PSEUDO RANDOM PROPERTIES OF CASCADE CONNECTIONS OF CLOCK CONTROLLED SHIFT REGISTERS

Dieter Gollmann

Institut für Systemwissenschaften
Johannes Kepler Universität Linz , Austria

Abstract. Shift registers are frequently used in generators of pseudo random sequences (see [1]). We will examine how cascade connections of clock controlled shift registers perform when used as generators of pseudo random sequences. We will derive results for the period, for the linear recursion and for the pseudo-randomness of their output sequences.

1.Introduction.

Cascade connections of clock controlled shift registers are a generalization of the idea of a "clock controlled automaton". Clock controlled automata were examined by P.Nyffeler [4]. A clock controlled shift register switches to its next state when input "one" is sent to its clock and remains unchanged when input "zero" is applied. We connect these clock controlled shift registers to a cascade connection as follows. The input to the cascade connection is sent to the clock of the first register. The input to the clock of the i-th register, i≥2 , is the sum (modulo 2) of the input to the clock of the (i-1)-th register and the output of the (i-1)-th register. Likewise the output of the cascade connection is the sum of the input to the clock of the last register and of the output of the last register (see also [2]).

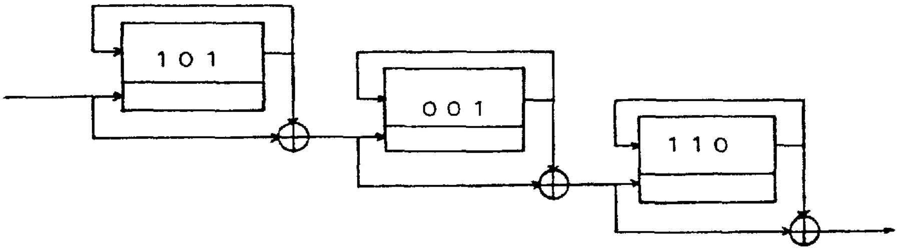

Fig.1. A cascade connection of clock controlled shift registers.

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 93-98, 1985.

All shift registers in the cascade connection shall be of the same length p, p>2 prime. Furthermore we exclude shift registers with the initial states "all zero" or "all one". We will examine output sequences generated by the input sequence 111... .

2.Results.

2.1. Periods of the output sequences.

Regard a cascade connection of n clock controlled shift registers of length p. Obviously any state trajectory - and therefore any output sequence - of this cascade connection has at most period p^n. We are able to prove

Theorem 1: Any output sequence of any cascade connection of n clock controlled shift registers of length p, p>2 prime, has period p^n.

Proof: Let k_i denote the number of ones in the output sequence of a cascade connection of i shift registers during the period p^i.
First we prove that any state trajectory of any cascade connection of n shift registers has period p^n.
This is obviously true for n=1 as the initial state of the shift register is non-trivial. With the same argument we get $\gcd(k_1,p)=1$.
Now assume that any state trajectory of any cascade connection of n shift registers has period p^n and that $\gcd(k_n,p)=1$.
The period of a state trajectory of a cascade connection of n+1 shift registers has to be a multiple of p^n and the number of ones sent to the last register during this period has to be a multiple of p. So we have $m \cdot k_n = n \cdot p$ for some natural numbers m,n. From $\gcd(k_n,p)=1$ we get m=p, the period of any state trajectory of any cascade connection of n+1 shift registers is p^{n+1}.
Let d denote the number of ones stored in the last register. We have

$$k_{n+1} = d(p^n-k_n) + (p-d)k_n = p(p^{n-1}d+k_n) - 2dk_n$$

and $\gcd(k_{n+1},p)=1$ follows from $\gcd(k_n,p)=\gcd(d,p)=1$ and p>2.
Finally the period of any output sequence of any cascade connection of n shift registers has to divide the period of the corresponding state trajectory. As $\gcd(k_n,p)=1$ this period has to be p^n.

q.e.d.

2.2. Linear recursion.

We introduce some further notations.

Let $(q_{i,1},..,q_{i,p})$ denote the initial state of the i-th register of some cascade connection of clock controlled shift registers.

Let $f_{i,k_{i-1}}$ denote the characteristical polynomial of the sequence $q_{i,1+mk_{i-1}}$, $1\le m\le p$, where the indices $1+mk_{i-1}$ are computed modulo p.

Then the property "p^2 does not divide $2^{p-1}-1$" is sufficient to prove that the characteristical polynomial f of the output sequence generated by the given initial state can be computed by

<u>Theorem 2</u>: $f(x) = (1-x)\prod_{i=1}^{n} f_{i,k_{i-1}}(x^{(p^{i-1})})$.

For the proof of this theorem see [3].

It is important to note that the linear recursion depends on the initial states of the shift registers in the cascade connection.

"p^2 does not divide $2^{p-1}-1$" is no severe restriction as $p=1093$ is the first prime number to violate this condition.

Theorem 2 generalizes P.Nyffeler's result for the linear recursion of clock controlled automata [4].

For prime numbers p with $C_p(x) = \sum_{i=0}^{p-1} x^i$ irreducible over GF(2) we can deduce

<u>Theorem 3</u>: $f(x) = 1-x^{(p^n)}$.

2.3. Pseudo-randomness.

Consider a sequence $R := ((R_i,q_i))_{i\in\mathbb{N}}$ of registers R_i with initial states q_i. The $2^k\times 2^k$-matrices $T(k;l) := (t(k;l)_{ij})$ give the relative frequencies of the transformations of the sequences of length k caused by the cascade connection of the registers $R_{(l-1)k+1},\dots,R_{lk}$.

<u>Lemma 1</u>: For any natural number k any cascade connection of k shift registers can transform any input sequence $x_1..x_k$ to any given output sequence $y_1..y_k$.

<u>Corollary</u>: $\forall k,l\in\mathbb{N},\forall i,j=1,..,2^k \ (\ t(k;l)_{ij} \ge \frac{1}{p^k} \ )$.

Proof of Lemma 1: This lemma is true for k=1 as the initial states of all shift registers are non-trivial.

We now assume that the lemma holds for some given number k.

Consider an arbitrary input sequence $x_0..x_k$, an arbitrary output sequence $y_0..y_k$ and an arbitrary cascade connection of k+1 shift registers.

$y_0=0$: We set register k+1 to the initial state 1..0 (the zero is at the output of the register). This initial state transforms some sequence $y'_1..y'_k$ to $y_1..y_k$.

Let q be the state of the first k registers that transforms $x_1..x_k$ to $y'_1..y'_k$. Furthermore there exists a state $\delta^{-1}(q,x_0)$ that is transformed by x_0 to q.

If input x_0 and initial state $\delta^{-1}(q,x_0)$ yield output zero the initial state of the last register shall be 1..0, otherwise ..01 .

Now $x_0..x_k$ is transformed to $y_0..y_k$.

$y_0=1$: We start with the last register in the initial state 0..1 and proceed as above.

If input x_0 and initial state $\delta^{-1}(q,x_0)$ yield output zero the initial state of the last register shall be 0..1, otherwise ..10 .

The corollary follows from the fact that p^k is the period of any state trajectory of any cascade connection of k shift registers of length p.

q.e.d.

T(k;l) is a primitive stochastic matrix for all $k,l \in \mathbb{N}$. We can make use of the following lemma.

Lemma 2: Let T be a stochastic matrix of dimension n×n with $\lambda := \min_{i,j} p_{ij} > 0$. Let d be a n-vector with $d \neq 0$, $\sum_{i=1}^{n} d_i = 0$. We define

$$d^* := Td \ , \ \Delta_0 := \sum_{i=1}^{n} |d_i| \ , \ \Delta_1 := \sum_{i=1}^{n} |d_i^*| \ .$$

We get: $\Delta_1 \leq (1 - n\lambda)\Delta_0$.

The proof of Lemma 2 is similiar to the proof of Lemma 4.1. in [5].

Theorem 4: With Lemma 1 and Lemma 2 we get for the matrices $T(k;l)$

$$\|\prod_{l=1}^{n} T(k;l)\Delta\| \leq (1-(\tfrac{2}{p})^k)^n\|\Delta\| \quad \text{for all } n\in\mathbb{N}.$$

Δ gives the difference between the initial distribution of the input sequences of length k and the vector $(2^{-k},..,2^{-k})^t$ (i.e. equal distribution of the sequences of length k).

Let $rf_n(y_1..y_k)$ denote the relative frequency of the sequence $y_1..y_k$ in the output sequence of some cascade connection of n shift registers during the period p^n. From Theorem 4 we get

$$\lim_{n\to\infty} rf_n(y_1..y_k) = 2^{-k} .$$

We extend this result to the information entropy

$$H_k(n) := \sum_{(y_1..y_k)=(0..0)}^{(1..1)} rf_n(y_1..y_k)\cdot ld(rf_n(y_1..y_k)) \; :$$

$$\lim_{n\to\infty} H_k(n) = k .$$

When we increase the length of a cascade connection the relative frequencies of the word of length k converge towards equal distribution for any number k, the entropy converges towards its maximum.

Remark. The sequence of matrices $(T(k;l))_{l\in\mathbb{N}}$ constitutes an inhomogenous Markov chain where the matrices $T(k;l)$ can be taken only from a finite set. Markov chains of this kind have been studied by J.Wolfowitz already in 1963 (see [6]).

The rate of convergence $(1-(\frac{2}{p})^k)$ given in Theorem 4 cannot be improved for k=1. If a shift register of length p contains only a single one we get

$$T(1;1) = \frac{1}{p}\begin{pmatrix} p-1 & 1 \\ 1 & p-1 \end{pmatrix} \quad \text{and} \quad T(1;1)\begin{pmatrix} d \\ -d \end{pmatrix} = \frac{p-2}{p}\begin{pmatrix} d \\ -d \end{pmatrix} .$$

3. Conclusion.

We build a cascade connection from clock controlled shift registers of equal length p, p>2 prime, where no shift register is in a trivial initial state. Any output sequence of such a cascade connection has period p^n (i.e. maximal period), the linear recursion of any output sequence can be computed directly from the initial states of the shift registers (except for the case "p^2 divides $2^{p-1}-1$"). For suitable prime numbers p we have linear recursion of length p^n independent of the initial states.

The sequences of length k occur in the output sequence of a cascade connection with relative frequencies converging towards equal distribution when we increase the length of the cascade connection. This holds for all numbers k.

Literature:

[1] H.Beker, F.Piper, Cipher Systems, Northwood, London, 1982

[2] D.Gollmann, On the identification of certain non-linear networks of automata, in: Cybernetics and Systems Research, ed.R.Trappl, North Holland, 1982

[3] D.Gollmann, Kaskadenschaltungen taktgesteuerter Schieberegister als Pseudozufallszahlengeneratoren, Dissertation, Universität Linz, 1983

[4] P.Nyffeler, Binäre Automaten und ihre linearen Rekursionen, Dissertation, Universität Bern, 1975

[5] E.Seneta, Non-negative Matrices, George Allen&Unwin Ltd, London, 1973

[6] J.Wolfowitz, Products of indecomposable, aperiodic, stochastic matrices, PAMS, 14, 733-737, 1963