (X) by the inverse of the feedback polynomials of the registers of shorter length.

Let us denote the inverse of the feedback polynomials by Divide the input polynomial F (X) by the polynomial $P'_n(X)$:

$$\frac{F(X)}{P'_n(X)} = g_n(X) + \frac{r_n(X)}{P'_n(X)} \qquad (1)$$

Then we will sequentially consider the leftovers $r_i(X)$, (i=n,m,l) as input polynomials for shorter shift registers by dividing them by a polynomial:

$$\frac{r_n(X)}{P'_m(X)} = g_m(X) + \frac{r_m(X)}{P'_m(X)} \qquad (2)$$

$$\frac{r_m(X)}{P'_l(X)} = g_l(X) + \frac{r_l(X)}{P'_l(X)} \qquad (3)$$

$$\frac{r_l(X)}{P'_k(X)} = g_k(X) + \frac{r_k(X)}{P'_k(X)} \qquad (4)$$

Analysis of formulas (1 - 4) shows that $g_n(X)$ is the output polynomial of the degree n register, $g_m(X)$ – the output polynomial of the register of degree m, which fills the bits from m + 1 to n of the shift register,

g_l – the output polynomial of the register of degree l, which fills the digits from l +1 to m, and so on;

$r_k(X)$ - the remainder remaining in the shift register, which has only one feedback and fills the digits from 1 to k. Thus, the signature can be written in the following form:

[illegible] (5)

Using this formula, you can calculate the signatures for the shift register numbered from 1 to n. If the numbering of the digits starts from zero, then the formula (5) will take the form:

[illegible] (6)

For example, for the GPSS developed by HP, formula (6) has the form:

[illegible] (7)

Consider an example of calculating a signature using the specified method for the above input sequence. Dividing the input sequence F (X) by the inverse polynomial $P'(X)$ we get the quotient: $g(X) = x^3 + x^2 + x + 1$ and the remainder $r_{16}(X) = x^{15} + x^{14} + x^{12} + x^{11} + x^7$... Then we will divide $r_{16}(X)$ to the inverse of the feedback polynomial of a 12-bit register $P(X) = x^{12} + x^5 + x^3 + 1$... As a result, we get the quotient $g_{12}(X) = x^3 + x^2 + 1$ and the remainder r12(X) = x11 + x9 + x6 + x2 + 1. Divide r12 (X) by the inverse of the feedback polynomial of the 9-bit register. As a result, we get the quotient

$g_9(X) = x_2$ and the remainder $r_9(X) = x^8 + x^6 + x^4 + 1$.

Divide r9 (X) by the inverse of the feedback polynomial of the 7-bit register. As a result, we get the quotient $g_7(X)=X$ and the remainder $r_7(X)=x^6 + x^4 + x + 1$.

Π Substituting the obtained values into the expression for r_c (X), we obtain

$r_c(X)=(x^3 + x^2 +1)\, x^{12} + x^2\, x^9 + x^8 + x^7 + x^6 + x^4 + x +1=x^{15} + x^{14} + x^{12} + x^{11} + x^8 + x^6 + x^4 + x + 1$.

Convert the resulting polynomial to binary form r_c(HP)=1101100101010011, which corresponds to the signature H953.

It can be seen from the given example that this method of calculation requires memorizing the generators of polynomials of degree r, m, l, k, as well as performing additional calculations to obtain a real signature.

Simplified signature calculation method

As noted earlier, the CA method consists in compressing the output reactions of the tested electronic components using a shift register with logical feedback into short words - signatures. The principle of implementation of the CA as a whole is based on mathematical relationships similar to those used in the formation of cyclic codes. However, due to the fact that the practical scheme of the divider itself, made on multi-input adders modulo 2, differs from the used cyclic code divider, the contents of the shift register CA and the result of dividing F (X) by P (X) do not match. It is known that the remainder obtained in the shift register has the form $R(X)= x^{15} + x^{14} + x^{12} + x^{11} + x^8 + x^6 + x^4 + x + 1$,

and the remainder when dividing F (X) by P '(X) has the form: $x^{15} + x^{14} + x^{12} + x^{11} + x^7$.

In this regard, it is necessary to analyze not the remainder of the division, but the quotient of the division. In accordance with this technique, the signature is calculated by multiplying the input polynomial F (X) by the monomial Xr and dividing this product by the inverse generating polynomial $P'(X)$:

$$\frac{F(X)X^r}{P'(X)} = Q(X) + \frac{R(X)}{P'(X)} \qquad (8)$$

CONCLUSION

In this case, the quotient of division has the same degree as F (X), and the signature is the last r digits.

$r_c(X)=[Q(X)] \bmod 2^r$

Let us consider an example of theoretical calculation of a signature by this method for an input sequence similar to the previously considered one. Multiplying the input polynomial F (X) by the monomial X^{16} we get:

$F(X)\,X^{16} = x^{35} + x^{34} + x^{33} + x^{32} + x^{31} + x^{30} + x^{29} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + X^{17} + x^{16}$.

Divide this polynomial by the inverse polynomial

$$P'(X)=x^{16}+x^9+x^7+x^4+1$$

As a result, we get the quotient $Q(X)=x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^8 + x^6 + x^4 + x + 1$. И остаток $R(X)= x^{15} + x^{13} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^2 + x$

Transforming Q (X) into binary form, we obtain Q (X)=11111100100101010011

The last 16 bits, according to the method, are the signature, i.e.

1101100101010011 matches the signature H953.

REFERENCES

1. Гуляев В.А, Кудряшов В.И «Автоматизация наладки и диагностирования микро УВК» -М. Энергоатомиздат.1992-256с.
2. Новик Г.Х, Сташин В.В, Мазур Е.И «Элементы теории сигнатурного анализа»/ Труды института инженеров железнодорожного транспорта, 1979 вып. 642.с.52-59.
3. Кудряшов В.И « Методы расчёта сигнатур и оценка достоверности сигнатурных анализаторов » / Электронное моделирование, 1985. №2.с 57-61.
4. 4.Джураев Р.Х, Минаров М. М « Теоретический расчёт сигнатур и оценка достоверности сигнатурного анализа», Теория и средства современных систем связи. Сборник научных трудов. Тошкент 1988. с.99-101.
5. Джураев Р.Х., Джаббаров Ш.Ю., Балтаев Ж.Б. «Системы технического обслуживания и эксплуатации сетей телекоммуникации».Учебник.-Т.: «Алоқачи».2019, 234 с.
6. Джураев Р.Х., Джаббаров Ш.Ю. Контроль и диагностика цифровых устройств систем передачи данных. (Монография). -Т.: «Алоқачи».2020, -168 с.

7. R.H. Djuraev, Sh.Yu. Djabbarov, J.B. Baltayev. «Raqamli tizimlarning texnik diagnostikasi». (Darslik). -T.: «Aloqachi»,2020, - 232 b.