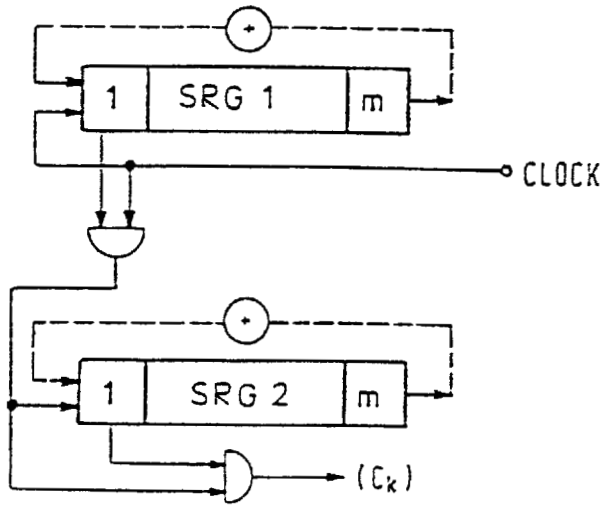
On the linear complexity of cascaded sequences

Rainer Vogel
Standard Elektrik Lorenz AG
Abt. CP/ERMF 2
Ostendstraße 3
7530 Pforzheim
RFA

In the papers [1][2] Kjeldsen derived very interesting properties of cascade coupled sequence generators. For applications in ciphering we are interested to know the linear complexity of such sequences. In the following we first consider the examples 1 and 2.

Example 1



This sequence-generator works as follows:
Shiftregister 1 (SRG 1) is shifted with every clock. If the output of this register is 1 shiftregister 2 (SRG 2) is shifted and the generated bit of SR 2 is used for c_k.

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 99-109, 1985.

If shiftregister 1 generates a 0 shiftregister 2 will not be shifted and the output of the generator is 0.

If we denote the sequence from shiftregister 1 with (a_k), the sequence from shiftregister 2 with (b_k), the sequence (c_k) at the output can be computed in the following way

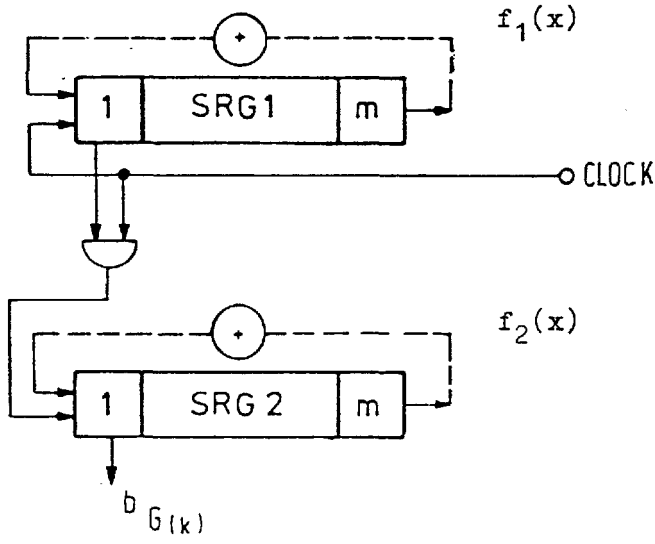
$$c_k = a_k \cdot b_{G(k)} \qquad k \varepsilon N$$

with $G(o) = 0$

$$G(k) = \sum_{i<k} a_i \qquad k \varepsilon N$$

(The last sum denotes a usual addition)

Example 2



If we are only interested to generate the sequence $b_{G(k)}$, we use the generator of example 2. This structure works in the following manner: Generates shiftregister 1 an 1 the register SRG 2 is shifted and the output of SRG 2 is used for the output of the generator. Otherwise SRG 2 is not shifted and the previous generated bit of SRG 2 is used as output bit.

Later we give further examples. To get some answers about the linear complexity, we begin with example 2. For if we have derived the minimal polynom g(x) of the sequence $(b_{G(k)})$, we can use known theorems (eg. Zierler [3]). Therefore we get for the minimal polynom h(x) of the sequence (c_k)

$$h(x) \mid f_1 \vee g.$$

$f_1 \vee g$ is the polynom with the zeros $\alpha \cdot \beta$, α zero of $f_1(x)$, β zero of $g(x)$.

$f_1 \vee g$ is also denoted Hadamard product of f_1 and g.

But first we still remember some properties of the sequences generated by the generator of example 1. More general formulations and proofs are in the papers [1], [2].

1. If the number of 1's computed over the period of (a_k) is relatively prime to the period p_2 of the sequence (b_k) then for the minimal period p of (c_k) holds the equation

   $$p = p_1 \cdot p_2.$$

   This conditions are always satisfied if the feedback polynoms of the shiftregister are primitive polynoms with the degree m. In this case we have then

   $$p = (2^m - 1).$$

2. The asumptions of the previous number are satisfied. Let $w_i\ (p_i)$ $i = 1,2$ the weight of (a_k) resp. (b_k) computed over the period p_1 resp. p_2, then for the frequency w of the 1's in (c_k) it holds

$$w = \prod_{i=1}^{2} \frac{w_i\ (p_i)}{p_i}$$

If (a_k) and (b_k) are PN-sequences with the period 2^m-1, we have

$$w = \prod_{i=1}^{2} \frac{2^{m-1}}{2^m-1} \hat{=} \frac{1}{4} .$$

General asumption for the rest of the paper: All feedbacks are primitive polynoms.

These last two results can be generalized on cascades with more than two stages. Further in the papers [1] [2] are results on the autocorrelation properties of such sequences.

Computation of the linear complexity of the sequence $(b_{G(k)})$.

All following proofs are based on a theorem, which we found in a very old book on algebra of Dickson [2]. (1900) In a slightly reformulation it says:

Theorem

$f_1(x)$, $f_2(x)$, ... $f_N(x)$ be the set of all irreducible polynoms of degree m and exponent e

$$e = (2^m - 1)/d.$$

$\lambda \varepsilon N$ be a number with the properties

(i) $(\lambda, d) = 1$

(ii) All prime divisors of λ are prime divisors of 2^m-1,

then holds

a) $\lambda \cdot m$ is the least number with the property $\lambda \cdot e \mid 2^{\lambda \cdot m} - 1$.

b) The polynoms $f_1(x^\lambda), \ldots f_N(x^\lambda)$ are irreducible of degree $m \cdot \lambda$ and exponent $\lambda \cdot e$ and the set $f_1(x^\lambda), \ldots f_N(x^\lambda)$ consists of all polynoms with these properties.

Proof [4, page 22]

In the special case

$$e = \lambda = 2^m - 1$$

$$d = 1$$ we get

a) $m \cdot (2^m - 1) = \min \{ k: (2^m - 1)^2 \mid 2^k - 1 \}$

b) The set $f_1(x^{2^m - 1}), \ldots f_N(x^{2^m - 1})$

is the set of all polynoms of degree $m \cdot (2^m - 1)$ with the exponent $(2^m - 1)^2$.

With the help of this theorem we examine the sequence $(b_{G(k)})$ and prove

$f_2(x^{2^m - 1})$ is the minimal polynom of $(b_{G(k)})$.

Proof

$(a_k) \longleftrightarrow f_1(x)$

$(b_k) \longleftrightarrow f_2(x)$

} primitive polynoms of degree m

With $p := 2^m - 1$ the sum $G(k)$ has the properties

$$G(k + n \cdot p) = G(k) + n \cdot G(p)$$

$$G(p) = 2^{m-1}$$

Using the operator $f(E^p)$ corresponding to the polynom $f(x^p)$, we get (E is the shift operator)

$$f_2(E^p)\, b_{G(k)} = \sum_{i=o}^{m} C_i \cdot b_{G(k+i\cdot p)}$$

$$= \sum_{i=o}^{m} C_i \cdot b_{G(k)+i\cdot G(p)}$$

$$= \sum_{i=o}^{m} C_i \cdot b_{G(k)+i\cdot 2^{m-1}}$$

$$(k' := G(k)) = \sum_{i=o}^{m} C_i \cdot b_{k'+i\cdot 2^{m-1}}$$

$$= f_2(E^{2^{m-1}})\, b_{k'}$$

$$= (f_2(E))^{2^{m-1}}\, b_{k'} = 0$$

With the theorem we now get

1. $f_2(x^{2^{m-1}})$ is the minimal polynom of the sequence $(b_{G(k)})$, because the polynom is irreducible.

   Thus the linear complexity of $(b_{G(k)})$ is $m \cdot (2^m - 1)$.

2. The sequence $(b_{G(k)})$ has the minimum period $(2^m - 1)^2$, because the exponent of $f_2(x^{2^{m-1}})$ is $(2^m - 1)^2$.

Remarks

1. With two cascaded shiftregisters of length 61 the linear complexity of $(b_{G(k)})$ has the value
   $K = 1.4 \cdot 10^{20}$.

2. If the cascade consists of n registers of length m, we get
   linear complexity $\geq m \cdot (2^m - 1)^{n-1}$ Period = $(2^m - 1)$

3. It is possible to replace shiftregister 1 through a nonlinear shiftregister which generates a de Bruijn sequence. In this case it is still possible to give a lower bound for the linear complexity.

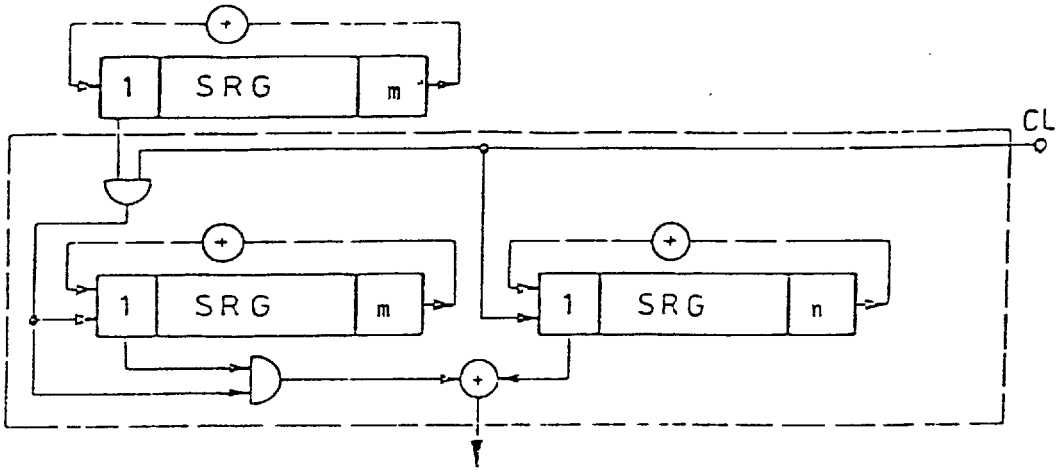
   Lower bound for the linear complexity in Example 1

   From previous considerations we see: The minimal polynom h(x) of the sequence $(c_k) = (a_k \cdot b_{G(k)})$ is a divisor of the polynom $f_1(x) \vee f_2(x^{2^m-1})$.

   But what about the degree of h(x)? The period $(2^m - 1)^2$ of the sequence (c_k) is an odd number. The irreducible components of h(x) have the power = 1. If we write the sequence (c_k) with the zeros of h (x) there must be zeros of order $(2^m - 1)^2$. The degree of each irreducible component with such a zero is equal $m(2^m - 1)$. For the degree of h(x) we get therefore the lower bound deg $h(x) \geq m \cdot (2^m - 1)$.

   It is only possible to get lower bounds, but this is sufficient for the applications.

Example 3



The sequences of example 1 have bad pseudo-noise properties, because the frequency of 1's at the output is only 1/4. To remove this defect we add (mod 2) another linear shiftregister sequence to the sequence (c_k). If we assume $(m,n) = 1$ the following Lemma shows that the resulting sequence has better pseudo-noise properties.

Lemma [1]

The periods of the sequences (a_k) und (b_k) are relatively prime. Each m-tuple of weight w occurs with the frequency $f^w (1-f)^{m-w}$ in (a_k) and with the frequency $g^w (1-g)^w$ in (b_k). Then each m-tuple of the weight w in the sequence $(a_k + b_k)$ occurs with frequency

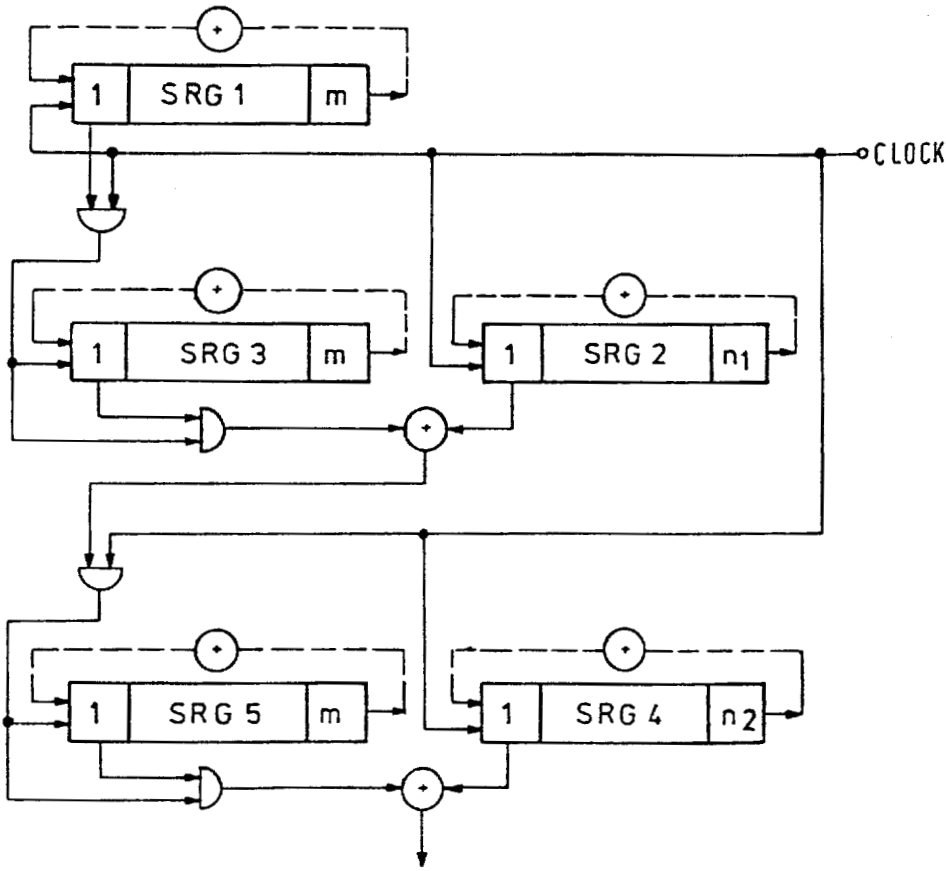
$$h^w (1-h)^{m-w} \quad \text{with}$$

$$h = f + g - 2 f \cdot g.$$

If the sequence of SRG 3 is a PN-sequence of period $(2^n - 1)$ $(m,n) = 1$) in the output sequence each m-tuple of weight w has thus the frequency $(\frac{1}{2})^m$.

For the linear complexity K of the output we have $K > m \cdot (2^m - 1)$.

Example 4



This example shows how a repetition of the method of example 1 leads to sequences of very high complexity. If we assume that all feedback polynoms are primitive polynoms, it is possible to proof that in each stage the number of 1's is relatively prime to $2^m - 1$. The output sequence of this structure has the least period $(2^m - 1)^3 \cdot (2^{n1} - 1) \cdot (2^{n2} - 1)$ if all the starting vektors of all registers are not equal 0.

As an example for the estimation of the linear complexity we examine the sequence (c_k) with the minimum period $\underbrace{(2^m - 1)^3}_{p^3} \cdot \underbrace{(2^{n1} - 1)}_{q}$.

We can represent this sequence with the zeros of its minimal polynom h(x). Two cases are possible.

Case 1

h(x) has zeros of order $p^3 \cdot q$. With the help of the Theorem it is easy to show that each irreducible component with such a zero has the degree $m\,(2^m - 1)^2 \cdot n_1$.

Case 2

There are no zeros of order $p^3 \cdot q$.
But in this case exists zeros of order p^3 of the polynom h(x). Again with the Theorem we get: The irreducible component that contains such a zero has the degree $m \cdot (2^m - 1)^2$.

Both cases yields for the linear complexity K

$$K \geq m \cdot (2^m - 1)^2.$$

From these considerations we can recognize that it is possible to generate sequences with very high complexities with such cascades.

References

1 Kjeldsen, Andresen
Some Randomness Properties
of Cascaded Sequences
IEEE TRANS INF. Th. Vol IT 26
No. 2, 227 ff (1980)

2 Johnsen, Kjeldsen
Loop-free Compositions of Certain
Finite Automata
INF. AND CONTROL 22, 303 - 319
(1973)

3 Zierler, Mills
Products of linear recurring seq.
J. Algebra 27, 1, 147 - 151 (1973)

4 Dickson
Linear groups with an exposition
of Galois field theory
Springer 1900 (Dover Publ. 1958)