Likelihood that a pseudorandom sequence generator has optimal properties

A. Fúster-Sabater(1) and L.J. García-Villalba(1)

(1) Department of Information Processing and Coding
Institute of Applied Physics, C.S.I.C., Serrano 144, 28006 Madrid, Spain
amparo@iec.csic.es

Abstract

The authors prove that the probability of choosing a nonlinear filter of m-sequences with optimal properties, that is, maximum period and maximum linear complexity, tends asymptotically to 1 as the linear feedback shift register length increases.

Pseudorandom sequence generators have multiple applications in radar systems, simulation, error-correcting codes, spread-spectrum communication systems and cryptography. One of the most interesting pseudorandom sequence generators is the nonlinear filter of m-sequences, as it produces sequences with optimal properties.

A nonlinear filter \( F \) is a \( k \)th order nonlinear function applied to the \( L \) stages of an LFSR with a primitive feedback polynomial. Let \( \{a_n\} \) be the LFSR output sequence; then the generic element \( a_n \) is \( a_n = \alpha^n + \alpha^{2^n} + \ldots + \alpha^{2^{(L-1)}}, n \), \( \alpha \in GF(2^L) \) being a root of the LFSR characteristic polynomial. Thus, the filtered sequence \( \{z_n\} \) can be represented as

\[
\{z_n\} = \{F(a_n, \ldots, a_{n+L-1})\}
\]

\[
= \sum_{i=1}^{N} \left( C_i \alpha^{E_i n} + \cdots + (C_i \alpha^{E_i n})^{2^{(r_i-1)}} \right) = \sum_{i=1}^{N} C_i \{S_n^{E_i}\}
\]

with \( r_i \) being the cardinal of coset \( E_i \), \( N \) the number of cosets \( E_i \) with binary weight \( \leq k \) and \( C_i \in GF(2^L) \) constant coefficients. Note that the \( i \)th term in the expression of \( \{z_n\} \) corresponds to the characteristic sequence \( \{S_n^{E_i}\} \) of coset \( E_i \). Therefore \( \{z_n\} \) can be written as the termwise sum of the characteristic

---

\( ^6 \)Work supported by CICYT (Spain) under grant TIC95-0800. Electronics Letters. Vol. 34, No. 7, pp. 646-647. April 1998. Elect. Lett. Online No: 19980499, INSPEC Accession Number: 5896277
sequences associated with every coset $E_i$. From the above the following can be noted:

(i) It can be proved \[2\] that every coefficient $C_i \in GF(2^{r_i})$, so that as long as $C_i$ is within its corresponding field, we shift along the sequence $\{S_{E_i}^n\}$.

(ii) If $C_i = 0$, then coset $E_i$ does not contribute to the linear complexity of the filtered sequence $\{z_n\}$.

(iii) The period of $\{z_n\}$ is the minimum common multiple of the periods of its corresponding characteristic sequences $\{S_{E_i}^n\}$ whose values are the divisors of $2^L - 1$.

Taking the above considerations into account, we can compute the probability of choosing a nonlinear filter $F$, whose output sequence $\{z_n\}$ has optimal properties. In fact, let $nfk$ be the number of $k$th order nonlinear filter functions and $nfm$ the number of the previous functions whose output sequences $\{z_n\}$ have maximum linear complexity ($C_i \neq 0, \forall i$), then

$$P_r = \frac{nfm}{nfk} = \frac{(2^{r_1} - 1)(2^{r_2-1} - 1)\cdots(2^N - 1)}{(2^L - 1)2^{(L-1)}\cdots2^{(l)}}$$

$$= \frac{\prod_{i=1}^{N} (2^{r_i} - 1)}{(2^L - 1)2^{(L-1)}\cdots2^{(l)}}$$

If $L$ is prime (which is the most common case), then all the cardinals $r_i$ equal $L$. Consequently, $nfm$ and $P_r$ can be rewritten as

$$nfm = (2^L - 1)^N = (2^L - 1)^{\frac{k}{2}} \sum_{i=1}^{k} \left(\begin{array}{c} L \\ i \end{array}\right) = (2^L - 1)^{\frac{k}{2}}$$

$$P_r = \frac{(2^L - 1)^{\frac{k}{2}}}{(2^L - 1)^{\frac{k}{2}} \cdots 2^{(l)}} > \frac{(2^L - 1)^{\frac{k}{2}}}{2^{N_k}} = \left(\frac{2L - 1}{2L}\right)^{\frac{k}{2}} = \left(1 - \frac{1}{2L}\right)^{\frac{N_k}{2L}} \\
\text{It is a well known fact that if } b_n \to \infty, \text{ then } (1 - b_n^{-1})^{b_n} \to e^{-1}. \text{ As } N_k \leq 2^L - 1, \text{ if } k \simeq L/2 \text{ then } N_k \simeq 2^{L-1}. \text{ Thus, } \\
P_r > e^{-\frac{N_k}{2L}} \simeq e^{-\frac{L}{2}}$$

For $L = 257$ (a typical value for the LFSR in communication systems), $P_r > 0.998$
In addition, this kind of nonlinear filter also has maximum period. Indeed, as those filters contain the characteristic sequences $\{S_n^E_i\}$ associated with all the cosets $E_i$, they also contain that of coset $E_1$ the period $[3]$, of which is $2^{L} - 1$.

Conclusions: Nonlinear filters of $m$-sequences are believed to be excellent pseudorandom sequence generators. This is not only because they are very easy to implement with high-speed electronic devices, but also because they are highly likely to produce sequences with optimal properties.

Acknowledgment: This work is supported by CICYT (Spain) under grant TIC95-0800.

References

[1] RUEPPEL, R.A.: ‘Stream cipher’ in SIMMONS, G. (Ed.): ‘Contemporary cryptology: The science of information integrity’ (IEEE Press, New York, 1991), pp. 65-134

[2] LIDL, R., and NIEDERREITER, H.: ‘Introduction to finite fields and their applications’ (Cambridge University Press, Cambridge, 1986)

[3] PARK, B., CHOI, H., CHANG, T., and KANG, K.: ‘Period of sequences of primitive polynomials’, Electron. Lett., 1993, 29, (4), pp. 390-392