THE VIRTUAL PERIODS OF LINEAR RECURRENCE SEQUENCES IN CYCLOTOMIC FIELDS

SHENXING ZHANG

Abstract. A linear recurrence sequence in a cyclotomic field produces a sequence of the generating fields of each term. We show that the later sequence is periodic after removing the first finite terms, and give a bound of its period. This can be applied to exponential sums.

Contents

1. The virtual periods of linear recurrence sequences 1
2. The virtual periods of exponential sums 3
References 5

1. The virtual periods of linear recurrence sequences

A *linear recurrence sequence* with dimension n is a sequence $\{a_k\}_{k\geq 0}$ such that for all $k \geq n$,

$$a_k = \sum_{i=1}^{n} c_i a_{k-i}$$

for some constant $c_1, \dots, c_n$ where $c_n \neq 0$.

Definition 1.1. We say a sequence $\{a_k\}_{k\geq 0}$ is *virtually periodic* if there exists integers $N, r \geq 1$ such that $a_n = a_{n+r}$ for any $n \geq N$. The minimal r is called the *virtual period* and the minimal N is called the *pre-period length*.

One can easily obtain the following result from [WY20, Theorem 3].

Theorem 1.2. *Let K be a field of characteristic 0 and L a finite extension of K. Let $\{a_k\}_{k\geq 0}$ be a linear recurrence sequence in L. Then the sequence $\{K(a_k)\}_{k\geq 0}$ of fields is virtually periodic.*

For $L = \mathbb{Q}(\mu_m)$ a cyclotomic field, we will reprove the Skolem-Mahler-Lech Theorem and the theorem above to estimate the virtual period, see [Han85], [Lec53, §2].

Date: October 4, 2021.
2020 *Mathematics Subject Classification.* 11B99, 11L07, 11T23.
Key words and phrases. linear recurrence sequence; periodic sequence; exponential sums.

Certainly, we may assume that $2 \mid m$. For $n > 1$, denote by

$$e_p = \begin{cases} 0, & p \nmid m, p > n+1; \\ 1 + \left[\log_p \frac{n}{p-1}\right], & p \nmid m, 2 < p \leq n+1; \\ 2 + [\log_2 n], & p = 2, \mathrm{ord}_2(m) = 1; \\ \mathrm{ord}_p(m) + \left[\log_p n\right], & 2p \mid m \end{cases} \tag{1.1}$$

for each prime p, where $[x]$ denote the greatest integer less than or equal x. Denote by

$$R_{m,n} = \prod_p p^{e_p} \tag{1.2}$$

and $R_{m,1} = m$. For odd m, we denote $R_{m,n} = R_{2m,n}$.

Theorem 1.3. *Let $\{a_k\}_{k\geq 0}$ be a linear recurrence sequence in $\mathbb{Q}(\mu_m)$ with dimension n.*

(1) There exists a positive integer $s \mid R_{m,n}$ such that the set $\{k : a_k = 0\}$ is a union of some $i + s\mathbb{N}$ and a finite set.

(2) The sequence $\{\mathbb{Q}(a_k)\}_{k\geq 0}$ is virtually periodic of virtual period $r \mid R_{m,n}$. Moreover, $\mathbb{Q}(a_k) \subseteq \mathbb{Q}(a_{k'})$ if $k \equiv k' \bmod r$ and $k' \geq N$ for pre-period length N.

Proof. (1) Let λ be a positive integer which is a common multiplier of the denominators of $a_0, \ldots, a_{n-1}, c_1, \ldots, c_n$. Then $a'_k := a_k \lambda^{k+1}$ satisfies

$$a'_k = \sum_{i=1}^{n} c_i \lambda^i a'_{k-i}$$

and $a'_0, \ldots, a'_{n-1}, c_1\lambda, \ldots, c_n\lambda^n \in \mathbb{Z}[\mu_m]$. Thus we may assume that $c_1, \ldots, c_n$ and all a_k lie in $\mathbb{Z}[\mu_m]$.

Let M be the $n \times n$ matrix with $M_{i,1} = c_i, M_{i,i+1} = 1$ for all i, and other entries are all zero. Denote

$$\mathbf{u} = (a_{n-1}, a_{n-2}, \ldots, a_0), \quad \mathbf{v} = (1, 0, \ldots, 0)^T.$$

Then $a_k = \mathbf{u}M^{k+1-n}\mathbf{v}$.

Let $\ell > 2$ be a prime splits completely in $K = \mathbb{Q}(\mu_m)$, such that $\ell \nmid c_n = (-1)^{n-1} \det M$. Let $\mathfrak{l}$ be a prime of K above ℓ and denote by $\mathcal{O}_\mathfrak{l}$ the completion of $\mathbb{Z}[\mu_m]$ at $\mathfrak{l}$. Then ℓ is a uniformizer of $\mathcal{O}_\mathfrak{l}$ and the residue field is $\kappa_\mathfrak{l} \cong \mathbb{F}_\ell$. Denote by $s(\ell)$ the order of the image of M under $\mathcal{O}_\mathfrak{l} \twoheadrightarrow \kappa_\mathfrak{l}$. Then $M^{s(\ell)} = I + \ell M'$ for some matrix M' over $\mathcal{O}_\mathfrak{l}$. For $i \geq n-1$, the function

$$a_{i+s(\ell)x} := \mathbf{u}M^{i+1-n}(I + \ell M')^x \mathbf{v} = \sum_{k\geq 0} \binom{x}{k} \mathbf{u}M^{i+1-n}M'^k\mathbf{v} \cdot \ell^k$$

on $x \in \mathcal{O}_\mathfrak{l}$ converges since $\mathrm{ord}_\ell\big(\ell^k/k!\big) > k\frac{\ell-2}{\ell-1}$ tends to infinity. If there are infinitely many integers x such that $a_{i+s(\ell)x} = 0$, then the set of these indices has an accumulation point in $\mathcal{O}_\mathfrak{l}$ in ℓ-adic topology. Hence the function a_{i+sx} must be zero identically by Weierstrass preparation theorem. From this we know that the set $\{k : a_k = 0\}$ has the predicated form.

If s is a positive integer such that $\{k : a_k = 0\}$ is a union of some $i + s\mathbb{N}$ and a finite set, then so is its multipliers. We take the minimal s. Then $s \mid s(\ell)$ is the order of an element in $\mathrm{GL}_n(\kappa_\mathfrak{l}) = \mathrm{GL}_n(\mathbb{F}_\ell)$. We will use the following proposition to estimate s.

Proposition 1.4 ([Dar05, §1, Corollary 1]). *Each maximal order of elements in* $\mathrm{GL}_n(\mathbb{F}_\ell)$ *has form*

$$\ell^t \times \mathrm{lcm}(\ell^{d_1}-1,\dots,\ell^{d_s}-1),$$

where $\sum_{i=1}^s k_i d_i = n$ *has integer solutions and* t *is the smallest non-negative integer such that* $\ell^t \geq \max\{k_1,\dots,k_s\}$*. In particular, the* p*-order of each maximal order is at most* $\max_{d\leq n}\mathrm{ord}_p(\ell^d-1)$.

We may assume that $n \geq 2$. For any rational prime $p \nmid m$, there exists a prime $\ell \nmid c_n$ which splits completely in K and ℓ is a primitive root modulo p^2. Thus

$$\mathrm{ord}_p(s) \leq \max_{d\leq n}\mathrm{ord}_p(\ell^d-1) = \begin{cases} 0, & p > n+1; \\ 1+\left[\log_p \frac{n}{p-1}\right], & 2 < p \leq n+1. \end{cases}$$

There exists a prime $\ell \nmid c_n$ which splits completely in K and $\ell \not\equiv 1 \bmod pm$ for any $p \mid m$. Then for each $p \mid m$, we have

$$\mathrm{ord}_p(s) \leq \max_{d\leq n}\mathrm{ord}_p(\ell^d-1) = \begin{cases} 2+[\log_2 n], & p=2, \mathrm{ord}_2(m)=1; \\ \mathrm{ord}_p(m)+\left[\log_p n\right], & \text{otherwise.} \end{cases}$$

(2) For $\sigma \in \mathrm{Gal}\big(\mathbb{Q}(\mu_m)/\mathbb{Q}\big)$, $\{\sigma(a_k)-a_k\}$ is a linear recurrence sequence satisfying

$$\sigma(a_k)-a_k = (\sigma\mathbf{u},\mathbf{u})\begin{pmatrix} \sigma M & \\ & M \end{pmatrix}^{k+1-n}\begin{pmatrix} \mathbf{v} \\ -\mathbf{v} \end{pmatrix}.$$

Similar to (1), let $\ell > 2$ be a prime splits completely in K such that $\ell \nmid c_n c_n^\sigma$. Then

$$M^{s(\ell)} \equiv (M^\sigma)^{s'(\ell)} \equiv I \bmod \mathfrak{l},$$

where $s(\ell), s'(\ell)$ are orders of two elements in $\mathrm{GL}_n(\mathbb{F}_\ell)$. Thus the set $\{k : \sigma(a_k)=a_k\}$ is a union of a finite set and some $i+r_\sigma\mathbb{N}$, where $r_\sigma \mid \mathrm{lcm}\big(s(\ell),s'(\ell)\big)$. By Proposition 1.4 and the estimation in (1), we have $\mathrm{ord}_p(r_\sigma) \leq e_p$ for each prime p.

Denote by r the least common multiplier of these r_σ. Then there exists N such that $\sigma(a_k)=a_k$ if and only if $\sigma(a_{k+r})=a_{k+r}$ for any $k \geq N$. Denote by H_k the set of $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ fixing a_k. As shown in [WY20, Theorem 3], $H_k = H_{k+r}$ for any $k > N$. Hence $\mathbb{Q}(a_k)=\mathbb{Q}(a_{k+r})$. Certainly, $r \mid R_{m,n}$.

For any integer $k \geq 0$, denote by k' the minimal one such that $k_0 \equiv k \bmod r$ and $k' \geq N$. Then $\sigma \in H_{k'}$ fixes $a_{k'+ir}$ for any $i \geq 0$ and the sequence $\{\sigma(a_{k'+ir})-a_{k'+ir}\}_{i\geq 0}$ is identically zero. This implies that $\{\sigma(a_{k+ir})-a_{k+ir}\}_{i\geq 0}$ is identically zero since it is a linear recurrence sequence. Hence a_k is fixed by $H_{k'}$ and $a_k \in \mathbb{Q}(a_{k'})$. □

2. The virtual periods of exponential sums

Let $f \in \mathbb{F}_q[x_1^{\pm 1},\dots,x_m^{\pm 1}]$ be a Laurent polynomial and $\chi : (\mathbb{F}_q^\times)^m \to \mathbb{C}^\times$ a character of order c. Define the *(toric) exponential sums*

$$S_k(f,\chi) = \sum_{x\in(\mathbb{F}_{q^k}^\times)^m} \psi\Big(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_p}\big(f(x)\big)\Big)\chi\big(\mathbf{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(x)\big) \in \mathbb{Z}[\mu_{pc}].$$

Then the L-function

$$L(T,f,\chi) = \exp\left(\sum_{k=1}^\infty \frac{T^k}{k} S_k(f,\chi)\right)$$

is a rational function over $\mathbb{Q}(\zeta_{pc})$ by the Dwork-Bombieri-Grothendick rationality theorem ([Bom66]). Write

$$L(T,f,\chi)=\frac{\prod_j(1-\beta_jT)}{\prod_i(1-\alpha_iT)}.$$

Then

$$S_k(f,\chi)=\sum_i\alpha_i^k-\sum_j\beta_j^k$$

and $\{S_k(f,\chi)\}_{k\geq 1}$ is a linear recurrence sequence in $\mathbb{Q}(\mu_{pc})$. Hence we have:

Theorem 2.1. *The sequence $\{\mathbb{Q}(S_k(f,\chi))\}_{k\geq 1}$ is virtually periodic with the period dividing $R_{pc,n}$, where n is the number of zeroes and poles of the L-function $L(T,f,\chi)$ and c is the order of χ. In particular, every prime factors of the virtual period are less than $n+1$ or divides pc.*

We will omit χ if it's trivial.

Example 2.2. Assume that d is a divisor of $q-1$. Let $f(x)=x^d+a\in\mathbb{F}_q[x]$ be a polynomial and χ the trivial character. Then by the Hasse-Davenport relation, we have

$$S_k(f)=-\sum_{i=1}^{d-1}\beta_i^k,\quad L(T,f)=\prod_{i=1}^{d-1}(1-\beta_iT),$$

where

$$\beta_i=-\psi\big(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)\big)\tau(\omega^{\frac{(q-1)i}{d}})\in\mathbb{Q}(\mu_{pd}),\quad \tau(\eta)=\sum_{x\in\mathbb{F}_q^\times}\eta(x)\psi\big(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)\big).$$

Then

$$a_k=\mathbf{u}M^k\mathbf{v},\quad \mathbf{u}=-\mathbf{v}^T=(1,\dots,1),\ M=\mathrm{diag}\left\{\beta_1,\dots,\beta_{d-1}\right\}.$$

Similarly to the proof of Theorem 1.3, we take a prime $\ell>2$ which splits completely in $\mathbb{Q}(\mu_{pd})$ and $\ell\nmid\det M$. Then $M^{\ell-1}\equiv I \bmod \ell$. Hence the virtual period of $\{\mathbb{Q}(S_k(f))\}_k$ divides $R_{pd,1}=pd$ or $2pd$.

If $d|(p-1)$ or $d\mid\frac{q-1}{p-1}$, we have $\deg S_k(x^d)=\frac{p-1}{\left(p-1,(q^k-1)/d\right)}$ by [Wan21, Theorem 4.8] and the degree sequence $\{\mathbb{Q}(S_k(f))\}_k$ is periodic with the period

$$\begin{cases} d, & \text{if } d\mid(p-1),\ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)=0;\\ pd, & \text{if } d\mid(p-1),\ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)\neq 0;\\ 1, & \text{if } d\mid\frac{q-1}{p-1},\ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)=0;\\ p, & \text{if } d\mid\frac{q-1}{p-1},\ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)\neq 0.\end{cases}$$

Example 2.3. The exponential sums $S_k(f)$ of $f=x_1+\cdots+x_{n-1}+\frac{a}{x_1\cdots x_{n-1}}$ are called *Kloosterman sums*. The sequence $\{\mathbb{Q}(S_k(f))\}_k$ is virtually periodic with the period dividing $R_{p,n}$, since $L(T,f)^{(-1)^n}$ is a polynomial of degree n by Deligne in [Del77].

It's known that if p is large with respect to $\log_p q, n$ and c, then the generating fields of twisted Kloosterman sums are known. See [Fis92] and [Zha21].

Example 2.4. It's easy to see that $R_{m,n} \mid R_{m,n+1}$. Bombieri in [Bom78, Theorem 1] showed that the number of zeroes and poles of $S_k(f)$ is at most $4d+5$, where d is the degree of f (be careful the different definitions of exponential sums). Hence the virtual period of $\{\mathbb{Q}(S_k(f))\}_{k\geq 1}$ divides $R_{p,4d+5}$.

Example 2.5. If f is so-called *non-degenerate*, then $L(T,f,\chi)^{(-1)^{n-1}}$ is a polynomial of degree $n!\mathrm{Vol}(\Delta)$, where Δ is the convex polyhedron in $\mathbb{R}^n$ associated to f. Hence the virtual period of $\{\mathbb{Q}(S_k(f,\chi))\}_{k\geq 1}$ divides $R_{p,n!\mathrm{Vol}(\Delta)}$. See [AS93, Corollary 2.12], [LW07, Theorem 1.3] and [Liu07, Theorem 1].

In particular, if f is a polynomial in one variable with $p \nmid d = \deg f$, then the virtual period of $\{\mathbb{Q}(S_k(f,\chi))\}_{k\geq 1}$ divides $R_{p,d}$.

Acknowledgments. The author would like to thank Daqin Wan and Yi Ouyang for many helpful suggestions. This work is partially supported by NSFC (Grant No. 12001510), the Fundamental Research Funds for the Central Universities (No. WK0010000061) and Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200).

References

[AS93] Alan Adolphson and Steven Sperber. Twisted exponential sums and Newton polyhedra. *J. Reine Angew. Math.*, 443:151–177, 1993.

[Bom66] Enrico Bombieri. On exponential sums in finite fields. pages 37–41, 1966.

[Bom78] E. Bombieri. On exponential sums in finite fields. II. *Invent. Math.*, 47(1):29–39, 1978.

[Dar05] M. R. Darafsheh. Order of elements in the groups related to the general linear group. *Finite Fields Appl.*, 11(4):738–747, 2005.

[Del77] P. Deligne. *Cohomologie étale*, volume 569 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1977. Séminaire de géométrie algébrique du Bois-Marie SGA $4\frac{1}{2}$.

[Fis92] Benji Fisher. Distinctness of Kloosterman sums. In *p-adic methods in number theory and algebraic geometry*, volume 133 of *Contemp. Math.*, pages 81–102. Amer. Math. Soc., Providence, RI, 1992.

[Han85] G. Hansel. A simple proof of the Skolem-Mahler-Lech theorem. In *Automata, languages and programming (Nafplion, 1985)*, volume 194 of *Lecture Notes in Comput. Sci.*, pages 244–249. Springer, Berlin, 1985.

[Lec53] Christer Lech. A note on recurring series. *Ark. Mat.*, 2:417–421, 1953.

[Liu07] Chunlei Liu. The L-functions of twisted Witt extensions. *J. Number Theory*, 125(2):267–284, 2007.

[LW07] Chunlei Liu and Dasheng Wei. The L-functions of Witt coverings. *Math. Z.*, 255(1):95–115, 2007.

[Wan21] Daqing Wan. Exponential Sums over Finite Fields. *J. Syst. Sci. Complex.*, 34(4):1225–1278, 2021.

[WY20] Daqing Wan and Hang Yin. Algebraic degree periodicity in recurrence sequences. *arXiv: Number Theory*, page 7, 2020.

[Zha21] Shenxing Zhang. The distinctness and generating fields of twisted kloosterman sums. *preprint*, 2021.

School of Mathematics, Hefei University of Technology, Hefei, Anhui 230009, China
Email address: zsxqq@mail.ustc.edu.cn