Distribution of recurrent sequences modulo prime powers (abstract)

Richard G.E. Pinch

University of Cambridge, Department of Pure Mathematics and Mathematical Statistics,
16 Mill Lane, Cambridge CB2 1SB, U.K.

Abstract. We study the distribution of linear recurrent sequences modulo p^n for prime p when the auxiliary polynomial is irreducible and the period is maximal. We show that such a sequence takes each possible value equally often up to an error of order $p^{n/2}$.

1 Introduction

In this paper we study the possible periods of linear recurrent sequences modulo p^n for prime p in the case when the the auxiliary polynomial is irreducible and the period is maximal: see [7]. We show that such a sequence takes each possible value equally often up to an error of order $p^{n/2}$, generalising the corresponding result for sequences to a prime modulus, [2], [3].

The result has applications to the generation of pseudo-random numbers [5], [6] and answers a question of Mascagni [4].

We give the results in the case $p = 2$, although they generalise readily to any characteristic.

Lemma 1. *Let x_n be a sequence modulo $M = 2^m$ with period R and let $Z(b)$ be the number of times a value b occurs in one full period of the sequence. Suppose that*

$$\left|\sum_{n=0}^{R-1} \zeta_M^{x_n}\right| < E$$

for ζ_M any M-th root of unity other than 1. Then

$$|Z(b) - R/M| \le E.$$

So an estimate for the error in an exponential sum can be converted into an estimate for the difference between the distribution of a recurrent sequence and the uniform distribution, and conversely.

Lemma 2. *Let f be a polynomial of degree k, irreducible over $\mathbf{Q}_2$, and let x_n be a recurrent sequence in $\mathbf{Z}_2$ with auxiliary polynomial f. Suppose that x_n has period exactly $2^k - 1$ modulo 2^l but not modulo 2^{l+1}. Then x_n has period exactly $\left(2^k - 1\right) 2^{m-l}$ modulo 2^m for $m \ge l$.*

We note that $(2^k-1)2^{m-1}$ is the maximum possible period for such a sequence.

Theorem 3. *Suppose that x_n is a sequence modulo $M=2^m$, with $m \geq 3$, satisfying a recurrence relation of degree k, with an auxiliary polynomial irreducible over $\mathbf{Q}_2$ and with maximal period $R=(2^k-1)2^{m-1}$. Then*

$$\left|\sum_{n=0}^{R-1} \zeta_M^{x_n}\right| \leq C_k 2^{m/2}.$$

where ζ_M is an M-th root of unity other than 1.

References

1. M. Ganley (ed.), *Cryptography and coding III*, IMA conference series (n.s.), vol. 45, Institute of Mathematics and its Applications, Oxford University Press, 1993, Proceedings, 3rd IMA conference on cryptography and coding, Cirencester, December 1991.
2. Rudolf Lidl and Harald Niederreiter, *Finite fields*, Encyclopaedia of Mathematics and its applications, vol. 20, Addison–Wesley, Reading Mass., 1983, 0-201-13519-1, Republished, Cambridge University Press, 1984.
3. ———, *Introduction to finite fields and their applications*, second ed., Cambridge University Press, 1994, First edition 1986.
4. M. Mascagni, S.A. Ciccaro, D.V. Pryor, and M.L. Robinson, *A fast, high-quality and reproducible lagged-Fibonacci pseudrandom number generator*, Technical report SRC-TR-94-115, Supercomputing Research Center, IDA, Bowie, MD, U.S.A., Feb 1994.
5. Harald Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), no. 6, 957–1041.
6. ———, *Recent trends in random number and random vector generation*, Ann. Oper. Res. **31** (1991), 323–346.
7. R.G.E. Pinch, *Recurrent sequences modulo prime powers*, In Ganley [1], Proceedings, 3rd IMA conference on cryptography and coding, Cirencester, December 1991., pp. 297–310.

This article was processed using the LaTeX macro package with LLNCS style