SIAM J. Discrete Math.
Vol. 18, No. 1, pp. 130–140

ON DECIMATIONS OF ℓ-SEQUENCES*

MARK GORESKY†, ANDREW KLAPPER‡, RAM MURTY§, AND IGOR SHPARLINSKI¶

Abstract. Maximal length feedback with carry shift register sequences have several remarkable statistical properties. Among them is the property that the arithmetic correlations between any two cyclically distinct decimations are precisely zero. It is open, however, whether all such pairs of decimations are indeed cyclically distinct. In this paper we show that the set of distinct decimations is large and, in some cases, all decimations are distinct.

Key words. feedback with carry shift register, arithmetic correlation, exponential sum, binary sequence, p-adic number

AMS subject classifications. 11A07, 11B50, 11L03, 11L07, 11L26, 11T23, 94A55, 94B40

DOI. 10.1137/S0895480102403428

1. Introduction.

If $\mathbf{a} = (a_0, a_1, a_2, \dots)$ is a periodic binary sequence, let $\mathbf{a}_\tau = (a_\tau, a_{\tau+1}, a_{\tau+2}, \dots)$ denote the τ-shifted sequence. If $\mathbf{a}, \mathbf{b}$ are periodic binary sequences with the same period T we say they are *cyclically distinct* if $\mathbf{a}_\tau \neq \mathbf{b}$, for every shift τ with $0 < \tau < T$.

Associate to $\mathbf{a}$ and $\mathbf{b}_\tau$ the 2-adic integers

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

We recall that if $\bar{b}_{i+\tau} = 1 - b_{i+\tau}$ denotes the complementary bit, then $-\beta_\tau = 1 + \sum_{i=0}^{\infty} \bar{b}_{i+\tau} 2^i$. Let

$$\gamma = \alpha - \beta_\tau = \sum_{i=0}^{\infty} c_i 2^i$$

be the difference. The sequence of bits $\mathbf{c} = (c_0, c_1, \dots)$ is eventually periodic (with period T), and the *arithmetic cross-correlation* $C_{\mathbf{a},\mathbf{b}}(\tau)$ is defined to be the number of zeroes minus the number of ones in a single window of size T within the periodic part of $\mathbf{c}$. The pair of sequences $\mathbf{a}, \mathbf{b}$ is said to have *ideal arithmetic cross-correlation* if $C_{\mathbf{a},\mathbf{b}}(\tau) = 0$ for every τ. In this paper we discuss families $\mathcal{S}$ of periodic binary sequences such that every pair $\mathbf{a}, \mathbf{b} \in \mathcal{S}$ of elements has ideal arithmetic cross-correlation. Further background on 2-adic numbers can be found in a book by

*Received by the editors March 4, 2002; accepted for publication (in revised form) January 20, 2004; published electronically July 20, 2004. Parts of this research were performed while the second and fourth authors were visitors at the Institute for Mathematical Sciences, National University of Singapore.

http://www.siam.org/journals/sidma/18-1/40342.html

†The Institute for Advanced Study, School of Mathematics, Princeton, NJ 08540 (goresky@ias.edu, www.math.ias.edu/∼goresky/). This author's research was partially supported by NSF grant 0002693.

‡Department of Computer Science, 779A Anderson Hall, University of Kentucky, Lexington, KY, 40506-0046, and the Institute for Advanced Study, School of Mathematics (klapper@cs.uky.edu). This author's research was partially supported by NSF grant 9980429.

§Department of Mathematics, Queen's University, Kingston, ON K7L 3N6, Canada, and the Institute for Advanced Study, School of Mathematics (murty@mast.queensu.ca).

¶Department of Computing, Macquarie University, NSW 2109, Australia (igor@ics.mq.edu.au).

Koblitz [15] and in a paper by Klapper and Goresky [14]. Further background on arithmetic correlations can be found in another paper by Goresky and Klapper [8].

The existence of such families is surprising in light of the Welch bound [11], which states that if $\mathcal{S}$ is a collection of S cyclically distinct binary sequences of period T, then there exist $\mathbf{a}, \mathbf{b} \in \mathcal{S}$ and a shift τ such that the (usual) periodic cross-correlation

$$c_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{T-1} (-1)^{a_i - b_{\tau+i}}$$

satisfies

$$c_{\mathbf{a},\mathbf{b}}(\tau) \geq T\sqrt{\frac{S-1}{ST-1}}.$$

Thus the Welch bound can be broached, by replacing the usual cross-correlation c with the arithmetic cross-correlation C.

The particular sequences of interest are called *long* sequences or ℓ-sequences; they are in many ways analogous to the binary m-sequences. Let q be a prime number such that 2 is a primitive root modulo q (meaning that the powers of 2 account for all the nonzero elements in $\mathbf{Z}/(q)$). Then a binary ℓ-sequence is any sequence of the form

$$a_i = (A2^{-i} \bmod q) \mod 2, \tag{1.1}$$

where $A \in \mathbf{Z}/(q)$ is nonzero. This equation means the following. Let $b = 2^{-1} \in \mathbf{Z}/(q)$ be the inverse of 2, modulo q. First compute Ab^i and reduce modulo q to obtain a number between 0 and $q-1$. Then reduce this number modulo 2. The sequence (1.1) is strictly periodic with period $q-1$, and different choices of A give rise to cyclic shifts of the same "base" sequence $a_i = (2^{-i} \bmod q) \mod 2$. (Up to a shift, this sequence may be described as the coefficient sequence of the 2-adic expansion of the fraction $-1/q$; it is also the reverse of the binary expansion of the fraction $1/q$.) These sequences have been studied since Gauss [7]. The related sequences $(g^i \bmod q) \mod \ell$ are used in the Digital Signature Standard and are important for an attack due to Nguyen and Shparlinski [18].

Such ℓ-sequences may be generated using feedback with carry shift registers as described in [13, 14], where their role in stream ciphers was investigated; see also [5] and [16]. This method of generating ℓ-sequences (and their mod p generalizations) was discovered independently by Marsaglia and Zaman [17] in special cases and by Couture and L'Ecuyer [4] in general, who proposed using them as pseudorandom number generators for Monte Carlo simulations.

These ℓ-sequences exhibit important randomness properties. In [1] it was shown that they have perfect distribution properties: for any $d < \log q$, every d-tuple of bits occurs either $\lceil (q-1)/d \rceil$ or $\lfloor (q-1)/d \rfloor$ times in a single period, where hereafter we use $\ln z$ and $\log z$ to denote the natural and binary logarithms of $z > 0$, respectively.

Let $\mathbf{x} = \mathbf{a}^d$ be the d-fold decimation of $\mathbf{a}$. That is, $x_i = a_{di}$. We say this decimation is *allowable* if d is relatively prime to $q-1$. In [8] it was shown that cyclically distinct allowable decimations of a single ℓ-sequence have ideal arithmetic cross-correlation; see the following theorem.

Theorem 1.1. *Let q be a prime number such that 2 is a primitive root modulo q and let $\mathbf{a} = (a_0, a_1, \dots)$ be an ℓ-sequence of period $q-1$. Let $\mathbf{x} = \mathbf{a}^d$ and $\mathbf{y} = \mathbf{a}^e$*

be allowable decimations of $\mathbf{a}$ *by* d *and* e*, respectively. Suppose* $\mathbf{x}$ *and* $\mathbf{y}$ *are cyclically distinct. Then for any shift* τ *the arithmetic crosscorrelation vanishes:* $C_{\mathbf{x},\mathbf{y}}(\tau) = 0$*.*

This theorem provides a family S of periodic sequences with ideal arithmetic cross-correlation. Unfortunately, however, even if $d \neq e$, the sequences $\mathbf{x}$ and $\mathbf{y}$ may fail to be cyclically distinct. On the basis of extensive experimental evidence the following conjecture was made [8].

Conjecture 1.2. *If* $q > 13$ *is prime,* 2 *is primitive modulo* q*, and* $\mathbf{a}$ *is an* ℓ*-sequence based on* q*, then every pair of allowable decimations of* $\mathbf{a}$ *is cyclically distinct.*

It is relevant to remark that by the celebrated result of Hooley [12], under the extended Riemann hypothesis, 2 is primitive for a set of primes of positive relative density.

If Conjecture 1.2 holds for a prime q, then the resulting family $\mathcal{S}$ consists of $\varphi(q-1)$ distinct elements with ideal arithmetic correlation (where φ is the Euler function). We have verified this conjecture for all primes $q < 2,000,000$. It can be restated in very elementary terms as follows.

Let $q > 13$ be a prime number such that 2 is primitive mod q. Let E be the set of even integers $0 \leq e \leq q-1$. Fix A with $1 \leq A \leq q-1$. Suppose the mapping $x \mapsto Ax^d \mod q$ preserves (but permutes the elements within) the set E. Then $d = 1$ and $A = 1$. The equivalence between these two statements follows from the fact that $\mathbf{a}^d$ and $\mathbf{a}^e$ are cyclically distinct if and only if $\mathbf{a}$ and $\mathbf{a}^h$ are cyclically distinct, where $h = d(e^{-1} \bmod q-1)$.

2. Previous and current results.

Conjecture 1.2 has turned out to be surprisingly resistant to proof. Suppose q is prime, 2 is a primitive root mod q, $\mathbf{a}$ is an ℓ-sequence with prime connection integer $q > 13$, and d is relatively prime to $q-1$. In [8] and [9] the following was shown.

Theorem 2.1. *Suppose*

(i) *either* $d = -1$ *(or, equivalently,* $d = q-2$*);*

(ii) *or* $q \equiv 1 \bmod 4$ *and* $d = (q+1)/2$*;*

(iii) *or*

$$1 < d \leq \frac{(q^2-1)^4}{2^{16}q^7(\ln q + 2)^4} \sim \frac{q}{(16 \ln q)^4}.$$

Then the decimation $\mathbf{a}^d$ *is cyclically distinct from* $\mathbf{a}$*.*

In this paper we give the complete proof of Theorem 2.1 (iii) (which was only sketched in [9]) and we improve substantially on this bound by removing the $\ln q$ factors. Let $\mathbf{a}, q, d$ be as above.

Theorem 2.2. *If* $d > 1$ *and*

$$d \leq \frac{(q^2-1)^4}{2^{24}q^7}$$

or if $d < 0$ *and*

$$|d| \leq \frac{(q^2-1)^4}{2^{25}q^7},$$

then the decimation $\mathbf{a}^d$ *is cyclically distinct from* $\mathbf{a}$*.*

Finally, we show that, asymptotically for large q, the collection of counterexamples to Conjecture 1.2 is a vanishingly small fraction of the set of all allowable decimations.

THEOREM 2.3. *For any fixed $\varepsilon > 0$ there is a constant $C_0(\varepsilon) > 0$ depending only on ε, such that there are at most $C_0(\varepsilon)q^{2/3+\varepsilon}$ decimations of an ℓ-sequence* **a** *with connection number q that are cyclic permutations of* **a**.

Finally, we show that for certain q, Conjecture 1.2 holds.

THEOREM 2.4. *If $q = 2p+1 = 8r+3$ with q, p, and r prime, and if 2 is primitive mod q, then Conjecture 1.2 holds for q sufficiently large.*

3. Preliminary estimates. Throughout this paper we fix a primitive qth root of unity, say, $\xi = e^{2\pi i/q} \in \mathbf{C}$. Define

$$S_d(a,b) = \sum_{x=0}^{q-1} \xi^{ax^d+bx}.$$

Then $S_d(0,0) = q$, $S_d(a,0) = S_d(0,b) = 0$ if a and b are nonzero, and

$$S_d(1,b) = S_d(\lambda^d, \lambda b) \tag{3.1}$$

for any $\lambda \neq 0$ (and for any b).

We need the following bound on the fourth moment of the sums $S_d(a,b)$ averaged over b; see [9].

LEMMA 3.1. *If $a \neq 0$ and $d > 1$, then*

$$\sum_{b=0}^{q-1} |S_d(a,b)|^4 \leq (d-1)q^3.$$

Proof. The proof follows the method of Davenport and Heilbronn [6]. Let $R(w,t)$ denote the number of solutions to the system of congruences

$$x + y \equiv w \bmod q,$$
$$x^d + y^d \equiv t \bmod q.$$

By solving for y using the first equation, we can reduce this to a single equation of degree $d-1$. (Since $d > 1$ is odd, the terms involving x^d cancel out.) Such an equation has at most $d-1$ solutions unless $w = t = 0$, when it has q solutions. Also, $R(w,t) = 0$ if one but not both of w and t is zero. Thus we have

$$\sum_{w=1}^{q-1}\sum_{t=1}^{q-1} R(w,t) = \sum_{w=0}^{q-1}\sum_{t=0}^{q-1} R(w,t) - q = q^2 - q$$

and

$$\sum_{w=0}^{q-1}\sum_{t=0}^{q-1} R^2(w,t) \leq (d-1)\sum_{w=1}^{q-1}\sum_{t=1}^{q-1} R(w,t) + q^2 = dq^2 - (d-1)q.$$

Therefore the sum

$$T = \sum_{a=0}^{q-1}\sum_{b=0}^{q-1} |S_d(a,b)|^4$$

is given by

$$T = \sum_{a=0}^{q-1}\sum_{b=0}^{q-1}\sum_{x_1=0}^{p-1}\sum_{x_2=0}^{p-1}\sum_{x_3=0}^{p-1}\sum_{x_4=0}^{p-1} \xi^{a(x_1^d+x_2^d-x_3^d-x_4^d)+b(x_1+x_2-x_3-x_4)},$$

which is q^2 times the number of solutions (x_1, x_2, x_3, x_4) to the system

$$\begin{aligned} x_1 + x_2 &\equiv x_3 + x_4 \bmod q, \\ x_1^d + x_2^d &\equiv x_3^d + x_4^d \bmod q \end{aligned}$$

with $0 \le x_1, x_2, x_3, x_4 \le q - 1$. Counting the number of pairs (x_1, x_2) and (x_3, x_4) independently gives

$$\sum_{a=0}^{q-1} \sum_{b=0}^{q-1} |S_d(a,b)|^4 = T = q^2 \sum_{w=0}^{q-1} \sum_{t=0}^{q-1} R^2(w,t) \le dq^4 - (d-1)q^3. \tag{3.2}$$

The terms for which $a = 0$ contribute the quantity

$$\sum_{b=0}^{q-1} |S_d(0,b)|^4 = q^4.$$

Thus

$$\sum_{a=1}^{q-1} \sum_{b=0}^{q-1} |S_d(a,b)|^4 \le (d-1)(q^4 - q^3).$$

Since d is relatively prime to $q-1$, the mapping $x \mapsto x^d$ is a permutation; hence (3.1) gives

$$\begin{aligned} \sum_{b=0}^{q-1} |S_d(a,b)|^4 = \sum_{b=0}^{q-1} |S_d(1,b)|^4 &= \frac{1}{q-1} \sum_{\lambda=1}^{q-1} \sum_{b=0}^{q-1} |S_d(\lambda^d, \lambda b)|^4 \\ &\le \frac{1}{q-1} \sum_{u=0}^{q-1} \sum_{v=0}^{q-1} |S_d(u,v)|^4 \le (d-1)q^3. \end{aligned} \tag{3.3}$$

This completes the proof of Lemma 3.1. □

Let $E = \{0, 2, \ldots, q-1\} \subset \mathbf{Z}/(q)$ denote the set of "even" elements. For any $b \in \mathbf{Z}$ define

$$\sigma_d(b) = \sum_{x \in E} \xi^{bAx^d} = \sum_{x=0}^{(q-1)/2} \xi^{bA2^d x^d}.$$

Then $\sigma_d(0) = |E| = (q+1)/2$.

Lemma 3.2. *For any $b \ne 0$ we have*

$$|\sigma_d(b)| \le \frac{2^{14/4}}{\pi}(d-1)^{1/4} q^{3/4} + 4 \ln q + 4 < 2^3 (d-1)^{1/4} q^{3/4}.$$

Proof. Davenport and Heilbronn [6] gave estimates on certain exponential sums. If we let

$$F(n) = \sum_{x=0}^{q-1} \xi^{f(x)+nx},$$

where n is an integer, then their Lemma 4 says that for any m,

$$\sum_{x=0}^{m} \xi^{f(x)} = \frac{m}{q} F(0) + O\left(\sum_{n=1}^{q-1} \frac{1}{n} (|F(n)| + |F(-n)|) \right) + O(\ln q).$$

Let us take $f(x) = ax^d$ (where $a = bA2^d$) and $m = (q-1)/2$. Then $F(0) = 0$ and $F(n) = S_d(a, n)$. By carefully examining Davenport and Heilbronn's proof, one sees that the constant on the first big-O is $2/\pi$ and the second big-O can be replaced by $4 \ln q + 4$. In other words,

$$|\sigma_d(b)| \le \frac{2}{\pi} \left(\sum_{n=1}^{q-1} \frac{1}{n} (|S_d(a,n)| + |S_d(a,-n)|) \right) + 4 \ln q + 4. \tag{3.4}$$

Applying Hölder's inequality to Lemma 3.1 gives

$$\sum_{n=1}^{q-1} \frac{1}{n} |S_d(a,n)| \le 4^{3/4} (d-1)^{1/4} q^{3/4}.$$

The same bound applies to the sum using $S_d(a, -n)$ in place of $S_d(a, n)$. The lemma follows. □

4. Proof of Theorem 2.1 (iii). Although Theorem 2.2 gives a better estimate than Theorem 2.1 (iii), we briefly include our original proof of it because it illustrates a technique which may some day be refined so as to give an even better estimate. As in the previous sections we suppose that q is a prime number, that 2 is primitive modulo q, and that d is relatively prime to $q-1$. Again let $E = \{0, 2, \ldots, q-1\} \subset \mathbf{Z}/(q)$ be the set of even numbers. Define

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

Its Fourier transform is given by

$$\hat{f_E}(b) = \frac{1}{q} \sum_{c=0}^{q-1} f_E(c) \xi^{-bc}.$$

By the Fourier inversion formula we have

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

Now assume that the mapping $x \mapsto Ax^d$ preserves (but permutes the elements within) the set E. Then

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

The left-hand side equals $|E| = (q+1)/2$ because if $b = 0$, then $\hat{f_E}(b) = (q+1)/(2q)$ and $\sigma_d(b) = |E| = (q+1)/2$. Thus

$$\frac{q^2-1}{4q} = \left| \sum_{b=1}^{q-1} \hat{f_E}(b) \sigma_d(b) \right| \le \left(\sum_{b=1}^{q-1} |\hat{f_E}(b)| \right) \max_{b \ne 0} |\sigma_d(b)|.$$

We need the following lemma; see [9].

Lemma 4.1. *The following inequality holds:*

$$\sum_{b=1}^{q-1} |\hat{f_E}(b)| \le 1 + \frac{1}{2}\ln\left(\frac{q-3}{2}\right) < \frac{\ln q + 2}{2}.$$

Combining this estimate with Lemma 3.2 gives

$$d > \frac{(q^2-1)^4}{2^{16}q^7(\ln q + 2)^4},$$

which completes the proof of Theorem 2.1. □

5. Proof of Theorem 2.2. In this section we use the technique for obtaining bounds from exponential sums that has been used by several authors (for example, see [3]).

As in the preceding sections, let E be the set of even integers between 0 and $q-1$ and assume that the conclusion of Theorem 2.2 is false. In other words, assume that $Ax^d \in E$ for every $x \in E$. Let W denote the set of integers between 0 and $\lfloor (q-2)/4 \rfloor$ and let $s = 2\lfloor (q-1)/4 \rfloor + 1$. It follows that the congruence

$$Ax^d \equiv 2(u-v) + s \bmod q, \qquad x \in E,\ u, v \in W,$$

has no solutions. Therefore

$$\begin{aligned} 0 &= \frac{1}{q}\sum_{u,v\in W}\sum_{x\in E}\sum_{b=0}^{q-1} \xi^{b(Ax^d-2(u-v)-s)} \\ &= \frac{1}{q}\sum_{b=0}^{q-1}\xi^{-bs}\sigma_d(b)\sum_{u,v\in W}\xi^{2b(u-v)} = \frac{1}{q}\sum_{b=0}^{q-1}\xi^{-bs}\sigma_d(b)\left|\sum_{u\in W}\xi^{bu}\right|^2. \end{aligned}$$

The term corresponding to $b = 0$ equals $|W|^2|E|/q$. Therefore

$$\frac{|W|^2|E|}{q} = -\frac{1}{q}\sum_{b=1}^{q-1}\xi^{-bs}\sigma_d(b)\left|\sum_{u\in W}\xi^{2bu}\right|^2 \le \frac{1}{q}\sum_{b=1}^{q-1}|\sigma_d(b)|\left|\sum_{u\in W}\xi^{2bu}\right|^2. \tag{5.1}$$

Using Lemma 3.2, we derive

$$\begin{aligned} \frac{|W|^2|E|}{q} &\le 2^3(d-1)^{1/4}q^{-1/4}\sum_{b=1}^{q-1}\left|\sum_{u\in W}\xi^{bu}\right|^2 \\ &\le 2^3(d-1)^{1/4}q^{-1/4}\sum_{b=0}^{q-1}\left|\sum_{u\in W}\xi^{2bu}\right|^2 \\ &= 2^3(d-1)^{1/4}q^{-1/4}(q|W|) = 2^3(d-1)^{1/4}q^{3/4}|W|. \end{aligned} \tag{5.2}$$

Since $|W| \ge (q-1)/4$ we obtain

$$d - 1 \ge \frac{|W|^4|E|^4}{2^{12}q^7} \ge \frac{(q^2-1)^4}{2^{24}q^7}.$$

A similar argument can be made for negative d. Suppose $d = -e$ with $e > 0$. The system of congruences

$$\begin{aligned} x + y &\equiv w \bmod q, \\ x^d + y^d &\equiv t \bmod q \end{aligned}$$

is equivalent to the single congruence

$$(w - x)^e + x^e \equiv t(w - x)^e x^e,$$

which has at most $2e$ solutions. This fact can be used in the proof of Lemma 3.1, which now says, If $a \neq 0$ and if $d = -e < 0$, then

$$\sum_{b=0}^{q-1} |S_d(a, b)|^4 \leq 2eq^3.$$

Lemma 3.2 then reads as follows: for any $b \neq 0$,

$$|\sigma_d(b)| < 2^3(2e)^{1/4} q^{3/4}.$$

Now go back to the beginning of the proof of Theorem 2.2, using this estimate for $|\sigma_d(b)|$ in (5.1). The factors $(d - 1)$ become replaced by $2e$, which leads to the conclusion

$$2e > \frac{(q^2 - 1)^4}{2^{24} q^7}.$$

This completes the proof of Theorem 2.2. □

6. Proof of Theorem 2.3. It follows from the proof of Theorem 8 of Canetti et al. [2] that for any fixed $\varepsilon > 0$, the sum of the numbers of solutions to the systems of congruences

$$\begin{aligned} x_1 + x_2 &\equiv x_3 + x_4 \bmod q, \\ x_1^d + x_2^d &\equiv x_3^d + x_4^d \bmod q \end{aligned} \tag{6.1}$$

over all $d = 0, 1, \ldots, q - 2$ is bounded by a function in $O\left(q^{11/3+\varepsilon}\right)$. Let D be the set of d such that the system of congruences (6.1) has more than $q^{3-\varepsilon}$ solutions. Then the cardinality of D satisfies $|D| \in O(q^{2/3+\varepsilon})$.

We claim that if there exists $A \neq 0$ such that $x \mapsto Ax^d$ preserves the set E of even elements, then $d \in D$. Suppose the contrary: fix such an A and d, and suppose that $d \notin D$. Then the number of solutions to (6.1) is no more than $q^{3-\varepsilon}$. Thus by (3.2) we obtain the bound

$$\sum_{a=0}^{q-1} \sum_{b=0}^{q-1} |S_d(a, b)|^4 = T \in O(q^{5-\varepsilon}).$$

Hence, as in (3.3), we conclude that

$$\sum_{b=0}^{q-1} |S_d(a, b)|^4 \leq \frac{1}{q - 1} \sum_{a=0}^{q-1} \sum_{b=0}^{q-1} |S_d(a, b)|^4 \in O(q^{4-\varepsilon}),$$

and thus $|S_d(a,b)| \in O(q^{1-\varepsilon/4})$ for every $b = 0, \ldots, q-1$. Hence

$$\sum_{n=1}^{q-1} \frac{1}{n} |S_d(a,n)| \in O(q^{1-\varepsilon/4} \ln q)$$

and this estimate can be used in (3.4) to give

$$|\sigma_d(b)| \in O(q^{1-\varepsilon/4} \ln q).$$

Now return to the beginning of the proof of Theorem 2.2 and use this estimate in (5.1). Then (5.2) becomes

$$\frac{|W|^2|E|}{q} \in O(q^{1-\varepsilon/4}|W| \ln q),$$

which is impossible. □

7. Proof of Theorem 2.3 and other large sets of distinct decimations.

Let G denote the set of decimations of an ℓ-sequence $\mathbf{a}$ with connection integer q. The set G is a multiplicative group isomorphic to $(\mathbf{Z}/(\varphi(q)))^*$. Let H denote the set of decimations that are cyclic shifts of $\mathbf{a}$. Then H is a subgroup of G.

Let $\Delta \subseteq G$ be a set of representatives for G/H, with $1 \in \Delta$. That is, for each coset dH, there is exactly one element in $dH \cap \Delta$.

Lemma 7.1. *The set $D = \{\mathbf{a}^d : d \in \Delta\}$ is a set of $|\Delta|$ pairwise cyclically distinct decimations with ideal arithmetic correlations.*

Proof. Suppose that $\mathbf{a}^d$ is a cyclic permutation of $\mathbf{a}^e$, with $d, e \in \Delta$. Then $\mathbf{a}^{de^{-1}}$ is a cyclic permutation of $\mathbf{a}$. Thus $de^{-1} \in H$, and by the hypotheses on Δ, $de^{-1} = 1$. That is, $d = e$. □

Corollary 7.2. *Let $\mathbf{a}$ be an ℓ-sequence with connection integer q. For any fixed $\varepsilon > 0$ there are constants $C_1(\varepsilon), C_2(\varepsilon) > 0$ depending only on ε, such that the following statements hold:*

(i) *The set $\{\mathbf{a}^d : d \in \Delta\}$ is a set of at least*

$$\frac{|G|}{|H|} \geq C_1(\varepsilon) q^{1/3-\varepsilon}$$

cyclically distinct sequences with ideal arithmetic correlations.

(ii) *If $\varphi(\varphi(q))$ has a prime factor $r > C_2(\varepsilon)q^{2/3+\varepsilon}$, then $\{\mathbf{a}^d : d \in \Delta\}$ is a set of at least r cyclically distinct sequences with ideal arithmetic correlations.*

Proof. The first statement follows from Theorem 2.3 and the lower bound

$$\frac{q}{\varphi(\varphi(q))} \in O((\ln \ln q)^2);$$

see Theorem 328 in [10].

We know that $|H|$ and $|\Delta|$ divide $|G| = \varphi(\varphi(q))$. Take $C_2(\varepsilon) = C_1(\varepsilon)^{-1}$. If $\varphi(\varphi(q))$ has a prime factor $r > C_2(\varepsilon)q^{2/3+\varepsilon}$, then r cannot divide $|H|$, and so $\{\mathbf{a}^d : d \in \Delta\}$ is a set of at least $r > C_2(\varepsilon)q^{2/3+\varepsilon}$ cyclically distinct sequences. This proves the second statement. □

Now consider integers q with the special form $q = 2p + 1 = 2^k r + 3$ with p and r prime. In this case $\varphi(\varphi(q)) = \varphi(2p) = p - 1 = 2^{k-1}r$. If k is small enough (for example, $k = 3$ as in the formulation of Theorem 2.4) and q is large enough, then r does not divide $|H|$. This implies that $|H|$ is a power of 2. We also have $|G| = (\mathbf{Z}/(2p))^* = (\mathbf{Z}/(p))^*$, which is a cyclic group. Thus either $|H|$ is trivial or H contains -1. However, we have already shown in Theorem 2.1 that $-1 \notin H$. It follows that all decimations are cyclically distinct. This proves Theorem 2.4. $\square$

In fact, as we have just seen, in Theorem 2.4 one can consider more general families of primes.

There is a heuristic for the density of such primes q. Artin's conjecture, which is true if the extended Riemann hypothesis is true [12], implies that there are at least $AN/\ln N$ primes $q < N$ such that 2 is primitive modulo q. (The constant A is known as Artin's constant and is about .3739558.) Of these, we expect about $1/\ln N$ to satisfy $q = 2p + 1$ with p prime. If p is congruent to 3 modulo 4, then q is congruent to 7 modulo 8, which would imply that 2 is a quadratic residue, hence, not primitive. Thus it must be the case that p is congruent to 1 modulo 4, so $q = 8r + 3$ for some r. We expect r to be prime with probability about $1/\ln N$, so we expect more than $AN/(\ln N)^2$ primes less than N that satisfy all these requirements. Experimentation shows that this estimate is a bit conservative for $N < 1,000,000,000$.

8. Conclusions. We have significantly increased the set of decimations of an ℓ-sequence $\mathbf{a}$ that are known to be cyclically distinct from $\mathbf{a}$. For sufficiently long ℓ-sequences we have shown that there is a large family of cyclically distinct decimations. In some special cases we have in fact shown that all decimations are cyclically distinct.

REFERENCES

[1] L. Blum, M. Blum, and M. Shub, *A simple unpredictable pseudo-random number generator*, SIAM J. Comput., 15 (1986), pp. 364–383.

[2] R. Canetti, J. B. Friedlander, S. Konyagin, M. Larsen, D. Lieman, and I. E. Shparlinski, *On the statistical properties of Diffie–Hellman distributions*, Israel J. Math., 120 (2000), pp. 23–46.

[3] J. H. H. Chalk, *Polynomial congruences over incomplete residue systems modulo k*, Proc. Kon. Ned. Acad. Wetensch., A92 (1989), pp. 49–62.

[4] R. Couture and P. L'Ecuyer, *On the lattice structure of certain linear congruential sequences related to AWC/SWB generators*, Math. Comp., 62 (1994), pp. 799–808.

[5] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*, Elsevier, Amsterdam, 1998.

[6] H. Davenport and H. Heilbronn, *On an exponential sum*, Proc. London Math. Soc., 41 (1936), pp. 449–453.

[7] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801. Yale University Press, New Haven, CT, 1966 (in English).

[8] M. Goresky and A. Klapper, *Arithmetic cross-correlations of FCSR sequences*, IEEE Trans. Inform. Theory, 43 (1997), pp. 1342–1346.

[9] M. Goresky, A. Klapper, and R. Murty, *On the distinctness of decimations of ℓ-sequences*, in Sequences and Their Applications—SETA '01, T. Helleseth, P. V. Kumar, and K. Yang, eds., Discrete Math. Comput. Sci., Springer-Verlag, New York, 2002.

[10] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Univ. Press, Oxford, UK, 1979.

[11] T. Helleseth and V. Kumar, *Sequences with low correlation*, in Handbook of Coding Theory, V. Pless and W. Huffman, eds., North–Holland Elsevier, Amsterdam, 1998.

[12] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math., 225 (1967), pp. 209–220.

[13] A. Klapper and M. Goresky, *2-adic shift registers*, in Fast Software Encrypt., Cambridge Security Workshop, R. Anderson, ed., Lecture Notes in Comput. Sci. 809, Springer-Verlag, New York, 1994.

[14] A. Klapper and M. Goresky, *Feedback shift registers, combiners with memory, and 2-adic*

span, J. Cryptology, 10 (1997), pp. 111–147.

[15] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta Functions*, Grad. Texts in Math. 58, Springer-Verlag, New York, 1984.

[16] J. C. Lagarias, *Pseudorandom number generators in cryptography and number theory*, Proc. Sympos. Appl. Math., 42 (1990), pp. 115–143.

[17] G. Marsaglia and A. Zaman, *A new class of random number generators*, Ann. Appl. Probab., 1 (1991), pp. 462–480.

[18] P. Q. Nguyen and I. E. Shparlinski, *The insecurity of the Digital Signature Algorithm with partially known nonces*, J. Cryptology, 15 (2002), pp. 151–176.