A NOTE ON SEQUENCES GENERATED BY CLOCK CONTROLLED SHIFT REGISTERS*

Bernard Smeets
Department of Computer Engineering
University of Lund
P.O. Box 118, S-221 00 Lund, SWEDEN

Summary - In this paper the linear feedback shift registers are determined that can generate the output sequence of two types of clock controlled shift registers suggested by P. Nyffeler. For one type of clock control sufficient conditions are given which guarantee that maximum linear complexity is obtained. Furthermore, it is shown that the randomness properties for sequences of maximal linear complexity depend on clocking procedure.

1. Introduction.

Pseudo random sequences generated by linear feedback shift registers are used in various crypto systems as running key generators. In general several linear feedback shift registers are used to produce the final pseudo random sequence. Since such a sequence is periodic, it can be generated by one single linear feedback shift register of finite length. The length of shortest linear feedback shift register that is able to produce the output sequence of a configuration is referred to as the linear complexity of the sequence. If the linear complexity of some periodic sequence is L, then 2L consecutive symbols will be sufficient to determine both the linear feedback and the initial state of a linear feedback shift register that can generate the sequence [1]. As a consequence, a configuration of linear feedback shift registers must be such that the generated sequences do have a large linear complexity.

This paper deals with two types of clock controlled shift registers, suggested by P. Nyffeler [2]. First the linear feedback shift registers are determined that can generate the output sequence of the clock controlled shift registers. For one configuration of clock control sufficient conditions are given which guarantee that maximal linear complexity is obtained. In the sequel of this paper (a_n) will denote a linear recurring sequence over GF(q) with period T_a whose minimal polynomial f_a is irreducible over GF(q), has degree

---

* This work was supported in part by the National Swedish Board for Technical Development under grants 81-3323 and 83-4364 at the University of Lund.

F. Pichler (Ed.): Advances in Cryptology - EUROCRYPT '85, LNCS 219, pp. 142-148, 1986.

$m \geq 1$, and satisfies $f_a(0) \neq 0$. Furthermore, (b_n) will denote a periodic sequence over GF(q) with period T_b. Throughout the paper it is assumed that (a_n) and (b_n) are generated by the linear feedback shift registers LFSRa and LFSRb respectively. It is also assumed that neither (a_n) nor (b_n) equals the null-sequence.

2. Cascade Clock Control

Consider the configuration of two shift registers as given in Fig. 1. The clock of the first shift register, LFSRa, is controlled by the sequence generated by the second shift register, LFSRb. At time instant $n>0$ LFSRb is clocked once and LFSRa is clocked $c(b_{n-1})$ times, where c is some function: $GF(q) \rightarrow \{0,\ldots,T_a-1\}$. To avoid a trivial situation, it is assumed that c(x) is not zero for all x in GF(q). Note that the function c may be part of the key information in a crypto system.

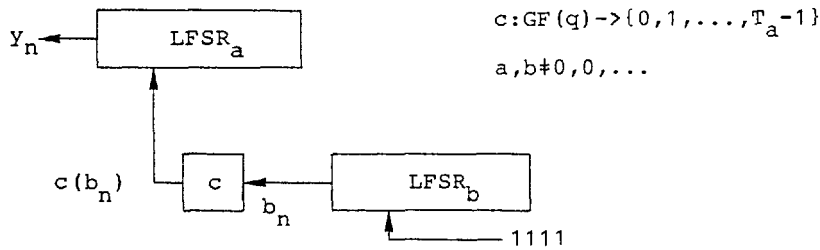

Fig. 1 Cascade Clock Control with two shift registers.

The sequence (y_n) obtained at the output is

$$y_n = a_{s(n)}, \quad \text{where} \quad s(n) = \sum_{k=0}^{n-1} c(b_k), \quad n=0,1,2,\ldots \tag{1}$$

Let T_b denote the period of (b_n). Furthermore, let $S=s(T_b)$, i.e., the number of clock pulses generated in one period of (b_n).

Theorem 1. The sequence (y_n) generated by the cascade clock control configuration of LFSRa and LFSRb has a minimal polynomial $f^*(x)$ such that

$$f^*(x) \mid f^{(S)}(x^{T_b}), \tag{2}$$

where $f^{(k)}$ denotes the minimal polynomial of the k-decimated sequence of (a_n), i.e., (a_{kn}).

Proof Let k and l be integers and let $k>0$. Consider now the sequence (a_{kn+l}), i.e., the l-th phase shift of (a_{kn}). It is easy to see that

$$h_{k,l}(x):=f^{(k)}(x)\sum_{n=0}^{\infty}a_{nk+l}x^n \in GF(q)[x] \quad \text{where} \quad \deg h_{k,l} < \deg f^k \tag{3}$$

Consider the formal power series $y(x)$ associated with the sequence (y_n), defined by $y(x)=\sum_{n=0}^{\infty} y_n x^n$. From (1) we have

$$y(x)=\sum_{n=0}^{\infty} y_n x^n=\sum_{n=0}^{\infty} a_{s(n)}x^n=\sum_{n=0}^{\infty}\sum_{m=0}^{T_b-1} a_{s(m)+nS}x^{m+nT_b}=$$

$$=\sum_{m=0}^{T_b-1} x^m \sum_{n=0}^{\infty} a_{s(m)+nS}x^{nT_b}. \tag{4}$$

Multiplying $y(x)$ with $f^{(S)}(x^{T_b})$ and using (3) and (4) gives us

$$f^{(S)}(x^{T_b})y(x)=\sum_{m=0}^{T_b-1} x^m h_{S,s(m)}(x^{T_b}):=h(x) \in GF(q)[x]$$

From (4) and $\deg x^m<T_b$, for $0\le m<T_b$, we have

$$\deg h(x) \le (T_b-1) + T_b(\deg f^{(S)}(x) -1) < T_b \deg f^{(S)}(x) \tag{5}$$

This implies that $y(x)=h(x)/f^{(S)}(x^{T_b})$. However, we also have $y(x)=h^*(x)/f^*(x)$, $\deg h^*<\deg f^*$, where $f^*(x)$ is the minimal polynomial for (y_n). The theorem follows from the minimality of f^*.

Under favourable conditions it can be shown that the polynomial given in (2) is the minimal polynomial of (y_n). Specializing a theorem by Serret on irreducible polynomials, see [3], we obtain the following result:

Theorem 2. Suppose $f^{(S)}(x)$ has degree d and has order $T_{a,S}$. Suppose also that
(i) all prime factors of $T_b \ge 2$ divide $T_{a,S}$ but not $(q^d-1)/T_{a,S}$,
(ii) $q^d \equiv 1 \bmod 4$ if $T_b \equiv 0 \bmod 4$,
then $f^{(S)}(x^{T_b})$ is prime over $GF(q)$. Hence, it is the minimal polynomial of (y_n). Furthermore it has degree $T_b d$ and has order $T_b T_{a,S}$.

When $f(x)$ is a maximum-length polynomial we have the following interesting special case of Theorem 2.

Corollary 1. If f(x) is a maximum-length polynomial of degree $m \geq 1$,

(i) $\gcd(S, q^m-1)=1$,

(ii) all prime factors of T_b divide T and

(iii) if the hypothesis (ii) in Theorem 2 is satisfied,

then $f^{(S)}(x^{T_b})$ is the minimal polynomial of (y_n).

Proof. We only need to show that condition (i) in Theorem 2 is satisfied. If f(x) is a maximum-length polynomial of degree $m \geq 1$, then f(x) has period $T=q^m-1$. From $\gcd(S, q^m-1)=1$ it follows that $T_{a,S}=T$. Together with the hypothesis that all the prime factors p of T_b divide T and $p \nmid 1$, this shows that the condition (i) in Theorem 2 is satisfied.

For some special instances of the binary case this corollary coincide with results given in [4] and [5]. An other result of Theorem 2 is the following corollary:

Corollary 2. Let p, an odd prime, divide 2^n-1 for some positive integer n. If the order of 2 mod p^k equals e for k=2,...d, where e is the order of 2 mod p, but $p^{d+1} \nmid 2^e-1$, then p^d divides 2^n-1.

Proof. Consider first the case $n=n'=$order of 2 mod p. Assume that $2^n-1=p^cQ$, with $p \nmid Q$ and $1 \leq c < d$. Let e be the order of 2 mod p^c, $e=\mathrm{ord}_2 p^c$, and correspondingly $e_1=\mathrm{ord}_2 Q$. Note that $\mathrm{lcm}(e,e_1)=n$. Since $\gcd(p,Q)=1$ we have $A:=\mathrm{ord}_2(p^cQ)^2 = \mathrm{lcm}(\mathrm{ord}_2 p^{2c}, \mathrm{ord}_2 Q^2)$. If $2c \leq d$, then $A \leq \mathrm{lcm}(e,e_1Q) \leq nQ$. If $2c>d$, then $A \leq \mathrm{lcm}(ep^{2c-d}, e_1Q) \leq nQp^{2c-d}$. Consider now the cascade clock control of two maximum length shift registers of length n. Theorem 2 implies that the minimal polynomial f of the output sequence is prime over GF(2) , is of degree $B:=n(2^n-1)$ and has period $(p^cQ)^2$. However we just have shown that deg $f=A<B$, hence $c>d$. Finally, let $n>n'$. Note that $2^{n'}-1 \mid 2^n-1$ iff $n' \mid n$ and $n'=\mathrm{ord}_2 p \mid n$ because $2^n=1$ mod p. This proves that $p^d \mid 2^{n'}-1 \mid 2^n-1$.

Note: this result can be obtained also by using only partial results on which Theorem 2 is based, [3].

3. Clock Controlled Sampling

Consider the configuration of two linear feedback shift registers as shown in Fig. 2. The output of the first register LFSRa is sampled under control of the outputs of the second register LFSRb and a mapping g from GF(q) onto GF(2). If $g(b_n)=1$ then the output symbol of LFSRa is loaded in cell D and it will become the new output y-symbol. Otherwise the new output y-symbol equals the previous y-symbol. It will be assumed that g is not the zero-map, i.e., not all elements of GF(q) are mapped to only 0.

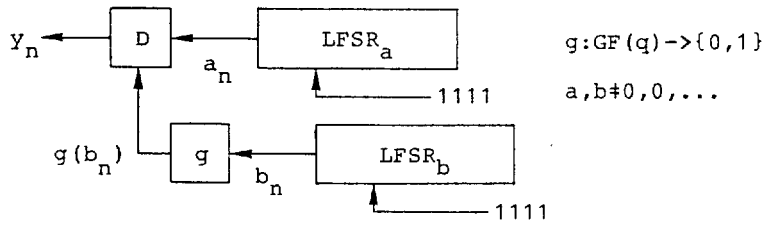

Fig. 2 Clock controlled sampling.

The sequence (y_n) obtained at the output is

$$y_n=a_{s(n)}, \quad \text{where} \quad s(n)= \max_{\substack{0\le k\le n \\ g(b_k)=1}} k, \quad n=0,1,2,... \tag{6}$$

where g is a mapping as explained above. Furthermore, assume that b_0 is such that $g(b_0)=1$. This restriction assures that the first output symbol in (y_n) is a_0 instead of the initial state of the memory cell D.

Theorem 3. The sequence (y_n) generated by the clock controlled sampling configuration of LFSRa and LFSRb has a minimal polynomial f^* such that

$$f^*(x) \mid f^{(T_b)}(x^{T_b}). \tag{7}$$

Proof Imitate the proof of Theorem 1 with T_b instead of S and use the fact that $s(nT_b+m)=nT_b+s(m)$.

For the binary case this result is connected with a result given in [2]. Let a be a zero of f(x), then it is easily shown that a is also a zero of (7). Thus f(x) divides $f^{(T_b)}(x^{T_b})$, hence it is much harder to guarantee that (7) is the minimal polynomial of (y_n).

4. Randomness aspects

Besides the linear complexity of the generated sequences, their statistical properties are of importance. Particularly, it is desirable that the symbols in the sequence do not depend (too much) on the preceding symbols. If for a sequence x the average conditional entropies $H(X_n)$,$H(X_n|X_{n-1})$, $H(X_n|X_{n-1},X_{n-2})$,...,$H(X_n|X_{n-1}..X_{n-m})$ form a rapid decreasing function then there is a strong dependence between a symbol and the symbols preceding it. From Theorem 2 it is clear that, as far as the linear complexity of the generated sequence is concerned, the clock function in the first type of clock control only plays a secondary roll. Though different clock functions give rise to different output sequences, the same

linear complexity may be obtained. For example, if we take the maximum-length polynomial $f(x)=x^5+x^2+1$ over GF(2) and $b=1/(x^5+x^3+1)$, then the clock functions c_0 and c_1, defined as $c_0(0)=0$, $c_0(1)=1$ and $c_1(0)=1$, $c_1(1)=2$, will result in two different sequences which have the same linear complexity L=155. However, the randomness properties of the two sequences (will generally) differ. This is illustrated by Fig. 3 which shows how the conditional entropies $H(X_n),H(X_n|X_{n-1}),H(X_n|X_{n-1},X_{n-2}),\ldots,H(X_n|X_{n-1}..X_{n-10})$ differ for the two different clock functions in the previous example.

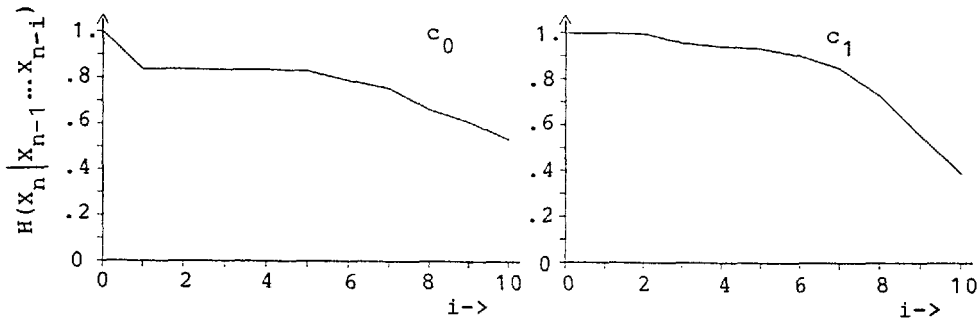

Fig. 3 The average conditional entropies $H(X_n),\ldots,H(X_n|X_{n-1}..X_{n-m})$ of the output symbols using two different clock functions c_0 and c_1

The symbol dependence observed when clocking is done according to c_0 is due to the fact that LFSRa stands still for almost half of the time. As a result of this observation one has to choose the clock function not only with respect to the linear complexity of the sequence but also the randomness properties have to be taken into account.

In the case of clock controlled sampling a symbol in the output stream may also be a repetition. This happens when no new symbol is loaded into the D element. Such repetitions can be avoided when one increases the number of instances in which a new symbol is loaded into D. However this causes the output sequence to become more identical to the sequence generated by LFSRa.

5. Conclusion

It has been shown that under certain well defined conditions we can guarantee a high linear complexity for the sequences produced by the cascade clock control configuration. The random properties of these sequences depend on the method of clocking. Furthermore, for the clock controlled sampling configuration it is much harder to guarantee a high linear complexity and (or) good random properties.

Acknowledgement

Thanks are due to Tore Herlestam for introducing me into this field and for the many stimulating discussions.

References

[1] J.L. Massey, "Shift-Register Synthesis and BCH Decoding", IEEE Trans. on Inf. Th., IT-15, Jan. 1969, pp. 122-127.

[2] P. Nyffeler, "Binäre Automaten und ihre Linearen Rekursionen," Ph.D dissertation, University of Bern, Switzerland, 1975.

[3] R. Lidl and H. Niederreiter, "Encyclopedia of Mathematics and its Applications, Finite Fields, Vol.20, Addison-Wesley Publishing Company, Reading, Mass., 1983.

[4] T. Beth and F.C. Piper, "The stop-and-go generator", Proceedings of EUROCRYPT 84 (Paris, 1984), to appear.

[5] W.G. Chambers and S.M. Jennings, "Linear Equivalence of Certain BRM Shift-Register Sequences," Electr. Letters, Vol. 20, Nov. 1984, pp. 1018-1019.