On Linear Recursion and Pseudorandom Measure*

János Folláth

University of Debrecen, Faculty of Informatics, Debrecen, Hungary
follathj@inf.unideb.hu

Abstract

Mauduit and Sárközy studied pseudorandom binary sequences of

$$E_N = \{e_1, \dots, e_N\} \in \{-1, +1\}^N$$

and introduced a mesure of pseudorandomness of binary sequences [1]:

Definition. *Combined (well-distribution-correlation) PR-measure of order k E_N is defined as:*

$$Q_k(E_N) = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_k} \right|.$$

They also gave a construction of a sequence with good pseudorandom measure. Later Brandstätter and Winterhof in [2] gave a lower bound for the linear complexity profile in the terms of the correlation measure (a measure contained in the previously defined one). The following result gives an upper bound for the pseudorandom measure for sequences with given linear complexity:

Theorem. *Let $\sigma = s_0, s_1, \dots$ be a homogeneous linear recurring sequence in $K = \mathbb{F}_q$ with a square-free minimal polynomial $m(x)$. Let $m(x)$ have the irreducible factorization $m(x) = m_1(x) \dots m_h(x)$, such that the $m_i(x)$ polynomials have degrees $d_1, \dots, d_h$. Then the corresponding sequence over $F = \mathbb{F}_{q^k}$, $k = l.c.m(d_1, \dots, d_h)$*

$$E_{q^k-1} = \{(-1)^{s_0}, (-1)^{s_1}, \dots, (-1)^{s_{q^k-1}}\}$$

then

$$\max_{l \le k} Q_l(E_{q^k-1}) \le 9dq^{k/2}k$$

where $d = \max_i c_i \frac{q^k-1}{q^{d_i}-1}$ with $c_i < q$ constant depending only on m_i.

*This research was supported by the European Union and the State of Hungary, co-financed by the European Social Fund in the framework of TÁMOP 4.2.4. A/2-11-1-2012-0001 'National Excellence Program'

Keywords: psuedorandom sequences, correlation measure, linear complexity, pseudorandom measure

References

[1] Christian Mauduit and András Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arith. 82 (4) pp 365-377., 1997

[2] Nina Brandstätter and Arne Winterhof, *Linear Complexity Profile of Binary Sequences With Small Correlation Measure*, Period. Math. Hungar. 52 (2) pp 1-8., 2006