Josef Pužman

Some nonlinear shift register generators

Kybernetika, Vol. 6 (1970), No. 6, (456)--462

Persistent URL: http://dml.cz/dmlcz/124793

KYBERNETIKA ČÍSLO 6, ROČNÍK 6/1970

Some Nonlinear Shift Register Generators

JOSEF PUŽMAN

In the contribution some shift register generators producing certain cyclic sequences are considered. The problem is concentrated on the searching procedure of suitable, in general nonlinear, feedback Boolean function to generate the sequences of length 2^n and $2^n - 1$. The number of such Boolean functions is derived and some of their necessary properties are established by means of which it is possible to reduce the amount of Boolean function being examined.

1. INTRODUCTION

In many applications the following problem arises. Let the n-stage shift register (the cascade of n delay elements) be given and let $f(x_1, x_2, \ldots, x_n)$ be the Boolean function of n variables which determined the dependency between the outputs of every stage of shift register and the input of the first one (so-called feedback Boolean function – FBF). Connection of both objects forms the general shift register generator (SRG). Further, let the SRG generate the binary cyclic sequence of a certain cyclic length. Then, it is natural to ask whether any FBF which realizes such sequencies exists, and, if so, to give the necessary and sufficient conditions for such FBF's. In our contribution we shall try to answer some questions concerning the cycles of length 2^n and $2^n - 1$ and to point out so far unsolved problems.

2. M- AND m-SEQUENCES

We shall start with the explanation of the action of general SRG. Let the stages of the shift register be numbered from the first delay element to the last one by positive integers $1, 2, \ldots, n$, the corresponding outputs of stages (variables of FBF) having the same indices. When the content of the shift register (its initial state) is $x_1, x_2, \ldots, x_n$ a consecutive state $yx_1 \ldots x_{n-1}$, where $y = f(x_1, \ldots, x_n)$ and $f(\ )$ is the FBF, will

appear after applying a shift pulse. Because of the finitness of number of stages (there are exactly 2^n different states) the sequence of at least $2^n + 1$ states must contain two identical ones; the shortest subsequence between identical states is called a cycle. Every SRG generates therefore the cycles except possibly for the first several states determined by the initial content of the shift register. Thus, the state diagram (a graphical representation of transitions between consecutive states of SRG) is decomposed into several connected subdiagrams, each of them forming a cycle with or without branches.

The m-sequences will be for us a cycle of length $2^n - 1$ states. For a given n, all m-sequences differ possibly by their vertex labeling. It is necessary, however, to point out that our definition of m-sequence is wider than usually, because we do not deal with its statistical properties, so that e.g. the pseudonoise sequences from [1] form a proper subset of our m-sequences.

The FBF can generate the m-sequence (it is understood with the corresponding shift register but for the sake of brevity we shall further speak only about FBF) in two ways: it produces two cycles (one of length $2^n - 1$ and other of length one) or one cycle (of length $2^n - 1$) with a branch (of length one). We shall prove the missing state in an m-sequence is just the state of n zeros (zero-state) or of n ones (one-state). First, let us recall Good's (or de Bruijn) diagram and the notion of the M-sequence.

Every state $x_1x_2 \dots x_n$ of SRG has two possible successors ($0x_1 \dots x_{n-1}$ and $1x_1 \dots x_{n-1}$) as well as two possible predecessors ($x_2 \dots x_n0$ and $x_2 \dots x_n1$), so that the state sequence from SRG is not arbitrary. If we, for some n, construct an oriented graph with 2^n vertices labelled by the states and with exactly two arrows entering and two arrows leaving every vertex according to its predecessors and successors, we obtain Good's diagram. A closed path through this diagram traversing each vertex exactly once is a sequence of all 2^n states (M-sequence). An m-sequence must be the part of an M-sequence, i.e. it is an M-sequence without a certain state.

3. THE NUMBER OF ALL m-SEQUENCES

Let us take three consecutive states of the M-sequence: $x_2x_3 \dots x_{n+1}$, $x_1x_2 \dots x_n$, $x_0x_1 \dots x_{n-1}$ (say). The removal of some state must not disconnect a cycle, so that if the missing state is $x_1x_2 \dots x_n$, the transition between $x_1x_3 \dots x_{n+1}$ and $x_0x_1 \dots x_{n-1}$ must exist. Considering also the primary transitions, the last condition implies $x_1 = x_2 = \dots = x_n$ and the possible missing state is zero- or one-state which can form either a cycle (zero or one) or a branch (zero or one).

Since there are $2^{2^{n-1}-n}$ possible different M-sequences (for a proof see [1]) the following theorem can be proved).

Theorem 1. *The number of different FBF's of n variables giving different m-sequences is* $2^{2^{n-1}-n+2}$.

Proof. Every M-sequence can turn into an m-sequence in four ways. It is possible to exclude either zero- or one-state and in both cases the missing state forms either a cycle or a branch. Since all $2^{2^{n-1}-n}$ M-sequences differ by their vertex labelling but each of them has the same transitions $00\ldots01 - 00\ldots0 - 10\ldots0$ and $11\ldots10 - 11\ldots1 - 01\ldots1$, the thus derived m-sequences are all different. On the other hand let some m-sequence be given and let its missing state be zero (say). Then this m-sequence must contain the transition $00\ldots01 - 10\ldots0$ (the other successor to $00\ldots01$ is just the zero-state and the same applies for the other predecessor to $10\ldots0$) and therefore it is possible to change it, by inserting the zero-state between $00\ldots01$ and $10\ldots0$, into an M-sequence being already included in the set of $2^{2^{n-1}-n}$ M-sequences. This and the fact that there is an one-to-one correspondence between FBF's and state diagrams completes the proof.

The direct corollary of the theorem is a necessary condition for FBF generating M- and m-sequences (see Table 1).

Table 1.

Fixed values of FBF in some entries for realizing M- and m-sequences

Entries of FBF	M-sequence	m-sequence with			
		a cycle		a branch	
		zero	one	zero	one
00...00	1	0	1	1	1
11...10	1	1	0	1	0
00...01	0	1	0	1	0
11...11	0	0	1	0	0

Notice the similarity between zero- and one-cycle (zero- and one-branch). If for zero-cycle (zero-branch) $f(x_1, \ldots, x_n) = y$ holds, then for one cycle (one-branch) $f(x_1, \ldots, x_n) = \bar{y}$ and vice versa ($x_1 \ldots x_n$ is one of the combinations of Table 1). It is possible however, to derive a more general result concerning a transformation of states. The state diagram of SRG is invariant with respect to the inversion of all states, e.g. an M-sequence changes into the M-sequence having the same order of inverse states; an m-sequence with zero-cycle changes into the m-sequence with one-cycle, etc. The transformation of an arbitrary state $x_1 \ldots x_n$ into $y_1 \ldots y_n$, where $y_i = \bar{x}_i$, changes the original FBF $f(x_1, \ldots, x_n)$ into $\overline{f(\bar{x}_1, \ldots, \bar{x}_n)}$ because the consecutive state is now $y_0 y_1 \ldots y_{n-1}$ where $y_0 = \overline{f(x_1, \ldots, x_n)} = \overline{f(\bar{y}_1, \ldots, \bar{y}_n)}$. It is sufficient therefore to consider only FBF's which realize always one of a couple of mutually complementary state diagrams.

As an example let us choose a linear FBF $a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n$, $a_i = 0$ or 1, producing the m-sequence with zero-cycle (in this case the number of nonzero coef-

ficients a_i is always even [2]). The new SRG generating the inverse m-sequence and one-cycle has as its FBF $a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n \oplus 1$ ($\bar{x}_i = x_i \oplus 1$, $1 \oplus 1 = 0$), which is also linear, although the resulting SRG is now nonlinear (for the definition of linear automaton see e.g. [2]).

4. SOME NECESSARY PROPERTIES OF FBF's

Finally, we shall deal with the truth table of FBF. A truth table of Boolean function $f(x_1, \ldots, x_n)$ is a table of all 2^n binary combinations of length n representing the values of variables x_i, $i = 1, 2, \ldots, n$, and the corresponding values of Boolean function. The binary combinations are usually arranged according to the increase of the binary numbers represented by them, and, at the same time, the least index of variable corresponds to the least significant digit in binary representation, and vice versa. As the decomposition of state diagram of SRG into pure cycles is equivalent to the existence of exactly one predecessor to every state, the necessary and sufficient condition for the FBF $f(x_1, \ldots, x_n)$ to realize only pure cycles is the equality $f(x_1, \ldots, x_n) = f'(x_1, \ldots, x_{n-1}) \oplus x_n$, or, which is the same, the bottom half of the values of FBF in the truth table is the complement of the top half.

As it has already been proved every m-sequence is obtainable from an M-sequence by changing the values of FBF in states 00 ... 0 and 10 ... 0 or 11 ... 1 and 01 ... 1 (note that now we record the states in the opposite order according to the entries in the truth table). When the SRG operates in one or two pure cycles (the case of M-sequences and some m-sequences), the above assertion for the truth table of FBF must hold. Considering only the values in the top half of the truth table without the values in entries 00 ... 0 and 01 ... 1 (let us call them the top variable part of the truth table) then this part must be complementary to the corresponding bottom variable part even for all m-sequences with a branch (clearly for other m-sequences and all M-sequences, too). Finally, it has been proved ([1] Theorem 5 of Chapter VI) that the FBF for $n > 2$ produces the odd number of pure cycles if and only if the top half of its truth table contains the odd number of ones. Since for M-sequences the values of FBF in the entries 00 ... 0 and 01 ... 1 are 1, and in the entries 10 ... 0 and 11 ... 1 are 0, the top as well as the bottom variable part of the truth table must contain also the odd number of ones. It must hold not only for M-sequences but also for all m-sequences.

Thus, we have proved the following useful theorem:

Theorem 2. *The necessary conditions for the truth table of FBF* $f(x_1, x_2, \ldots, x_n)$, $n > 2$, *to produce an* M- *or an* m-*sequence are*:

a) *the values of FBF in entries* 00 ... 0, 01 ... 1, 10 ,., 0 *and* 11 ... 1 *are given by Table* 1;

b) *the top variable part of the truth table is the complement of the bottom variable part*;

c) *the top as well as the bottom variable part of the truth table contains the odd number of ones*;

d) *if an FBF* $f(x_1, \ldots, x_n)$ *realizing some* M- *or* m-*sequence is known, the FBF* $\overline{f(\bar{x}_1, \ldots, \bar{x}_n)}$, *with the variable part of its truth table being written in the opposite order (from below upwards) to the variable part of the truth table of* $f(x_1, \ldots, x_n)$ *and with the corresponding change in remaining entries in accordance with Table 1, generates the complement of original state diagram.*

5. EXAMPLES

First, let us solve the case $n = 2$ which is not included in Theorem 2. As there exist one FBF realizing an M-sequence and four FBF's realizing m-sequences, all entries from Table 1 form the corresponding truth tables. For $n = 3$ the number of basic FBF's giving m-sequences with cycles is 2. The linear theory shows that also

Table 2.

Variable parts of the truth tables of 4 variable FBF's realizing M- and m-sequences

x_4	x_3	x_2	x_1	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
0	0	0	1	0	0	0	0	1	1	1	1
0	0	1	0	0	1	1	1	0	0	1	1
0	0	1	1	0	1	1	0	1	0	1	1
0	1	0	0	1	1	0	0	0	0	1	0
0	1	0	1	1	0	1	1	1	1	1	1
0	1	1	0	1	0	0	1	0	1	0	1

two linear FBF's exist for realizing an m-sequence with zero-cycle [2] ($x_1 \oplus x_3$ and $x_2 \oplus x_3$) so that no nonlinear FBF exists producing this state diagram. Two FBF's give an inverse state diagram (i.e. an m-sequence with one-cycle): $x_1 \oplus x_3 \oplus 1$ and $x_2 \oplus x_3 \oplus 1$. Finally, four FBF's form the m-sequence with a branch: the zero-branch $x_1 \oplus x_3 + \bar{x}_2\bar{x}_3$ and $x_2 \oplus x_3 + \bar{x}_1\bar{x}_3$ and their inverses (the one-branch) $\bar{x}_1\bar{x}_3 + x_1\bar{x}_2x_3$ and $\bar{x}_2\bar{x}_3 + \bar{x}_1x_2x_3$. The case of $n = 4$ is shown in Table 2 describing the top variable parts of the truth tables of 8 basic FBF's which allow, with the aid of Table 1 and complementations. all 64 FBF's to be obtained. Among them there are 14 nonlinear FBF's producing an m-sequence with zero-cycle (e.g. $x_2 + x_3 \oplus x_4$, $x_1 + x_2 \oplus x_4$, $x_1 \oplus x_2 + x_3 \oplus x_4$, etc.); only two are linear.

In general, for $n > 2$ there are $2^{2^{n-1}-n-1}$ variable parts, giving with the aid of Table 1 and of the condition d of Theorem 2 all M- and m-sequences, so that their

number rapidly increases with increasing n; for $n = 5$ there are already 1024 such variable parts from the 8192 satisfying the properties of Theorem 2.

As another example we shall show a simple method of M-sequence generator synthesis from the given linear SRG producing an m-sequence with zero-cycle. The latter can be defined by the irreducible and primitive polynomial $F(x)$ over GF(2): $F(x) = x^n \oplus c_{n-1}\, x^{n-1} \oplus \ldots \oplus c_1 x \oplus 1$. Since the linear SRG consists of the

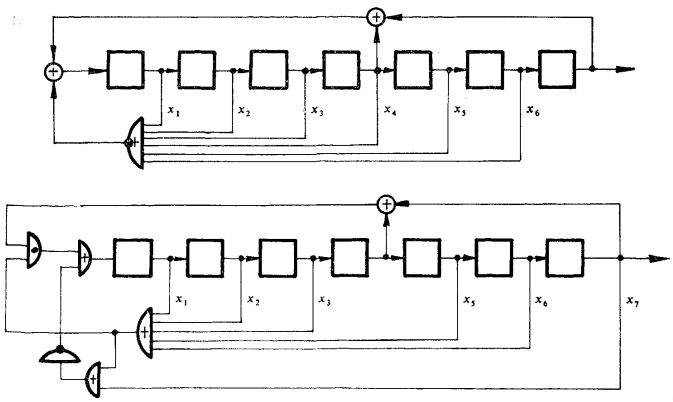

Fig. 1.

n-stage shift register with feedbacks from those delay units, to which there corresponds $c = 1$, to the first delay unit, its FBF is $f(x_1, x_2, \ldots, x_n) = x_n \oplus c_1 x_{n-1} \oplus \oplus \ldots \oplus c_{n-1} x_1$. The FBF $f_M(x_1, x_2, \ldots, x_n)$ of M-sequence generator and $f(x_1, x_2, \ldots \ldots, x_n)$ differ only in entries $00 \ldots 00$ and $10 \ldots 00$ (as it is shown in Table 1), so that

$$f_M(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n) \oplus \prod_{i=1}^{n-1} \bar{x}_i = f(x_1, x_2, \ldots, x_n) \left(\sum_{i=1}^{n-1} x_i\right) + \prod_{i=1}^{n} \bar{x}_i$$

Let e.g. $F(x) = x^7 \oplus x^3 \oplus 1$, i.e. $f(x_1, x_2, \ldots, x_7) = x_7 \oplus x_4$. Then $f_M(x_1, x_2, \ldots \ldots, x_7) = x_7 \oplus x_4 \oplus \bar{x}_1\bar{x}_2\bar{x}_3\bar{x}_4\bar{x}_5\bar{x}_6 = (x_7 \oplus x_4)(x_1 + x_2 + x_3 + x_5 + x_6) + + \overline{(x_1 + x_2 + x_3 + x_5 + x_6 + x_7)}$ and the corresponding SRG can be realized from the linear one by adding either one NOR circuit with six inputs and one mod 2 sum, or one OR circuit with five inputs, two OR circuits and one AND circuit with two inputs and one invertor (see Fig. 1).

6. CONCLUSION

In spite of a certain success in obtaining some necessary conditions for FBF's which facilitate the searching procedure among all FBF's, the gain for greater n is

not very high (the number of FBF's being necessary to test is by Theorem 2 $\sum_{i \text{ odd}} \binom{2^{n-1}-2}{i} = 2^{2^{n-1}-3}$, i.e. 2^{n-2}-fold). It is therefore necessary to find sufficient conditions ba means of which it would be possible to decide whether or not a certain FBF realizes an M- or an m-sequence. For the sake of completeness the same remains to be derived even for other types of state diagrams.

(Received December 4, 1969.)

REFERENCES

[1] Golomb S. W.: Shift Register Sequences. Holden-Day, San Francisco 1967.
[2] Gill A.: Linear Sequential Circuits. McGraw-Hill, New York 1966.

VÝTAH

Některé nelineární generátory s posuvnými registry

JOSEF PUŽMAN

V příspěvku se studují některé generátory s posuvnými registry produkující určité cyklické posloupnosti. Problém se soustřeďuje na vyhledání vhodných, obecně nelineárních, zpětnovazebních Booleových funkcí ke generování posloupnosti délky 2^n a $2^n - 1$. Odvozuje se počet takových Booleových funkcí a některé jejich nutné vlastnosti, což umožňuje značně zmenšit celkový objem Boleových funkcí, které je třeba prověřit.

Ing. Josef Pužman, Ústředí pro rozvoj automatizace a výpočetní techniky, Revoluční 24, Praha 1.