On the Distinctness of Decimations of ℓ-Sequences

Mark Goresky* Andrew Klapper† Ram Murty‡

January 18, 2002

1 Introduction

Let q be a prime integer such that 2 is primitive modulo q. The class of binary sequences known as ℓ-sequences can be described in five ways [2]. An ℓ-sequence is the output sequence from a maximal period feedback with carry shift register (FCSR) with connection number q. It is a single codeword in the Barrows-Mandelbaum arithmetic code. It is the 2-adic expansions of a rational number r/q, where $\gcd(r, q) = 1$. It is the reverse of the binary expansion of the same rational number r/q. And it is the sequence $a_i = (A2^{-i} \text{mod } q)\text{mod } 2$, where $\gcd(A, q) = 1$. (By $(x \text{ mod } q)\text{mod } 2$ we mean first reduce x modulo q to a number between 0 and $q-1$, then reduce the result modulo 2.) The period of such an ℓ-sequence is $q - 1$.

These sequences are known to have several good statistical properties similar to those of m-sequences. They form families with remarkable *arithmetic crosscorrelations*. The arithmetic cross-correlation $C(\mathbf{a}, \mathbf{b})(\tau)$ (with shift τ) of $\mathbf{a} = a_0, a_1, \cdots$ and $\mathbf{b} = b_0, b_1, \cdots$ is the number of ones minus the number of zeroes in one period of (the periodic part of) the sequence $\mathbf{c} = c_0, c_1, \cdots$ formed by adding $\mathbf{a}$ to $\mathbf{b}$ *with carry* [3]. This sequence $\mathbf{c}$ may also be described as the coefficient sequence of the 2-adic number $\alpha + \beta$ where

$$\alpha = \sum_{i=0}^{\infty} a_i 2^i \quad \text{and} \quad \beta_\tau = \sum_{i=0}^{\infty} b_{i+\tau} 2^i.$$

A pair of sequences has *ideal arithmetic correlations* if $C_{\mathbf{a},\mathbf{b}}(\tau) = 0$ for every τ.

Theorem 1.1 *([3]) Every pair of cyclically distinct sequences in S has ideal arithmetic correlations.*

*The Institute for Advanced Study, School of Mathematics, (www.math.ias.edu/~goresky/). Research partially supported by N.S.F. grant # 0002693.

†Dept. of Computer Science, 779A Anderson Hall, University of Kentucky, Lexington, KY, 40506-0046 and the Institute for Advanced Study, School of Mathematics. E-mail: klapper@cs.uky.edu. Project sponsored by the National Science Foundation under grant # 9980429.

‡Queen's University, Kingston, Ontario, K7L3N6, Canada, (www.mast.queensu.ca/ murty).

Recall that the d-decimation of the sequence $\mathbf{a} = a_0, a_1, \cdots$ is the sequence $\mathbf{a}^d = a_0, a_d, a_{2d} \cdots$. On the basis of extensive experimental evidence (covering all primes less than $50,000$), we made the following conjecture.

Conjecture 1.2 *If $q > 13$ and $\mathbf{a}$ is an ℓ-sequence based on a prime q, then every (distinct) pair of decimations $\mathbf{a}^d$, $\mathbf{a}^e$ of $\mathbf{a}$ is cyclically distinct, provided d and e are relatively prime to $q-1$.*

The conjecture implies that the set of decimations of $\mathbf{a}$ is a family of $\phi(q-1)$ sequences with period $q-1$ and ideal arithmetic correlations. This result would be in stark contrast to the case of ordinary correlations, where there are well known upper bounds on the size of a family of sequences with bounded correlations. In this paper we report on progress toward proving Conjecture 1.2. We do not have a complete proof, but in many cases can show that decimations are distinct.

2 Distinct Decimations

First note that $\mathbf{a}^d$ is cyclically distinct from $\mathbf{a}^e$ if and only if $\mathbf{a}^{de^{-1}}$ is cyclically distinct from $\mathbf{a}$ (where e^{-1} is computed modulo $q-1$). In this paper we show that for various d, the decimation $\mathbf{a}^d$ is cyclically distinct from $\mathbf{a}$. Throughout we assume $q > 13$.

2.1 The case $d = -1$

Theorem 2.1 *The decimation $\mathbf{a}^{-1}$ (reversal) is cyclically distinct from $\mathbf{a}$.*

Proof sketch: This is proved using a previous result [2] which characterizes the numbers of occurrences of bit patterns of lengths t and $t+1$ in $\mathbf{a}$, where $t = \log_2(q+1)$. If $\mathbf{a}$ equals a shift of its reversal, then the number of occurrences of a bit pattern in $\mathbf{a}$ equals the number of occurrences of the reversal of the bit pattern. By considering a series of such bit patterns we derive enough constraints on q to obtain a contradiction. $\square$

2.2 The case of small d

By the fifth characterization of an ℓ-sequence, $\mathbf{a}^d$ is a cyclic permutation of $\mathbf{a}$ if and only if there exists $A \in \mathbf{Z}/(q)$ such that $(A2^{-id} \bmod q) \bmod 2 \equiv (2^{-i} \bmod q) \bmod 2$ for every i. By assumption, 2 is primitive modulo q, so this holds if and only if $(Ax^d \bmod q) \bmod 2 \equiv (x \bmod q) \bmod 2$ for every x. That is, the map $x \mapsto Ax^d$ permutes the set E of even elements modulo q.

Using this point of view and deep results from analytic number theory [1] we obtain the following results.

Theorem 2.2 *For q sufficiently large, the decimation $\mathbf{a}^d$ is cyclically distinct from $\mathbf{a}$ whenever*

$$d \leq \frac{q}{2^8(1+\log_e(q))^4}.$$

Proof sketch: We define

$$f_E(x) = \begin{cases} 1 & \text{if } x \in E \\ 0 & \text{otherwise.} \end{cases}$$

We proceed using Fourier analysis of f_E. Let ζ be a primitive complex qth root of 1 and let

$$\hat{f}_E(b) = \frac{1}{q}\sum_{c=0}^{q-1} f_E(c)\zeta^{-bc}$$

be the cth Fourier coefficient of f_E. Thus by Fourier inversion,

$$f_E(a) = \sum_{b=0}^{q-1} \hat{f}_E(b)\zeta^{ba}.$$

Suppose as above that $x \mapsto Ax^d$ permutes E. Then

$$\sum_{x\in E} f_E(Ax^d) = \sum_{b=0}^{q-1} \hat{f}_E(b) \sum_{x\in E} \zeta^{bAx^d}.$$

The left hand side equals $|E| = (q+1)/2$. Let

$$S_b = \sum_{x\in E} \zeta^{bAx^d} = \sum_{x=0}^{(q-1)/2} \zeta^{bA2^dx^d}$$

If $b = 0$, then $\hat{f}_E(b) = (q+1)/(2q)$ and $S_b = |E| = (q+1)/2$. Thus

$$\frac{q^2-1}{4q} = |\sum_{b=1}^{q-1} \hat{f}_E(b)\zeta^{ba}| \le (\sum_{b=1}^{q-1} |\hat{f}_E(b)|) \max_{b\ne 0} |S_b|.$$

Lemma 2.3 *We have*

$$\sum_{b=1}^{q-1} |\hat{f}_E(b)| \le 1 + \frac{1}{2}\ln(\frac{q-3}{2}).$$

Thus

$$\frac{q^2-1}{4q} \le \left(1 + \frac{1}{2}\ln(\frac{q-3}{2})\right) \max_{b\ne 0} |S_b|. \tag{1}$$

Sums of the form S_b have been estimated by Davenport and Heilbronn [1]. Their results can be improved to show

Lemma 2.4 *For $b \ne 0$ and $d > 1$ we have*

$$S_b \le q^{3/4} d^{1/4}.$$

Combining this with equation (1) proves the theorem. $\square$

2.3 The case $d = (q+1)/2$

Now suppose $d = (q+1)/2$. Then $Ax^d \equiv Ax \bmod q$ if x is a square, and $Ax^d \equiv -Ax \bmod q$ otherwise. Suppose that $x \mapsto Ax^d \bmod q$ permutes the even elements $\{0, 2, \cdots, q-1\}$ and define $\sigma(x) = 1$ if x is even and $\sigma(x) = -1$ if x is odd.

Lemma 2.5 *For all* $x \in \{0, 1, 2, \cdots, q-1\}$ *we have*

$$\sigma(x) = J(x, q)\sigma(Ax)$$

and

$$\sigma(x) = J(A, q)\sigma(A^2 x),$$

where $J(x, q)$ *is the Jacobi symbol of* x *over* q*.*

This puts sufficiently many constraints on A to derive a contradiction.

Theorem 2.6 *Suppose that* $(q+1)/2$ *is odd. Then the decimation* $\mathbf{a}^{(q+1)/2}$ *is cyclically distinct from* $\mathbf{a}$*.*

3 Conclusions

We have shown that many decimations of an ℓ-sequence $\mathbf{a}$ are cyclically distinct from $\mathbf{a}$. There is experimental evidence that all such decimations are cyclically distinct. This remains an open problem.

References

[1] H. Davenport and H. Heilbronn, *Proc. London Math. Soc..*, **41** (1936) pp. 449-453.

[2] A. Klapper and M. Goresky, Feedback Shift Registers, Combiners with Memory, and 2-Adic Span, *Journal of Cryptology* **10** (1997) pp. 111-147.

[3] A. Klapper and M. Goresky, Arithmetic Cross-Correlations of FCSR Sequences, *IEEE Transactions on Information Theory* **43** (1997) pp. 1342-1346.