Structural Means Generating Pseudorandom Sequences Of Fixed Weight Binary Patterns

Rabah AlShboul† and Vitaliy A. Romankevich††

Computer Science Department Al Albayt University Mafraq, Jordan
Department of Applied Mathematics Igor Sikorsky Kyiv Polytechnic Institute Kyiv, Ukraine

Summary
The article defines and solves the actual problem of structural realization aimed to generate fixed weight pseudorandom binary pattern sequences with enhanced productivity. The general approach underlying proposed solution is to organize a controlled (operated) shift in the output register structure. In this case logical decomposition of the output register into two non-overlapping and synchronous sub-circuits is performed. Choice of the decomposition point is determined by the current state of pseudorandom equal probability binary patterns formation unit. The schematic implementation of the proposed structure main units was elaborated in detail, as well as an valuation methodology for both hardware and statistical parameters of the proposed shaper was developed. A comparison of the obtained characteristics with analogous values for a functionally closest known technical solution, which was considered in detail at the beginning of the work, is made. It is suggested to use the value of the mathematical expectation of the path traversed by an arbitrary (any) bit in the output register in one shift stroke to estimate the probabilistic characteristics of the controlled shift based devices. The article gives some data obtained as a result of simulation of the shaper in question. It is shown that the main advantage of the proposed structure of the shaper is the increased speed as compared with known solutions for which the minimum allowable period of sync signals depends linearly on the number of bits in output vector. It is shown that the considered structural approach to the generation of pseudorandom patterns is characterized by a significant (up to several times) increase in velocity, while the probabilistic quality indicators of the generated sequences of proposed device are at the same level as it is for known generators.

Key words:
Pseudorandom sequences, fixed weight, binary patterns, statistical modeling of the behavior, pseudorandom generator.

1. Introduction

The need to develop effective high-performance specialized structural means for obtaining pseudorandom (PR) sequences with specified properties is due to the importance and range of their possible applications, such as hardware and software resources of procedures for statistical modeling of the behavior of multiprocessor fail-safe systems in the failure flow [1-3], automated diagnostic complexes for pseudorandom testing of complex digital objects, devices for transmitting and processing information, and a number of others. So it is necessary to provide the possibility of forming high performance with specified (arbitrary) multiplicity of system components' failure characteristics in the process of modeling the behavior of multiprocessor fault-tolerant systems in the flow of failures. Higher requirements for the clock frequency of testers based on pseudo-random methods are also put forward in systems for diagnosing complex digital devices. When monitoring memory circuits, pseudorandom test sequences are used to ensure that the mutual influence of certain memory cells is checked. In view of the foregoing, it can be argued that the task of developing specialized structural tools that perform the functions of obtaining high-performance PR sequences of multi-bit binary patterns is sufficiently important and relevant [4,5].

The authors of the article have been working on the structural synthesis of specialized digital devices for generating sequences of fixed weight binary pseudorandom patterns for a number of years [6-8]. In particular, a multichannel signal generator with variable probability, constructed on the basis of the controlled shift register (CSR), has been developed and studied. The basis of this circuit is the organization of the binary code shift in the output register under the control of signals from the master (reference, control) pseudorandom pattern generator (PRPG) forming equal probability binary patterns.

2. An earlier solution

Fig. 1 shows the general structure of the multichannel shaper. The output N-bit register Rg can be implemented basing on using the delay elements (for example, in the form of clocked D-type flip-flops (FF)). The three logic circuits SS1, SS2 and SS3 serve to organize the controlled shift in the register Rg: the SS1 circuit contains the signal conditioning elements at the Rg data inputs, the SS2 circuit arranges communication of Rg register bits under controllable shift (in other words, SS2 implements the synchronization signals forming the shift).

Manuscript received October 5, 2017
Manuscript revised October 20, 2017

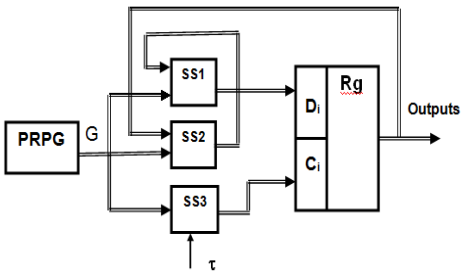

Fig. 1

Shift in register Rg is of a circular nature. If the FF of Rg register are T1, T2, TN, SS3 circuit outputs - C1, C2, CN, SS1 circuit outputs - a1, a2,… aN and PRPG outputs - g1, g2,… gN, than the nature of the register Rg bits connection is that the outputs b1, b2, b3… bN are associated with the transmission from the neighboring b2=f(b1), b3=f(b2),… bN=f(bN-1). For b1 bit the condition b1=f(bN) is fulfilled and $\forall$ i = 1, 2, 3… N [bi=f(b(i-1)mod N)]. Taking into account the latter relation, the operation of the SS1, SS2 and SS3 circuits, controlling some (any) i-th channel (i=1,2,3…N), can be described by next equations.

For SS1 circuit Di=ai=b(i-1)modN·gi, where: Di –D-input state of FF Rg Ti. Recall that in this case (i=1) →(Di= a1= bN· g1).

For SS3 circuit Ci= gi·τ, where τ – output of the synchronization clock generator.

For circuit SS2:

$$b_i = b_{(i-1)\bmod N} \cdot \overline{g_i} \vee T_i \cdot g_i .$$

On the basis of the logical relationships above, the functional circuit of the shaper channel i=1,2,…N can be represented in Fig. 2, which, for the sake of simplicity, the initial installation of the Rg register FF' circuits does not showed. Suppose that during initial installation of register Rg, a pattern of k ones and N-k zeros appeared (distribution of k ones on Rg register bits is not essential). Obviously, ring connection of the register bits will result in weight not changeability of any subsequent patterns and that weight can be k=0,1,2,…N-1,N. Let us estimate the probability of a state at an arbitrary i output of the Rg register (the identity of the channel structure and the circular topology of the transport chain allows us to assume that the relations given below are valid for any value i=1,2,…N). It's obvious that P(Ti=1)= P(ai=1), so the probability of Ti state is equal to the state of the i-th output of the SS1 circuit. After a sufficiently large number of PR-shifts on average, k of ones will be roughly uniformly distributed over the Rg register. In other words, the mathematical expectation of zeros' number between two ones will be N/k-1. According to Fig. 2 P(ai1)=P(gi=1)· P(b(i-1)modN=1), where P(ai') – is the probability of a single ai output state with gi=1.

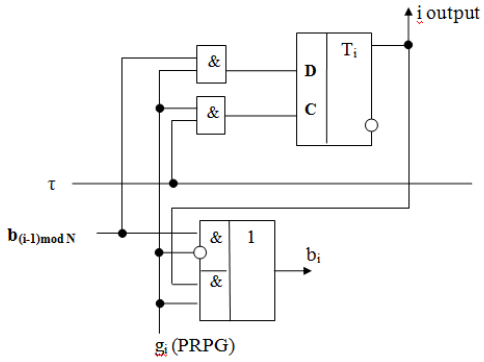

Fig. 2

Similarly: $P(a_i^0)=P(g_i=0)\cdot P(T_i=1)$, where: $P(a_i^0)$ – probability of one conservation in T_i FF with $g_i=0$. Then:

$$P(T_i) = \frac{1}{2} \cdot \frac{1}{N/k} + \frac{P(T_i)}{2},$$

Therefore $P(T_i)=k/N$. So changing (setting) the weight of the initial code in the register *Rg* of $0 \div N$ range, we obtain a number of possible values of the output probabilities: *0, 1/N, 2/N, 3/N, (N-1)/N*, 1. The complexity *L* of such a shaper can be estimated from Fig. 2: $L=2L(T)+5$, where $2L(T)$ is the total complexity of the Rg register T_i FF or PRPG bits' implementation.

3. Device of enhanced features

The presence of a sequential signal propagation path bi (Fig. 2) leads to a linear dependence of delay in this circuit on the value N of the device output pattern, and, consequently, to a decrease in the generator clock frequency. This is the main drawback of the above-mentioned technical solution.

The general principle underlying proposed solution is illustrated by the structure, shown in Fig. 3, and consists in the controlled shift organization in the shaper output register, as shown in Fig. 4.

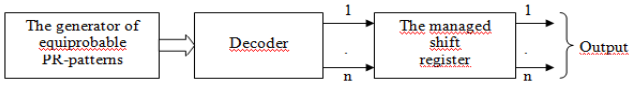

Fig. 3

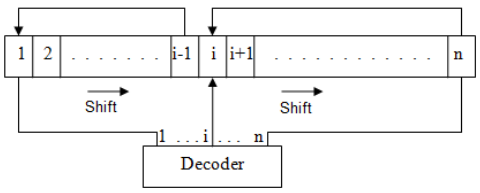

Fig. 4

In accordance with Fig. 4 to each output of the decoding circuit *i=1,2,…n*, n-bit the output pattern of the shaper, the bit of the controllable shift output register CSR is mapped. When the m-bit pattern *(m=]log₂n[)* arrives at the input of the decoder, the output register is logically decomposed into two independent shift structures in accordance with the following boundary conditions for performing the shift operations:

$(DC_1=1) \rightarrow (R_1 := R_n)$,
$(DC_2=1) \rightarrow [(R_2 := R_n)\&(R_1 := R_1)]$,
$(DC_3=1) \rightarrow [(R_3 := R_n)\&(R_1 := R_2)]$,
. . . . . .
$(DC_i=1) \rightarrow [(R_i := R_n)\&(R_1 := R_{i-1})]$,
. . . . . .
$(DC_n=1) \rightarrow [(R_n := R_n)\&(R_1 := R_{n-1})]$,

where $DC_r=1$ – the state of the decoder when an equal probability pattern *r=1,2,…n* arrives, R_r – is the state of the *r-th* bit of the CSR output register. The implementation of j-th CSR bit, *j=2,3,…n*, is shown in Fig. 5, where K is the designation of the switch *"2→1"*, DC_j is the state of the j-th output of the decoder, CB (common bus) is the state of the common bus uniting the CSR bits outputs.

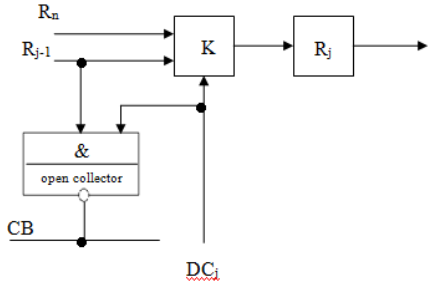

Fig. 5

Some difference, related to the organization features of controlled shift, has the first bit of CSR R1, structure of which is shown in Fig. 6.

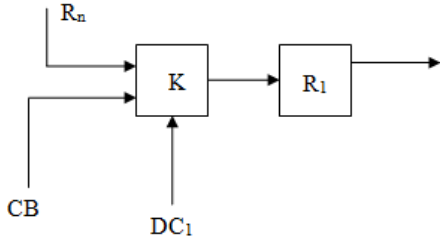

Fig. 6

The operating conditions of the circuit in Fig. 5 can be written in the form of the relations:

$$\begin{cases} (DC_j=1) \rightarrow [(OUT_K = R_n)\ \&\ (CB: = R_{j-1})], \\ (DC_j=0) \rightarrow (OUT_{K:} = R_{j-1}), \end{cases}$$

Where: OUT_K - the output state of the *K* switch, *j=2, 3, n*. For the circuit in Fig. 6, the difference from the circuit in Fig. 5 can be shown as a condition $(DC_1=0) \rightarrow (OUT_K: =CB)$.

4. Comparative evaluation of parameters

It is possible to estimate some parameters of the proposed shaper and compare the obtained values with similar values for the circuit considered at the beginning of this work.

As a characteristic of the statistical properties of shapers based on controlled shift, we can choose the value M[l] of the mathematical expectation for a path traversed by any bit in a single clock cycle. For the precede (known) device, we can write:

$$M[l_1]=0\cdot\left(1-\frac{1}{2}\right)+1\cdot\frac{1}{2}+2\cdot\left(1-\frac{1}{2}\right)\cdot\frac{1}{2}+3\cdot\left(1-\frac{1}{2}\right)^2\cdot\frac{1}{2}+\ldots+n\cdot\left(1-\frac{1}{2}\right)^{n-1}\cdot\frac{1}{2}.$$

Or in general:

$$M[l_1]=\sum_{i=1}^{n}\left(i\cdot\frac{1}{2^i}\right)=\frac{1}{2^1}+\frac{2}{2^2}+\frac{3}{3^3}+\ldots+\frac{n-1}{2^{n-1}}+\frac{n}{2^n}.$$

The M[l1] quantity can also be represented as:

$$M[l_1]=\sum_{i=1}^{n}\frac{i}{2^i}=\sum_{i=1}^{n}\frac{i-1}{2^i}+\sum_{i=1}^{n}\frac{1}{2^i}.$$

In its turn:

$$\sum_{i=1}^{n}\frac{i-1}{2^i}=\sum_{i=2}^{n}\frac{i-2}{2^i}+\sum_{i=2}^{n}\frac{1}{2^i}.$$

Or for any $1\le k\le n$:

$$M[l_1]=\sum_{i=k}^{n}\frac{i-k}{2^i}+\sum_{j=1}^{k}\sum_{i=j}^{n}\frac{1}{2^i}.$$

Obviously, for k=n we obtain:

$$M[l_1]=\sum_{j=1}^{n}\sum_{i=j}^{n}\frac{1}{2^i}.$$

The sum of the geometric progression terms:

$$\sum_{i=j}^{n}\frac{1}{2^i}=\frac{2^{n-j+1}-1}{2^n}.$$

Then:

$$M[l_1]=\sum_{j=1}^{n}\frac{2^{n-j+1}-1}{2^n}.$$

Therefore, for the limit:

$$\lim_{n\to\infty}M[l_1]=\sum_{j=1}^{\infty}\lim_{n\to\infty}\frac{2^{n-j+1}-1}{2^n}=\sum_{j=1}^{\infty}\lim_{n\to\infty}\left(\frac{1}{2^{j-1}}-\frac{1}{2^n}\right)=\sum_{j=1}^{\infty}\frac{1}{2^{j-1}}=$$

$$1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\ldots=2$$

Let $M[l_2]$ be the mathematical expectation of the path length traversed by any bit of the output vector in the proposed embodiment of the shaper. Let $P(n-2)$ be the probability of finding this bit in any of $(n-2)$ bits of output register, $P(i+1)$ is the probability of finding the bit in some $(i+1)$ bit, $i=1,2,\ldots n-1$, $P(n)$ is the probability that the bit is in n place. In other words, the output register is conventionally divided into three regions in accordance with the PR selection of one of the n bits of the register (Fig. 4), namely: one-bit regions i and n and a region of the remaining $(n-2)$ bits. It is obvious that in this case $P(n-2)+P(i)+P(n)=1$. Therefore, we can write:

$$\mathrm{M}[l_2]=1\cdot P(-2)+\frac{n}{2}\cdot P(i+1)+\frac{n}{2}\cdot P(n),$$

where: $n/2$ – is the mathematical expectation of each logical shift group length in the PR-selection of the i-th bit. If we consider that

$$P(n-2)=\frac{n-2}{n}, P(i+1)=P(n)=\frac{1}{n}$$, then

$$\mathrm{M}[l_2]=\frac{n-2}{n}+\frac{n}{2}\cdot\frac{1}{n}+\frac{n}{2}\cdot\frac{1}{n}=\frac{n-2}{n}+1$$.

Or, passing to the limit, we finally obtain: $\lim_{n\to\infty}\mathrm{M}[l_2]=2$.

Some statistical data obtained as a result of modeling the considered shaper are presented in table 1.

Table 1

n	Weight	The number of patterns	The number of cycles	Percentage of ones	Probability of one	Inaccuracy
16	1	16	25	0,08	0,0625	0,0175
	2	120	617	0,1151	0,125	0,0099
	3	560	4519	0,1892	0,1875	0,0017
	4	1820	14640	0,2516	0,25	0,0016
	5	4368	36568	0,311	0,3125	0,0015
	6	8008	91755	0,3738	0,375	0,0012
	7	11440	101894	0,4366	0,4375	0,0009
	8	12870	125938	0,5005	0,5	0,0005
20	1	20	22	0,0909	0,05	0,0409
	2	190	681	0,0911	0,1	0,0089
	3	1140	9888	0,1516	0,15	0,0016
	4	4845	37932	0,1985	0,2	0,0015
	5	15504	169396	0,2501	0,25	1E-04
	6	38760	377458	0,2999	0,3	1E-04
32	1	32	70	0,04286	0,03125	0,01161
	2	496	2283	0,0648	0,0625	0,0023
	3	4960	38969	0,09244	0,09375	0,00131
	4	35960	335183	0,1251	0,125	1E-04

Let us show that the main advantage of the proposed shaper structure is the increased speed with respect to the technical solution, for which, as follows from the circuit, shown in Fig. 3, the clock frequency should be determined basing on the minimum allowable clock period $T_1 \geq 2(n\cdot\tau_e+\tau_t)$, τ_e is the delay of one logic element, τ_t is the switching interval of the memory element in the shift register of the equal probability PR-patterns' generator (assuming that it is implemented in a widely known way: a shift register with linear feedback [9]). At the same time, taking into account the schematic features of the structures shown in Fig. 5 and 6, it can be written that the clock period of the proposed shaper is determined by the relation:

$$T_2 \geq \tau_{tg}+\tau_{DC}+\tau_{sr},$$

where: τ_{tg} – is the time of the output register address-bit number formation, τ_{DC} – delay on the decoder (Fig. 4), τ_{sr} – interval of the shift in the output register. According to [10], we can assume that $\tau_{DC}=\tau_e=20ns$, $\tau_t=\tau_{tg}=40ns$, a $\tau_{sr}=60ns$ (taking into account the delays introduced by the commutation elements in Figures 5 and 6). Then, for example, for $n=64$ we get that $T_1 \geq 2(64\cdot 20+40)=2640ns$, a $T_2 \geq 120ns$.

Let's perform a comparative analysis of the hardware costs for the two shaper variants. In accordance with Fig. 1 and 2, the complexity of the controllable shift structure depends linearly on the number of bits of the output pattern and can be estimated by the value $L_1=24n$ binary gates with two-inputs (t.g.).

For the shaper in question, the complexity of the circuit implementation (also in the number of t.g.) is found as:

$$L_2=L_R+L_{DC}+L_G,$$

Where: $L_R \cong 12n$ – complexity of the output shift register and switching elements, $L_{DC}=(m-1)n$ – complexity of the PR-patterns decoder, $m=\log_2 n$ (to simplify the analysis, we assume that m is a positive integer digit), L_G – complexity of the probabilistic shaper.

For specific values of n=64, m=6, we get:

$L1=24\cdot 64=1536$ t.g.,

$L_2=12\cdot 64+5\cdot 64+6\cdot 10=1148$ t.g..

Acknowledgments

The work proposes a structural implementation of a controlled equal weight pseudorandom binary patterns sequence generator with the value of the weight can be changed. The proposed solution is characterized by a significant (several times) increase in the speed (i.e., the clock frequency of the device operation) and while maintaining the statistical quality parameters (average path length of the bits in the output register under a pseudorandom shift, for example) of equal weight patterns in generated sequences. At the same time logical decomposition of the generator output register makes the complexity low. The disadvantage of the considered generator is the repetition of some vectors during a period from which the solutions described in [4 and 5] are free.

References

[1] Романкевич О.М., Карачун Л.Ф., Романкевич В.О. До питання побудови моделі поведінки багатомодульних систем // Наукові вісті НТУУ "КПІ".- 1998.- №1.-С.38-40.

[2] Романкевич А.М., Романкевич В.А., Мораведж Сейед Милад О повышении надёжности реконфигурируемых отказоустойчивых систем управления сложными объектами // Электронное моделирование.- т.32, №4.- 2010.- с.85-92.

[3] Романкевич В.А. Об одной модели поведения отказоустойчивой многопроцессорной системы // Радиоэлектроника и информатика.-Харьков.-1999.- №1.- С. 75-76.
[4] Sanchez S., Criado R. A Generator of Pseudo-Random Numbers Sequences with a Very Long Period // Mathematical and Computer Modelling.- No. 42.- 2005.- pp. 809-816
[5] Remya J., Binu K. M., Susan A. FPGA Implementation of High Quality Random Number Generator using LUT based Shift Registers // Procedia Technology.- No. 24.- 2015.- pp. 1155-1162
[6] Романкевич В.А., Майданюк И.В. Структурный метод формирования двоичных псевдослучайных векторов заданного веса // УСиМ. - 2011. - № 5. - С. 28-33, 58.
[7] Романкевич А.М., Майданюк И.В., Романкевич В.А. О формировании функций управления для генератора последовательностей двоичных векторов // Радіоелектронні і комп‘ютерні системи.-№6, 2014.- С.157-163
[8] Гроль В.В., Романкевич В.А., Потапова Е.Р., Мораведж Сейед Милад. Структурный метод генерации псевдослучайных последовательностей специального вида // Радіоелектронні і комп‘ютерні системи.-№5, 2010.- С.230-236
[9] Gill A. Linear sequential circuits / Arthur Gill. 1966, New York: McGraw-Hill.
[10] Texas Instruments Inc., Logic Guide, www.ti.com, Texas Instruments Literature number SDYU001AA, Europe, 2014.