

A Comment on “Bound for Linear Complexity of BBS Sequences”

Sean Murphy

Information Security Group
Royal Holloway
University of London
Egham, Surrey TW20 0EX, U.K.

March 19, 1998

Abstract

Montoya Vitini *et al* gave a lower bound for the linear complexity of Blum–Blum–Shubb sequences. We show this result is incorrect.

The lower bound for the linear complexity of Blum–Blum–Shubb sequences [1] given by Montoya Vitini *et al* [3] depends on Proposition 1 of this paper [3]. This Proposition can be phrased as:

A binary sequence of length $2p_2q_2$ (p_2, q_2 odd primes with certain properties) has linear complexity at least p_2q_2 .

The properties of the odd primes p_2, q_2 are not relevant to the justification of Proposition 1 given in [3], and the claim is not true for any odd primes p_2, q_2 . We give a counterexample for the odd primes $p_2 = 5$ and $q_2 = 11$ that satisfy the criteria for primes given in [3]. We consider the linear feedback shift register (LFSR) represented by the polynomial

$$(X^2 + 1)Q_5(X)Q_{11}(X) = X^{16} + X^{11} + X^5 + 1$$

of degree 16, where Q_i denotes the i^{th} cyclotomic polynomial over $GF(2)$ [2]. This LFSR generates the following periodic sequence s of period $2p_2q_2 =$

$2 \times 5 \times 11 = 110$:

00000000000000001000010000110001100011100111001111011110
1111111111111110111101111001110011100011000110000100001

s has linear complexity 16 and not at least $p_2q_2 = 5 \times 11 = 55$ as claimed by the proposition.

A minimal polynomial for a sequence of period $2p_2q_2$ must divide

$$X^{2p_2q_2} - 1 = (X^2 + 1)Q_{p_2}(X)^2Q_{q_2}(X)^2Q_{p_2q_2}(X)^2.$$

The justification of Proposition 1 given in [3] claims that if a minimal polynomial for a sequence of period $2p_2q_2$ does not divide $Q_{p_2}(X)Q_{q_2}(X)Q_{p_2q_2}(X)$, then it must be of the form $A(X)Q_{p_2}(X)Q_{q_2}(X)Q_{p_2q_2}(X)$, where $A(X)$ divides $Q_{p_2}(X)Q_{q_2}(X)Q_{p_2q_2}(X)$. This claim is false as, for example, the LFSR represented by the polynomial $(X^2 + 1)Q_{p_2}(X)Q_{q_2}(X)$ generates a sequence of period $2p_2q_2$.

References

- [1] BLUM, L. BLUM, M., and SHUB, M.: A simple unpredictable pseudo-random number generator, *SIAM J. Comput.*, 1986, **15**, pp364–383
- [2] LIDL, R., and NIEDERREITER, H.: Introduction to Finite Fields and their Applications Cambridge University Press, 1994
- [3] MONTROYA VINTINI, F., MUÑOZ MASQUÉ, J., and PEINADO DOMÍNGUEZ, A.: Bound for the Linear Complexity of BBS Sequences, *Electronics Letters*, 1998, **34**, pp450–451