S©MR

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ
Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru
ISSN 1813-3304

*Том 20, № 2, стр. 144–145 (2024)* УДК 519.7
https://doi.org/10.33048/semi.2023.20.??? MSC 11A07,
94A55, 11B50, 11L07

# ON DECIMATIONS OF HALF-$\ell$-SEQUENCES

**V. EDEMSKIY**

*Представлено* П.П. Петровым

**Abstract:** Half-$\ell$-sequences have several remarkable statistical properties. In particular, the arithmetic correlations between any two cyclically distinct decimations of them are equal to zero when prime connection number $p \equiv 1 \pmod 8$. In this paper we show that a $d$-fold decimation of a half-$\ell$-sequence with such prime connection number is cyclically distinct from the original half-$\ell$-sequence when $p$ is large and $d$ is small.

**Keywords:** half-$\ell$-sequence, decimation, arithmetic correlation.

## 1 Introduction

Goresky and Klapper propose an architecture of new shift registers to design sequences which they call the feedback with carry shift registers (FCSRs) and study the properties of series of the output sequences of FCSRs. We refer the reader to the monograph [6] for the theory on FCSRs. In particular, they show that every pair of cyclically distinct allowable decimations of $\ell$-sequences has ideal arithmetic correlations [8]. The $\ell$-sequence can be defined as the output sequence of maximal period FCSR with connection number $q$ such that 2 is a primitive root modulo $q$ (thus $q$ is a power of a prime) or as the 2-adic expansion of rational number $r/q$, where $\gcd(r, q) = 1$.

Edemskiy, V., On decimations of half-$\ell$-sequences.

This work was funded by the Russian Science Foundation under (grant 24-21-00442).
*Received 28 January, published .*

The arithmetic cross-correlation is the with-carry analogue of the cross-correlation of sequences. If $(s_i)$ and $(t_i)$ are two eventually periodic sequences with period $N$ and $\alpha$ and $\beta_\tau$ are the 2-adic numbers corresponding to sequences $(s_i)$ and shifting $(t_{i+\tau})$ by $\tau$ positions then the shifted arithmetic cross-correlation of $(s_i)$ and $(t_i)$ is the number of zeros minus the number of ones in a complete period of length $N$ of $\alpha - \beta_\tau$. When $(s_i) = (t_i)$, the arithmetic cross-correlation is called the arithmetic autocorrelation of $(s_i)$.

In conclusion of paper [8], authors made a conjecture that if $q > 13$ is a prime and $(s_i)$ is an $\ell$-sequence based on $q$, then every pair of decimations of $(s_i)$ is cyclically distinct. This conjecture was discussed in [1, 9, 7, 14] and was proved in [3] when $q$ is a prime and in [10] when $q$ is a power of a prime.

Output sequences generated by FCSRs with connection integer $q$ are called *half-$\ell$-sequences* when their period $T = \mathrm{ord}_q(2) = \varphi(q)/2$, where $q$ is an odd prime power, $\mathrm{ord}_q(2)$ is an order of 2 modulo $q$, and $\varphi(\cdot)$ is the Euler phi function [11]. Various properties of half-$\ell$-sequence have been considered in [11, 12, 13]. The arithmetic cross-correlation of half-$\ell$-sequences is studied in [2]. It was noted in [2] that any pair of allowable decimations of $(s_i)_{i\geq 0}$ has ideal arithmetic cross-correlation when $p \equiv 1 \pmod 8$ if they are cyclically distinct. Thus, it is interesting to study whether the decimations of half-$\ell$-sequences will be cyclically distinct as for $\ell$-sequences. In this work, we show that decimations are distinct in many cases when the connection number is a sufficiently large prime.

The paper is organized as follows. Our main result is in 2, the estimates of exponential sums is in Section 3, a proof of result is in Section 4, and the conclusions follow in Section 5.

## 2 Preliminaries and Main result

In this section, we recall some definitions and present our main result. Let $p$ be a prime such that an order of 2 modulo $p$ is equal to $(p-1)/2$. In this case, $p \equiv \pm 1 \pmod 8$ and 2 is a square residue modulo $p$. We consider a half-$\ell$-sequence $(s_n)$ with period $(p-1)/2$. According to [6] the sequence $(s_n)$ can be defined as follows:

$$s_i = (u2^{-i} \bmod p) \bmod 2, \tag{1}$$

for some $u$ with $\gcd(u, p) = 1$, $i = 0, 1, 2, \ldots$. In other words, this is a $(p-1)/2$-periodic binary sequence generated by FCSR with connection integer $p$.

Let $(c_i) = (s_{ic})_{i\geq 0}$ be the $c$-fold of $(s_i)$, where $c$ is integer. If $\gcd(c, (p-1)/2) = 1$ then this $c$-fold is an allowable decimation. Let $(s_{ic})_{i\geq 0}$ and $(s_{ie})_{i\geq 0}$ be decimations of $(s_i)$, where $\gcd(c, (p-1)/2) = \gcd(e, (p-1)/2) = 1$. It was noted in [2] that any pair of allowable decimations of $(s_i)_{i\geq 0}$ have ideal arithmetic cross-correlation for $p \equiv 1 \pmod 8$ when they are cyclically distinct. It is clear that $(s_{ic})_{i\geq 0}$ and $(s_{ie})_{i\geq 0}$ are cyclically distinct if and only if $(s_i)$ and $(s_{di})$ are cyclically distinct, where $d = c(e^{-1} \pmod{(p-1)/2})$.

In this paper we show that decimations of half-$\ell$-sequence are cyclically distinct when $p$ is large and $d$ is small. Our main contribution in this paper is the following statement.

**Theorem 1.** *Let $(s_i)$ be a half-$\ell$-sequence and $p \equiv 1 \pmod 8$. For $p$ sufficiently large, the decimation $(s_{di})$ is cyclically distinct from $(s_i)$ if*

$$1 < d < \frac{4p}{10^4 \ln^4 p}$$

*for $d > 0$ and*

$$1 <\mid d \mid< \frac{4p}{3 \cdot 10^4 \ln^4 p}$$

*for $d < 0$.*

In conclusion of this section we make a few remarks. Let $(s_i)$ and $(s_{di})$ be not cyclically distinct, i.e. there exists $k$ such that $s_i = s_{k+id}$ for all $i \geq 0$. Then

$$(u2^{-i} \bmod p) \bmod 2 = (u2^{-k-id} \bmod p) \bmod 2 \text{ for all } i \geq 0.$$

Denote by $Q$ and $NQ$ are sets of square residues and non-square residues modulo $p$ respectively. Since $2 \in Q$, it follows by (1) that a set $\{u2^{-i} \bmod p,\ i = 0, 1, 2, \ldots, (p-3)/2\}$ is equal to $Q$ if $u \in Q$, and equals $NQ$ if $u \in NQ$. Thus, the mapping $\varphi :\ x \to Ax^d \bmod p$ where $A = 2^{-k}u^{-d+1}$ preserves the parity of an integers from $Q$ or $NQ$. Hence, the conclusion about the cyclically distinct decimations is essentially equivalent to the statement that the mapping $Ax^d$, with $\gcd(d, (p-1)/2) = 1$ and $\gcd(p, A) = 1$, preserves the parity of integers from $Q$ or $NQ$ if and only if $d = 1$ and $A \equiv 1 \pmod p$. Further, we will study the properties of this map to use the estimates of exponential sums from [4]. Unlike [9], for the upper estimate of some exponential sum, we will use the result of Vinogradov, not Davenport and Heilbronn, and we will get the lower estimate in a simple way. In this case, we need to use the map $Ax^{2d}$, which is not a permutation of $\mathbb{Z}_p$ unlike $Ax^d$. Here and further, we denote by $\mathbb{Z}_p = \{0, 1, \ldots, q-1\}$ the residue class ring modulo $p$ and by $\mathbb{Z}_p^*$ the unit group of $\mathbb{Z}_p$.

## 3 Exponential sums for $p \equiv 1 \pmod 8$

In this section, we suppose that $p \equiv 1 \pmod 8$. Then $d$ is odd, since $\gcd(d, (p-1)/2) = 1$. Let $Q_0$ and $NQ_0$ be sets of even square residues and even non-square residues modulo $p$, respectively. Denote by $g$ a primitive root modulo $p$. Since $-1 \equiv g^{(p-1)/2} \pmod p$, it follows that $-1 \in Q$, and we see that $\mid Q_0 \mid = \mid NQ_0 \mid = (p-1)/4$.

Let $\left(\frac{x}{p}\right)$ be the Legendre symbol, i.e.,

$$\left(\frac{x}{p}\right) = \begin{cases} 1, & \text{if } x \in Q, \\ 0, & \text{if } x = 0, \\ -1, & \text{if } x \in NQ. \end{cases}$$

**Lemma 1.** *Let $\xi$ be a primitive complex $p$th root of 1 and $c$ be an integer. Then*

$$\sum_{y\in Q_0\ (y\in NQ_0)} \xi^{cAy^d} = \frac{1}{2}\sum_{x=1}^{(p-1)/2}\left(1\pm\left(\frac{x}{p}\right)\right)\xi^{cA2^dx^d}.$$

*Here a sign + if $y\in Q_0$ and - when $y\in NQ_0$.*

*Доказательство.* Define two sets $I = Q\cap\{1,2,\dots,(p-1)/2\}$ and $J = NQ\cap\{1,2,\dots,(p-1)/2\}$. It is clear that

$$\frac{1}{2}\sum_{x=1}^{(p-1)/2}\left(1\pm\left(\frac{x}{p}\right)\right)\xi^{cA2^dx^d} = \sum_{x\in I\ (x\in J)}\xi^{cA2^dx^d}.$$

Let $y = 2x$. Since $2\in Q$, we observe that $y\in Q_0$ when $x\in I$ and $Q_0 = 2I$ and $y\in NQ_0$ if $x\in J$ and $NQ_0 = 2J$. This completes the proof of this statement. □

According to [15]( Ex. 12, Chap. 5), if for an integer $m>1$ and a function $\Phi(x)$ exists $\Delta$ such that

$$|\sum_{x=1}^{m-1}\Phi(x)\xi^{bx}|\le\Delta\ \text{ for } b=1,2,\dots,m-1$$

then

$$\sum_{x=M}^{M+N}\Phi(x) = \frac{N}{m}\sum_{x=1}^{m-1}\Phi(x)+\theta\Delta(\ln m-1)$$

for $m>60$. Here $|\theta|<1$ and $0<M<M+N<m$.

Let $\Phi(x) = \left(1\pm\left(\frac{x}{p}\right)\right)\xi^{ax^d}$ where $a$ is an integer. Then for $p>60$ we get

$$|\sum_{x=1}^{(p-1)/2}\Phi(x)|\le\frac{p-1}{2p}|\sum_{x=1}^{p-1}\Phi(x)|+\Delta(\ln p-1). \tag{2}$$

Further, we will estimate the sums in this inequality.

**Lemma 2.** *Let notation be as before and* $\gcd(a,p)=1$. *Then*

$$|\sum_{x=1}^{p-1}\Phi(x)|\le\sqrt{p}+1.$$

*Доказательство.* By definition

$$\sum_{x=1}^{p-1}\Phi(x) = \sum_{x=1}^{p-1}\xi^{ax^d}\pm\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\xi^{ax^d}.$$

Since $\gcd(d,p-1)=1$, we have a map $x^d$ which is a permutation of $\mathbb{Z}_p^*$ and

$$\sum_{x=1}^{p-1}\xi^{ax^d} = \sum_{z=1}^{p-1}\xi^{az} = -1.$$

Further, we see that $\left(\frac{ax^d}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{x}{p}\right)$. Hence

$$\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\xi^{ax^d} = \pm\sum_{z=1}^{p-1}\left(\frac{z}{p}\right)\xi^{z}.$$

The last sum is called Gauss sum. It is well known that $|\sum_{z=1}^{p-1}\left(\frac{z}{p}\right)\xi^z| = \sqrt{p}$. The statement of this lemma follows from the last remark. □

**Lemma 3.** *Let notation be as before. Then*

*(i)* $\sum_{x=0}^{p-1}\left(1+\left(\frac{x}{p}\right)\right)\xi^{ax^d+bx} = \sum_{z=0}^{p-1}\xi^{az^{2d}+bz^2}$;

*(ii)* $\sum_{x=0}^{p-1}\left(1-\left(\frac{x}{p}\right)\right)\xi^{ax^d+bx} = \sum_{z=0}^{p-1}\xi^{ag^dz^{2d}+bgz^2}$ *where* $g$ *is a primitive root modulo* $p$.

*Доказательство.* We will prove the second statement. Since the first equality can be proved by the same method as the second one, its proof is omitted here.

It is obvious that

$$\sum_{x=0}^{p-1}\left(1-\left(\frac{x}{p}\right)\right)\xi^{ax^d+bx} = 1+2\sum_{x\in NQ}\xi^{ax^d+bx}.$$

Since $g$ is a primitive root modulo $p$, we see that $NQ = \{gz^2 \mid z = 1,2,,\ldots,(p-1)/2\}$. Hence

$$\sum_{x=0}^{p-1}\left(1-\left(\frac{x}{p}\right)\right)\xi^{ax^d+bx} = 1+2\sum_{z=1}^{(p-1)/2}\xi^{ag^dz^{2d}+bgz^2}.$$

We finish the proof. □

According to [4] the following statement holds.

**Lemma 4** ([4])**.** *Let* $a,b = 1,2,\ldots,p-1$. *Then*

(1) $|\sum_{z=1}^{p-1}\xi^{az^{2d}+bz^2}| \le \sqrt{2}d^{1/4}p^{3/4}$ *when* $d>0$;

(2) $|\sum_{z=1}^{p-1}\xi^{az^{2d}+bz^2}| \le (12\mid d\mid)^{1/4}p^{3/4}$ *when* $d<0$;

Using Lemmas 2-4 and (2) we obtain

$$|\sum_{x=1}^{(p-1)/2}\Phi(x)| \le \frac{p-1}{2p}(\sqrt{p}+1) + (1+\sqrt{2}d^{1/4}p^{3/4})(\ln p - 1)$$

or

$$|\sum_{x=1}^{(p-1)/2}\Phi(x)| < \sqrt{2}d^{1/4}p^{1/4}\ln p \tag{3}$$

for $p>60$, $d>0$. Similarly,

$$|\sum_{x=1}^{(p-1)/2}\Phi(x)| < (12\mid d\mid)^{1/4}p^{1/4}\ln p \tag{4}$$

for $p > 60$, $d < 0$.

## 4 Proof of Theorem 1

In this section we finish the proof of Theorem 1. Suppose to the contrary that the map $\varphi : \ x \to Ax^d \bmod \ p$ preserves the parity of integers from $Q$ or $NQ$ when $p > 60$.

It is clear that

$$| \sum_{y \in Q_0 \ (y \in NQ_0)} \xi^{cAy^d} | \geq | \operatorname{Im} \sum_{y \in Q_0 \ (y \in NQ_0)} \xi^{cAy^d} |$$

where $\operatorname{Im} w$ is an imaginary part of a complex number $w$.

Let $c = (p-1)/2$. Since the map $Ax^d$ preserves the parity of integers from $Q$ or $NQ$, it follows that

$$| \operatorname{Im} \sum_{y \in Q_0 (y \in NQ_0)} \xi^{cAy^d} | = | \sum_{y \in Q_0 (y \in NQ_0)} \sin(\pi(p-1)y/p) |$$

and

$$| \operatorname{Im} \sum_{y \in Q_0 \ (y \in NQ_0)} \xi^{cAy^d} | \geq 2 \sum_{j=1}^{(p-1)/8} \sin 2\pi j/p = 2 \frac{\sin \frac{(p+7)\pi}{8p} \cdot \sin \frac{(p-1)\pi}{8p}}{\sin \frac{\pi}{p}}.$$

Since $\sin \pi/p < \pi/p$ and $p > 88$, we see that $| \operatorname{Im} \sum_{y \in Q_0 \ (y \in NQ_0)} \xi^{cAy^d} | > 0,32p/\pi > p/10$ for $c = (p-1)/2$. Hence by Lemma 1 and (3) for $d > 0$ we get

$$p/10 < \sqrt{2} d^{1/4} p^{3/4} \ln p/2 \text{ or } d > \frac{4p}{10^4 \ln^4 p}.$$

Let $d < 0$. Then by Lemma 1 and (4) we have

$$p/10 < (12 \mid d \mid)^{1/4} p^{3/4} \ln p/2 \text{ or } \mid d \mid > \frac{4p}{3 \cdot 10^4 \ln^4 p}.$$

This completes the proof of Theorem 1.

**Remark 1.** *Since* $| \sum_{z=0}^{p-1} \xi^{az^2} | = \sqrt{p}$ *when* $\gcd(a, p) = 1$, *it follows that*

$$| 1 + 2 \sum_{y \in Q_0 \ (y \in NQ_0)} \cos(2\pi y/p) | = \sqrt{p}.$$

*Hence, we have*

$$| \sum_{y \in Q_0 \ (y \in NQ_0)} \xi^{cAy^d} |^2 > (\sqrt{p}/2 - 1)^2 + p^2/100$$

*and*

$$(\sqrt{p}/2 - 1)^2 + p^2/100 < d^{1/2} p^{1/2} \ln^2 p/2.$$

*However, this does not significantly improve the estimate of* $d$.

## 5 Final remark and Conclusions

(i) Using the results from [5], we can obtain additional restrictions for $d$. According to [5] we know that

$$|\sum_{z=1}^{p-1} \xi^{az^k+bz^l}| < \gcd(k-l, p-1) + 2.292 D^{13/46} p^{89/92}$$

where $D = \gcd(k, l, p-1)$. In our case, $k = 2d, l = 2$, thus we get

$$|\sum_{z=1}^{p-1} \xi^{az^{2d}+bz^2}| < 2 + 2.292 \cdot 2^{13/46} p^{89/92}$$

when $\gcd(2d-2, p-1) = 2$. Hence, if the map $\varphi: \ x \to Ax^d \mod p$ preserves the parity of integers from $Q$ or $NQ$ then

$$0,32p/\pi < \left(2 + 2.292 \cdot 2^{13/46} p^{89/92}\right) \ln p.$$

This is impossible when $p > 10^{119}$. Thus, the decimation $(s_{di})$ is cyclically distinct from $(s_i)$ for $p > 10^{119}$ when $(s_i)$ is a half-$\ell$-sequence, $p \equiv 1 \pmod 8$ and $\gcd(2d-2, p-1) = 2$. It is clear that if $\gcd(2d-2, p-1) < Cp^r$, where $C$ is a positive integer and $0 < r < 1$ then we can always find $p_0$ such that $(s_i)$ and $(s_{di})$ are cyclically distinct for $p > p_0$. For example, if $\gcd(2d-2, p-1) < p^{89/92}$ then $p_0 > 10^{124}$. This approach does not work when $\gcd(2d-2, p-1) = \alpha p$ where $\alpha$ is a real number.

(ii) We have shown that many decimations of a half-$\ell$-sequence are cyclically distinct when $p$ is a sufficiently large prime. There is experimental data confirming that all such decimations are cyclically distinct in a lot of cases. So, the following conjecture can be posed.

**Conjecture 1.** *If $p > 17$ is a prime and $(s_n)$ is a half-$\ell$-sequence based on $p \equiv 1 \pmod 8$, then each pair of decimations of $(s_n)$ is cyclically distinct.*

For $p = 17$, we have $(s_{-i})$ $(d = -1)$ is a cyclic shift of half-$\ell$-sequence $(s_i)$. The map $15x^7$ preserves the parity of $Q$, and the map $4x^7$ of $NQ$ when $p = 17$.

Proving this Conjecture using the method from [3] seems very difficult. If this Conjecture will be true then we will have large families of cyclically distinct sequences with ideal arithmetic correlations distinct from families based on $\ell$-sequences.

(iii) The half-$l$-sequences have no ideal arithmetic cross-correlation when $p \equiv 7 \pmod 8$. But we can also consider decimations of these sequences in this case. If $p \equiv 7 \pmod 8$ then $-1 \in NQ$ and $Q = -NQ$. Hence, if $d$ is odd and mapping $\varphi: \ x \to Ax^d \mod p$ preserves the parity of integers from $Q$ then it also preserves the parity of integers from $NQ$ and vice versa. So, this map preserves (but permutes the elements within) the set of even residues modulo $p$. According to Theorem 1.1 from [3] it is impossible.

For even $d$, it is sufficient to estimate a sum $\sum_{z=0}^{p-1} \xi^{az^{2d}+bz}$. This can be done in the same way as in Lemma 4.

Moreover, using the autocorrelation properties of the half-$l$-sequences obtained in Theorem 3 [12] when $p \equiv 7 \pmod 8$ we can claim that Theorem 17 from [10] is valid in this case as well. More precisely, if $p \equiv 7 \pmod 8$ and $d$ satisfies that $d+1$ and $d-1$ are not divisible by order of 3 modulo $p$, then the decimation $(s_{di})$ is cyclically distinct from $(s_i)$.

## References


[1] J. Bourgain, T. Cochrane, J. Paulhus, C. Pinner, *Decimations of $\ell$-sequences and permutations of even residues mod $p$*, SIAM J. Discrete Math., **23** (2009), 842–857.

[2] Z. Chen, V. Edemskiy, Z. Niu, Y. Sang, *Arithmetic correlation of binary half-$\ell$-sequences*, IET Inf. Secur., **17(2)** (2023), 289–293.

[3] T. Cochrane, S. Konyagin, *Proof of the Goresky -Klapper Conjecture on Decimations of $\ell$-sequences*, SIAM Journal on Discrete Math., **25(4)**(2011), 1812-1831.

[4] T. Cochrane, C. Pinner, *An improved Mordell type bound for exponential sums*, Proc. Amer. Math. Soc., **133** (2005), 313–320.

[5] T. Cochrane, C. Pinner, *Explicit bounds on monomial and binomial exponential sums*, Quart. J. Math., **62** (2011), 323–349

[6] M. Goresky, A. Klapper, *Algebraic Shift Register Sequences*, Cambridge University Press, Cambridge (2012)

[7] M. Goresky, A. Klapper, R.Murty, I. Shparlinski, *On decimations of $\ell$-sequences*, SIAM J. Discrete Math., **18** (2–4), 130-140.

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

[9] M. Goresky, A. Klapper, R. Murty, *On the distinctness of decimations of $\ell$-sequences*, in Proceedings of SETA'01, T. Helleseth, ed., Discrete Math. Comput. Sci., Springer Verlag, New York, 2002.

[10] W.F. Qi, H. Xu, *Further results on the distinctness of decimations of $\ell$-sequences*, IEEE Trans. Inform. Theory, **52** (2006), pp. 3831–3836.

[11] T. Gu, A. Klapper, *Distribution properties of half-$\ell$-sequence*, SETA 2014, LNCS **8865** (2014), 234-245.

[12] T. Gu, A. Klapper, *Statistical properties of half-$\ell$-sequences*, Cryptogr. Commun., **8(3)** (2016), 383-400.

[13] Z. Niu, Y. Sang, *On the linear complexity of binary half-$\ell$-sequences*, Int. J. Netw. Secur., **24 (3)** (2022), 444-449.

[14] T. Tian, W.-F. Qi, *Autocorrelation and Distinctness of Decimations of $\ell$-Sequences*, SIAM Journal on Discrete Math., **23 (2)**( 2009), 805-821.

[15] I. M. Vinogradov, *Elements of Number Theory*, Moscow, 1965.



Vladimir Edemskiy
Yaroslav-the-Wise Novgorod State University,
str. B. St. Petersburgskaya, 41,
173003, Veliky Novgorod, Russia
*Email address*: vladimir.edemsky@novsu.ru