Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 37 (1991)

Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE EVALUATION OF SELBERG CHARACTER SUMS

Autor: Evans, Ronald J.

Kapitel: §1. Introduction

DOI: https://doi.org/10.5169/seals-58741

L'Enseignement Mathématique, t. 37 (1991), p. 235-248

THE EVALUATION OF SELBERG CHARACTER SUMS

by Ronald J. EVANS

ABSTRACT. The evaluations of Selberg character sums conjectured on p. 207 of *Enseignement Math. 27* (1981) are proved.

§ 1. INTRODUCTION

Many of the classical special functions over **C** have character sum analogs over finite fields. For example, the Gauss and Jacobi sums defined in (1.1) are analogs of the gamma and beta integrals

$$\Gamma(a) = \int_0^\infty e^{-x} x^a \frac{dx}{x}, \qquad \beta(a,b) = \int_0^1 x^a (1-x)^b \frac{dx}{x(1-x)}.$$

Some identities for character sums over finite fields seem more difficult to prove than their classical counterparts; compare, e.g., the Hasse-Davenport product formula for Gauss sums [7, (7)] with the Gauss multiplication formula for gamma functions. The identities for n-dimensional Selberg character sums given in Theorems 1.1, 1.1a provide further examples. Their counterparts are the well known n-dimensional Selberg integral extensions of the gamma and beta integral formulas.

The case $n = 3$ of the Selberg character sum identity in Theorem 1.1 has been used to evaluate a sum connected with the root system G_2 [8]. The case $n = 2$ is equivalent to an analog of Dixon's summation formula [11, (2.1.5)] involving hypergeometric ${}_3F_2$ character sums over finite fields. We remark that hypergeometric character sums have been used, e.g., in the computation of the number of points on hypersurfaces [13], [12], in proving congruences for Apery numbers [14], and in graph theory [6], [9].

Let $GF(q)$ be a finite field of q elements, where q is a power of an odd prime. Fix a multiplicative character $\tau: GF(q)^* \to \mathbf{C}^*$ of order $q-1$ and a nontrivial additive character $\psi: GF(q) \to \mathbf{C}^*$. Extend τ by defining $\tau(0) = 0$. Let $\phi = \tau^{(q-1)/2}$ be the quadratic character on $GF(q)$. For all integers a, b, define the Gauss sums $G(a)$ and Jacobi sums $J(a,b)$ by

(1.1) $$G(a)=\sum_{\xi\in GF(q)^*}\tau(\xi)^a\psi(\xi)\,,\qquad J(a,b)=\sum_{1\neq\xi\in GF(q)^*}\tau(\xi)^a\tau(1-\xi)^b\,.$$

For integers $n\geqslant 0$ and $a,b,c>0$, define the Selberg character sums

(1.2) $$S_n(a,b,c)=\sum_E\tau((-1)^{an}E(0)^aE(1)^b\Delta_E^c)\phi(\Delta_E)\,,$$

(1.2a) $$S_n(a,c)=\sum_E\psi(e_{n-1})\tau(E(0)^a\Delta_E^c)\phi(\Delta_E)\,,$$

(1.2b) $$S_n(c)=\sum_E\psi(e_{n-1}^2/2-e_{n-2})\tau(\Delta_E)^c\phi(\Delta_E)\,,$$

where each sum is over all monic polynomials

(1.3) $$E=E(x)=x^n+e_{n-1}x^{n-1}+e_{n-2}x^{n-2}+\cdots+e_0$$

of degree n over $GF(q)$, and where Δ_E denotes the discriminant of E (with the convention that $\Delta_E=1$ when $\deg(E)\leqslant 1$). Define the following products:

(1.4) $$P_n(a,b,c)=\prod_{j=0}^{n-1}\frac{G(a+jc)G(b+jc)G(c+jc)\bar{G}(a+b+(n-1+j)c)}{qG(c)}\,,$$

(1.4a) $$P_n(a,c)=\prod_{j=0}^{n-1}\frac{G(a+jc)G(c+jc)}{G(c)}\,,$$

(1.4b) $$P_n(c)=\prod_{j=0}^{n-1}\frac{G(c+jc)\phi(2)G((q-1)/2)}{G(c)}\,,$$

where $\bar{G}$ denotes the complex conjugate of G.

The object of this paper is to prove Theorems 1.1, 1.1a, and 1.1b below. These results, analogs of n-dimensional integral formulas of Selberg [3, (1.1), (1.3), (1.2)], [2], verify conjectures made in 1981 [7, (29), (29a), (29b)]. The decisive breakthrough came in 1990 when Anderson [1] proved a somewhat weakened form of Theorem 1.1. The proofs here are based on modifications of the method in [1]. The modifications are designed to handle complications arising from "imprimitive" L-functions (see §2).

THEOREM 1.1. *For all integers* $n,a,b,c>0$, *if none of*

$$a+b+(n-1+j)c\qquad(0\leqslant j\leqslant n-1)$$

are divisible by $q-1$, *then* $S_n(a,b,c)=P_n(a,b,c)$.

THEOREM 1.1a. *For all integers* $n, a, c > 0$, $\quad S_n(a,c) = P_n(a,c)$.

THEOREM 1.1b. *For all integers* $n, c > 0$, $\quad S_n(c) = P_n(c)$.

Given a monic polynomial E over $GF(q)$, define $\sigma(E) = 0$ if E is not squarefree, $\sigma(E) = 1$ if $E = 1$, and otherwise let $\sigma(E)$ denote the sign of the permutation of the zeros of E effected by the q^{th} power automorphism of $\overline{GF(q)}$. For odd q, $\sigma(E) = \phi(\Delta_E)$. If $\phi(\Delta_E)$ is replaced by $\sigma(E)$ in the definitions (1.2), (1.2a) of $S_n(a,b,c)$, $S_n(a,c)$, then Theorems 1.1 and 1.1a remain valid without the stipulation "q odd"; the proofs for even q are virtually the same. This observation is due to Serre; see [1].

The following result is equivalent to Theorem 1.1, as was shown in [10, p. 116].

THEOREM 1.2. *For integers* $n,a,b,c > 0$, *if none of* $a + jc$ $(0 \leqslant j \leqslant n-1)$ *are divisible by* $q-1$, *or if none of* $b + jc$ $(0 \leqslant j \leqslant n-1)$ *are divisible by* $q-1$, *or if none of* $a + b + (n-1+j)c$ $(0 \leqslant j \leqslant n-1)$ *are divisible by* $q-1$, *then* $S_n(a,b,c) = P_n(a,b,c)$.

Theorems 1.3 and 1.4 below, analogs of more recent Selberg integral formulas (see [4]), were stated as conjectures in [5]. They are consequences of Theorems 1.1a and 1.1b, respectively, as is shown in [5, Theorems 2.2 and 2.5].

THEOREM 1.3. *For all integers* $n, a, b, c > 0$,

$$\sum_E \tau(E(0)^a (1 + e_{n-1})^b \Delta_E^c)\phi(\Delta_E)$$

$$= \begin{cases} \dfrac{G(-b-na-n(n-1)c)}{G(-b)} P_n(a,c)\,, & \text{if} \quad b \not\equiv 0 \pmod{q-1} \\[2ex] \dfrac{\tau(-1)^{an} G(b)}{G(b+na+n(n-1)c)} P_n(a,c)\,, & \text{if} \quad b + na + n(n-1)\,c \\ & \qquad \not\equiv 0 \pmod{q-1}\,, \end{cases}$$

where the sum is over all polynomials E *of degree* n *given by (1.3).*

THEOREM 1.4. *For* $w \in GF(q)^*$ *and all integers* $n, b, c > 0$ *with* $b \not\equiv 0 \pmod{q-1}$,

$$\sum_E \tau((w + e_{n-1}^2/2 - e_{n-2})^b \Delta_E^c)\phi(\Delta_E)$$

$$= \tau(w)^{b+n(q-1)/2+cn(n-1)/2} \frac{G(-b-cn(n-1)/2-n(q-1)/2)}{G(-b)} P_n(c)\,,$$

where the sum is over all polynomials E *of degree* n *given by (1.3).*

Acknowledgement. We are very grateful to G. W. Anderson for helpful correspondence on L-functions and character sums.

§2. L-FUNCTIONS

Throughout this section, V denotes a *monic* polynomial over $GF(q)$, and υ ranges over the distinct monic irreducible factors of V over $GF(q)$. Write

$$V = \prod_{\upsilon | V} \upsilon^{\operatorname{ord}_\upsilon V}, \quad F = F_V = \prod_{\upsilon | V} \upsilon . \tag{2.1}$$

If no exponent $\operatorname{ord}_\upsilon V$ in (2.1) is divisible by $q - 1$, then V is said to be *primitive.* Note that $V = 1$ is primitive. For any monic polynomial

$$W = W(x) = x^n + w_{n-1}x^{n-1} + w_{n-2}x^{n-2} + \cdots + w_0 \tag{2.2}$$

over $GF(q)$, set

$$\alpha(W) = w_{n-1}, \quad \beta(W) = w_{n-1}^2/2 - w_{n-2} . \tag{2.3}$$

Define the L-functions

$$L(t, V) = \sum_W \tau(R(V, W))t^{\deg W}, \tag{2.4}$$

$$L_1(t, V) = \sum_W \psi(\alpha(W))\tau(R(V, W))t^{\deg W}, \tag{2.4a}$$

$$L_2(t, V) = \sum_W \psi(\beta(W))\tau(R(V, W))t^{\deg W}, \tag{2.4b}$$

where in each sum, W ranges over all monic polynomials over $GF(q)$, and $R(V, W)$ is the resultant of V and W. It is easily checked that

$$\begin{aligned} L(t, 1) &= (1 - qt)^{-1}, \quad L_1(t, 1) = 1, \\ L_2(t, 1) &= 1 + \phi(2)G((q-1)/2)t . \end{aligned} \tag{2.5}$$

Since the summands in (2.4), (2.4a), (2.4b) are multiplicative in W, each of the L-functions has an Euler product expansion. Thus we have the following result.

LEMMA 2.1. *Write $V = GH$ where G and H are monic, relatively prime polynomials over $GF(q)$ with G primitive and H a $(q-1)$th power. Then*

$$L(t, V) = L(t, G) \prod_{\upsilon | H} (1 - \tau(R(G, \upsilon))t^{\deg \upsilon}), \tag{2.6}$$

$$L_1(t, V) = L_1(t, G) \prod_{\upsilon | H} (1 - \psi(\alpha(\upsilon))\tau(R(G, \upsilon))t^{\deg \upsilon}), \tag{2.6a}$$