ELEMENTARY ESTIMATES FOR A CERTAIN TYPE OF SOTO-ANDRADE SUM

IMIN CHEN

Abstract. This paper shows that a certain type of Soto-Andrade sum can be estimated in an elementary way which does not use the Riemann hypothesis for curves over finite fields and which slightly sharpens previous estimates for this type of Soto-Andrade sum. As an application, we discuss how this implies that certain graphs arising from finite upper half planes in odd characteristic are Ramanujan without using the Riemann hypothesis.

1. Introduction

In [6], Soto-Andrade introduced a class of character sums which arose from the representation theory of GL_2 over a finite field. Following some of the conventions in Katz [2], we define these character sums as follows.

Let K/k be an extension of finite fields of degree n, where k has q elements and characteristic p. Let $\omega : K^\times \to \mathbb{C}^\times$ and $\epsilon : k^\times \to \mathbb{C}^\times$ be multiplicative characters of K and k, respectively, and let $N(u)$ and $T(u)$ be the norm and trace from K to k. Given a $t \in k$, a Soto-Andrade sum $S_{\epsilon,\omega}(t)$ is defined to be

Definition 1.1.

$$S_{\epsilon,\omega}(t) = \sum_{u \in K^1} \epsilon(t - T(u))\omega(u)$$

where $K^1 = \{u \in K, N(u) = 1\}$.

Non-trivial estimates for Soto-Andrade sums $S_{\epsilon,\omega}(t)$ were given in [2] using l-adic cohomology, though the case of $n = 2$ was shown to follow from the Riemann hypothesis for curves over finite fields. Another approach for $n = 2$ which uses class field theory of function fields to reduce to the Riemann hypothesis can be found in [4].

In this note, we make the simple remark that for $t = 0$, $S_{\epsilon,\omega}(t)$ can be estimated in an elementary way which does not require the Riemann hypothesis for curves over finite fields. The estimates obtained in this paper also slightly sharpen the estimates given in [2] for this particular case. As an application, we discuss how this implies that certain graphs arising from finite upper half planes in odd characteristic are Ramanujan without using the Riemann hypothesis for curves over finite fields.

2. An elementary estimate for $S_{\epsilon,\omega}(0)$

To begin, we note the following.

Date: 30 November 1998.

1991 *Mathematics Subject Classification.* Primary 11L40; Secondary 05C25, 20G40.

This research was supported by an NSERC postdoctoral fellowship and a grant from CICMA.

Lemma 2.1.

$$S_{\epsilon,\omega}(t) = \frac{1}{q-1} \sum_{\alpha^{q-1}=1} A_{\epsilon,\alpha\omega}(t)$$

where α runs through all multiplicative characters of K of order $q-1$ (such characters are of the form $\alpha(u) = \alpha' \circ N(u)$ for a multiplicative character α' of k) and

$$A_{\epsilon,\omega}(t) = \sum_{u \in K} \epsilon(t - T(u))\omega(u).$$

Proof. We simply note that

$$\begin{aligned}\sum_{u \in K^1} \epsilon(t - T(u))\omega(u) &= \sum_{u \in K} \left(\sum_{\alpha^{q-1}=1} \frac{1}{q-1} \alpha(u) \right) \epsilon(t - T(u))\omega(u) \\ &= \frac{1}{q-1} \sum_{\alpha^{q-1}=1} \sum_{u \in K} \epsilon(t - T(u))\alpha\omega(u)\end{aligned}$$

□

We now regard $A_{\epsilon,\omega}(t)$ as a complex function in $t \in k$ and then compute its Fourier transform (this follows the strategy in [2] in some sense where one computes the Fourier transform of $S_{\epsilon,\omega}(t)$ as a complex function in $t \in k$) This yields the following formulae.

Lemma 2.2.

$$\hat{A}_{\epsilon,\omega}(s) = \begin{cases} \textit{if } s \neq 0 & g_{\epsilon,\psi} \cdot g_{\omega,\psi} \cdot \overline{\epsilon\omega(s)} \\ \textit{if } s = 0 & \begin{cases} \textit{if } \epsilon = \omega = 1 & q^{n+1} \\ \textit{otherwise} & 0 \end{cases} \end{cases}$$

where $g_{\epsilon,\psi}$ is the Gauss sum associated to ϵ and a non-trivial additive character $\psi : k \to \mathbb{C}^\times$.

Proof. If $s \neq 0$, then

$$\begin{aligned}
\hat{A}_{\epsilon,\omega}(s) &= \sum_{t\in k} A_{\epsilon,\omega}(t)\psi(st) \\
&= \sum_{t\in k}\sum_{u\in K} \epsilon(t-T(u))\omega(u)\psi(st) \\
&= \sum_{u\in K}\omega(u)\sum_{t\in k}\epsilon(t-T(u))\psi(st) \\
&= \sum_{u\in K}\omega(u)\sum_{t'\in k}\epsilon(t')\psi(s(t'+T(u)) \\
&= \sum_{u\in K}\omega(u)\sum_{t'\in k}\epsilon(t')\psi(st')\psi(sT(u)) \\
&= \sum_{u\in K}\omega(u)\psi(sT(u))\overline{\epsilon(s)}\sum_{t'\in k}\epsilon(st')\psi(st') \\
&= g_{\epsilon,\psi}\cdot\overline{\epsilon(s)}\sum_{u\in K}\omega(u)\psi(sT(u)) \\
&= g_{\epsilon,\psi}\cdot\overline{\epsilon(s)\omega(s)}\sum_{u\in K}\omega(su)\psi(T(su)) \\
&= g_{\epsilon,\psi}\cdot g_{\omega,\psi}\cdot\overline{\epsilon\omega(s)}
\end{aligned}$$

If $s = 0$, then

$$\begin{aligned}
\hat{A}_{\epsilon,\omega}(s) &= \sum_{t\in k} A_{\epsilon,\omega}(t)\psi(st) \\
&\sum_{t\in k}\sum_{u\in K}\epsilon(t-T(u))\omega(u) \\
&\sum_{u\in K}\omega(u)\sum_{t\in k}\epsilon(t-T(u)) \\
&= 0
\end{aligned}$$

unless $\epsilon = \omega = 1$, in which case it is equal to q^{n+1}. ☐

By Fourier inversion, we may express $A_{\epsilon,\omega}(t)$ in terms of Gauss sums.

Lemma 2.3.

$$A_{\epsilon,\omega}(t) = \begin{cases} \textit{if } \epsilon=\omega=1 & \begin{cases} \textit{if } t\neq 0 & q^{n-1}(q-1)-1 \\ \textit{if } t=0 & q^{n-1}(q-1) \end{cases} \\ \textit{otherwise} & \begin{cases} \textit{if } t\neq 0 & \frac{1}{q}g_{\epsilon,\psi}\cdot g_{\omega,\psi}\cdot g_{\overline{\epsilon\omega_{|k}},\psi}\overline{\epsilon\omega(-t)} \\ \textit{if } t=0 & \begin{cases} \textit{if } \epsilon\omega_{|k}=1 & \frac{q-1}{q}g_{\epsilon,\psi}\cdot g_{\omega,\psi} \\ \textit{otherewise} & 0 \end{cases} \end{cases} \end{cases}$$

Proof. By Fourier inversion, we see that

$$A_{\epsilon,\omega}(t) = \frac{1}{q}\sum_{s\in k}\hat{A}_{\epsilon,\omega}(s)\overline{\psi(st)}.$$

If $\epsilon = \omega = 1$, then we can directly compute

$$\begin{aligned} A_{\epsilon,\omega}(t) &= \sum_{u\in K} \epsilon(t - T(u))\omega(u) \\ &= \#\{u \in K : T(u) \neq t \text{ and } u \neq 0\} \\ &= q^n - \#\{u \in K : T(u) = t\} - (1 - \delta(t)) \\ &= q^{n-1}(q-1) - 1 + \delta(t). \end{aligned}$$

Suppose now that one of $\epsilon, \omega \neq 1$. Then we have the following computations. If $t \neq 0$, then

$$\begin{aligned} A_{\epsilon,\omega}(t) &= \frac{1}{q} \sum_{s\in k} g_{\epsilon,\psi} \cdot g_{\omega,\psi} \overline{\epsilon\omega(s)\psi(st)} \\ &= \frac{1}{q} g_{\epsilon,\psi} \cdot g_{\omega,\psi} \sum_{s\in k} \overline{\epsilon\omega(s)\psi(st)} \\ &= \frac{1}{q} g_{\epsilon,\psi} \cdot g_{\omega,\psi} \cdot \epsilon\omega(-t) \sum_{s\in k} \overline{\epsilon\omega(-st)}\psi(-st) \\ &= \frac{1}{q} g_{\epsilon,\psi} \cdot g_{\omega,\psi} \cdot g_{\overline{\epsilon\omega_{|k}},\psi} \cdot \epsilon\omega(-t) \end{aligned}$$

If $t = 0$, then

$$\begin{aligned} A_{\epsilon,\omega}(t) &= \frac{1}{q} \sum_{s\in k} g_{\epsilon,\psi} \cdot g_{\omega,\psi} \overline{\epsilon\omega(s)\psi(st)} \\ &= \frac{1}{q} \sum_{s\in k} g_{\epsilon,\psi} \cdot g_{\omega,\psi} \overline{\epsilon\omega(s)} \\ &= 0 \end{aligned}$$

unless $\epsilon\omega_{|k} = 1$, in which case it is equal to $\frac{q-1}{q} g_{\epsilon,\psi} \cdot g_{\omega,\psi}$. □

From here on, we assume that one of $\epsilon, \omega \neq 1$ to avoid the following degenerate case.

Lemma 2.4. *If $\epsilon = \omega = 1$, then*

$$S_{\epsilon,\omega}(t) = \frac{q^n - 1}{q - 1} - \#\{u \in K^1 : T(u) = t\}.$$

Proof. If $\epsilon = \omega = 1$, we can directly compute

$$\begin{aligned} S_{\epsilon,\omega}(0) &= \sum_{u\in K^1} \epsilon(t - T(u))\omega(u) \\ &= \#\{u \in K^1 : T(u) \neq t\} \\ &= \frac{q^n - 1}{q - 1} - \#\{u \in K^1 : T(u) = 0\}. \end{aligned}$$

□

The following is then easily deduced from the above lemmas.

Theorem 1. *If one of $\epsilon, \omega \neq 1$, then*

$$S_{\epsilon,\omega}(0) = \begin{cases} \frac{1}{q} g_{\epsilon,\psi} \cdot \sum_{\phi^m=1} g_{\phi\beta^{-1}\omega,\psi} & \text{if } \epsilon\omega_{|k} = \beta'^n \text{ is an } n\text{-th power} \\ 0 & \text{otherwise} \end{cases}$$

where $\beta(u) = \beta' \circ N(u)$ and ϕ runs through all multiplicative characters of K of order dividing $m = (n, q-1)$.

Proof. From Lemma 2.1, we have that

$$S_{\epsilon,\omega}(0) = \frac{1}{q-1} \sum_{\alpha^{q-1}=1} A_{\epsilon,\alpha\omega}(0) \tag{1}$$

where $\alpha(u) = \alpha' \circ N(u)$ runs through all multiplicative characters of K of order $q-1$.

Since $\epsilon\alpha_{|_k}\omega_{|_k} = \epsilon{\alpha'}^n\omega_{|_k}$, by Lemma 2.3, we see that $A_{\epsilon,\alpha\omega} = 0$ except in the case that $\epsilon{\alpha'}^n\omega_{|_k} = 1$. Thus, if $\epsilon\omega_{|_k}$ is not an n-th power, then we see that $S_{\epsilon,\omega}(0) = 0$.

On the other hand, if $\epsilon\omega_{|_k} = {\beta'}^n$ is an n-th power, then setting $\beta(u) = \beta' \circ N(u)$, we see that the terms $A_{\epsilon,\alpha\omega}$, where $\alpha = \phi\beta^{-1}$ and ϕ is a multiplicative character of K of order $m = (n, q-1)$, contribute to the sum in 1. Hence, we have

$$S_{\epsilon,\omega}(0) = \frac{1}{q} g_{\epsilon,\psi} \sum_{\phi^m=1} g_{\phi\beta^{-1}\omega,\psi}.$$

□

Corollary 2.5. *If one of $\epsilon, \omega \neq 1$, then*

$$|S_{\epsilon,\omega}(0)| \leq (n, q-1) q^{\frac{n-1}{2}}.$$

Remark 2.6. *In the estimates given in* [2]*, the coefficient of $q^{\frac{n-1}{2}}$ is taken to be n or the prime-to-p-part of n if p divides n.*

3. An application to graph theory

In this section, let K/k be a *quadratic* extension of finite fields, where k has q elements and *odd* characteristic p. The group $G = \mathrm{GL}_2(k)$ acts on $\mathbb{P}^1(K)$ via fractional linear transformations and leaves invariant $\mathbb{P}^1(k) \subset \mathbb{P}^1(K)$. An analogue of the classical Poincaré upper half plane, is $\mathfrak{H} = \mathbb{P}^1(K) - \mathbb{P}^1(k) = \{z \in K \mid z \notin k\}$. Let δ be a non-square in k and choose an element $\theta \in \mathrm{GL}_2(k)$ such that $\theta^2 = \delta$. The given field K can thus be realised as $K \cong k(\theta) \subset M_2(k)$ so that $\mathfrak{H}$ can be described as $\mathfrak{H} = \{x + y\theta \mid x \in k, y \in k^\times\} \subset M_2(k)$.

In [7], certain graphs arising from $\mathfrak{H}$ were introduced and studied. Following [1], we briefly recall their construction and main properties (the description given in [1] is restricted to the case $k = \mathbb{F}_p$ so $q = p$, but the construction still holds for general k with the provision that p is replaced by q). For an equivalent description using double cosets, see [3] or [4].

Given two points $z, w \in \mathfrak{H}$, the hyperbolic distance between z and w is defined to be $d(z,w) = \frac{N_{K/k}(z-w)}{\mathrm{Im}(z)\mathrm{Im}(w)}$ where $\mathrm{Im}(x + y\theta) = y$. The hyperbolic distance is invariant under the action of G. For each $a \in k$, we define the graph G_a to be the graph whose vertices are points of $\mathfrak{H}$ and whose edges connect any two points of $\mathfrak{H}$ if the hyperbolic distance between them is a. It was shown in [1], that G_a is a $(q+1)$-regular graph for $a \neq 0$ nor 4δ.

An eigenvalue λ of the adjacency matrix of G_a is said to be *non-trivial* if $|\lambda| \neq q+1$. A $(q+1)$-regular graph is said to be *Ramanujan* if all the non-trivial eigenvalues of its adjacency matrix have absolute value $\leq 2\sqrt{q}$. There has been some interest in establishing that the graphs G_a are Ramanujan for $a \neq 0$ nor 4δ [7] (see also [1] and [3] for further background on this topic).

The non-trivial eigenvalues of the adjacency matrix of G_a are given by

$$\lambda_\chi = -\sum_{y \in k} \epsilon(\frac{a}{\delta} y + (y-1)^2)\chi(y)$$
$$\lambda_\omega = \omega(-1) S_{\epsilon,\omega}(\frac{a}{\delta} - 2)$$

for all non-trivial characters χ of $k^\times$, and all characters ω of $K^\times$ which are non-trivial on K^1, where ϵ denotes the unique quadratic character of $k^\times$ (c.f. [4] and the references cited therein for more details).

The character sum λ_χ is essentially a *Legendre character sum* [5]. According to [4], Evans and Stark independently showed that $|\lambda_\chi| \leq 2\sqrt{q}$ using Weil's estimate [8] which relies on the Riemann hypothesis for curves over finite fields.

It was shown in [5], Proposition 3, using elementary methods that

Proposition 3.1.

$$\sum_{y \in k} \epsilon(1+y^2)\chi(y) = \begin{cases} 0 & \text{if } \chi \text{ is not a square} \\ \psi(-1)J(\epsilon, \overline{\psi}) + \epsilon(-1)J(\epsilon, \epsilon\overline{\psi}) & \text{if } \chi = \psi^2 \end{cases}$$

where $J(A, B)$ denotes the Jacobi sum of two characters A, B of $k^\times$. It follows for $a = 2\delta$, that $|\lambda_\chi| \leq 2\sqrt{q}$ using the fact that the Jacobi sums in the expressions above have absolute value $\sqrt{q}$. On the other hand, for $a = 2\delta$, we have that $S_{\epsilon,\omega}(\frac{a}{\delta} - 2) = S_{\epsilon,\omega}(0)$ so λ_ω is $\leq 2\sqrt{q}$ in absolute value by Corollary 2.5. Hence, for the special case $a = 2\delta$ we obtain (without the Riemann hypothesis for curves over finite fields) that

Corollary 3.2. *$G_{2\delta}$ is a Ramanujan graph.*

4. Acknowledgements

I would like to thank S. Edixhoven and l'Institut de Recherche Mathématique de Rennes for their warm hospitality during my stay there in Spring 1998.

References

[1] N. Celniker, S. Poulos, and A. Terras. Is there life on finite upper half planes? In *A tribute to Emil Grosswald: Number Theory and Related Analysis*, volume 143 of *Contemporary Mathematics*. AMS, 1993.

[2] N. Katz. Estimates for Soto-Andrade sums. *Journal für die Reine und Angewandte Mathematik*, 438:143–161, 1993.

[3] Wen-Ch'ing Winnie Li. Number-theoretic constructions of ramanujan graphs. *Astérisque*, 3-4(228):101–120, 1995.

[4] Wen-Ching Winnie Li. Estimates of character sums arising from finite upper half planes. In Cohen S. and Niederreiter H., editors, *Finite fields and applications (Glasgow, 1995)*, number 233 in London Mathematical Society Lecture Notes. Cambridge University Press, 1996.

[5] Y. Sawabe. Legendre character sums. *Hiroshima Mathematical Journal*, 22:15–22, 1992.

[6] J. Soto-Andrade. Geometrical Gelfand models, tensor quotients, and Weil representations. In *Proceedings of Symposia in Pure Mathematics*, volume 47, pages 305–316, 1987.

[7] A. Terras. Are finite upper half plane graphs Ramanujan? In *Expanding Graphs (Princeton, NJ, 1992)*, volume 10 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 125–142. American Mathematical Society, Providence, RI, 1993.

[8] A. Weil. On some exponential sums. In *Proceedings of the National Academy of Sciences*, volume 34, pages 204–207, 1948.

Department of Mathematics and Statistics, McGill University, Montreal, Quebec, Canada, H3A 2K6
E-mail address: chen@math.mcgill.ca