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.
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

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

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

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

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

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

where each sum is over all monic polynomials

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

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:

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

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

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

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*

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

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

and

$$L_2(t, V) = L_2(t, G) \prod_{v|H} (1 - \psi(\beta(v))\tau(R(G, v))t^{\deg v}) . \tag{2.6b}$$

The next lemma evaluates certain generating functions defined in terms of the function L (but not L_1 or L_2).

LEMMA 2.2. *For all integers* $a, b > 0$,

$$\sum_W \tau(W^a(0)\, W^b(1))L(t, W^{q-1})z^{\deg W}$$

$$= \begin{cases} \dfrac{1 + \tau(-1)^a J(a, b)z}{(1-qt)\,(1+\tau(-1)^a J(a, b)zt)}, & \text{if} \quad a \not\equiv 0 \pmod{q-1} \\ & \quad\text{or} \quad b \not\equiv 0 \pmod{q-1}, \\ \dfrac{(1-z)^2(1-qzt)}{(1-qt)\,(1-qz)\,(1-zt)^2}, & \text{if} \quad a \equiv b \equiv 0 \pmod{q-1}, \end{cases} \tag{2.7}$$

$$\sum_W \psi(\alpha(W^b))\tau(W(0)^a)L(t, W^{q-1})z^{\deg W} = \frac{1 + \bar{\tau}^a(b)G(a)z}{(1-qt)\,(1+\bar{\tau}^a(b)G(a)zt)}, \tag{2.7a}$$

and

$$\sum_W \psi(\beta(W^b))L(t, W^{q-1})z^{\deg W} = \frac{1 + \phi(2b)G((q-1)/2)z}{(1-qt)\,(1+\phi(2b)G((q-1)/2)zt)}, \tag{2.7b}$$

where in each sum, W *ranges over all monic polynomials over* $GF(q)$ *and* α, β *are as defined in (2.3).*

Proof. Fix monic $V = V(x)$ and let w range over monic irreducibles over $GF(q)$. By (2.6),

$$\begin{aligned} &\sum_W \tau(R(V, W))L(t, W^{q-1})z^{\deg W} \\ &= L(t, 1)\sum_W z^{\deg W}\tau(R(V, W)) \prod_{w|W} (1 - t^{\deg w}) \\ &= L(t, 1)\sum_W \prod_{w|W} \{(1 - t^{\deg w})\, (\tau(R(V, w))z^{\deg w})^{\mathrm{ord}_w W}\} \\ &= L(t, 1)\prod_w \left\{1 + (1 - t^{\deg w}) \sum_{m=1}^{\infty} (\tau(R(V, w))z^{\deg w})^m\right\} \\ &= L(t, 1)\prod_w \frac{1 - \tau(R(V, w))\,(zt)^{\deg w}}{1 - \tau(R(V, w))z^{\deg w}} = \frac{L(t, 1)L(z, V)}{L(zt, V)} . \end{aligned}$$

Taking $V = x^a(x-1)^b$, we easily deduce (2.7). The proofs of (2.7a) and (2.7b) are similar. $\square$

It is shown in [1, Prop. 2.1] that if V is primitive of degree > 0, then $L(t, V)$ is a polynomial in t of degree $(\deg F - 1)$ with leading coefficient

$$\varepsilon(V) = \sigma(F)\tau(R(V, F'))G^*(\deg V)^{-1} \prod_{v|F} G^*(\mathrm{ord}_v V)^{\deg v}, \tag{2.8}$$

where

$$G^*(a) := q/G(-a).$$

By (2.6), if V is a $(q-1)$th power, then

$$L(t, V) = (1-qt)^{-1} \prod_{v|V} (1 - t^{\deg v}),$$

but otherwise $L(t, V)$ is a polynomial of degree $(\deg F - 1)$. The following lemma shows that for all V, $L_1(t, V)$ and $L_2(t, V)$ are polynomials of degrees $\deg F$ and $\deg F + 1$, respectively. Moreover, for primitive $V \neq 1$, the coefficient $\varepsilon_1(V)$ of $t^{\deg F}$ in $L_1(t, V)$ and the coefficient $\varepsilon_2(V)$ of $t^{1+\deg F}$ in $L_2(t, V)$ are given explicitly.

LEMMA 2.3. *For each monic polynomial V over $GF(q)$, $L_1(t, V)$ and $L_2(t, V)$ are polynomials in t of degrees $\deg F$ and $1 + \deg F$, respectively. If moreover $V \neq 1$ is primitive, the leading coefficients of $L_1(t, V)$ and $L_2(t, V)$ are given by*

$$\varepsilon_1(V) = \psi(\alpha(F))\sigma(F)\tau(R(V, -F')) \prod_{v|F} G^*(\mathrm{ord}_v V)^{\deg v}, \tag{2.8a}$$

and

$$\varepsilon_2(V) = \phi(2)G((q-1)/2)\psi(\beta(F))\sigma(F)\tau(R(V, F')) \prod_{v|F} G^*(\mathrm{ord}_v V)^{\deg v}, \tag{2.8b}$$

respectively, where $G^*(a) = q/G(-a)$.

Proof. Fix an integer $m > \deg F$ and fix $\alpha \in GF(q)$. Since $m > \deg F$, it is not hard to see that the monic polynomials W over $GF(q)$ of degree m with $\alpha(W) = \alpha$ run through each residue class modulo F exactly $q^{m-1-\deg F}$ times. Since $R(V, W)$ depends only on the residue class of W modulo F, the coefficient of t^m in $L_1(t, V)$ thus equals

$$\sum_{\substack{W \text{ monic} \\ \deg W = m}} \psi(\alpha(W))\tau(R(V, W))$$

$$= q^{m-1-\deg F} \sum_{\substack{U \\ \deg U < \deg F}} \tau(R(V, U)) \sum_{\alpha \in GF(q)} \psi(\alpha) = 0 .$$

Therefore $L_1(t, V)$ is a polynomial of degree $\leqslant \deg F$. Similar reasoning with $\beta(W)$ in place of $\alpha(W)$ shows that $L_2(t, V)$ is a polynomial of degree $\leqslant 1 + \deg F$. In view of (2.5), (2.6*a*) and (2.6*b*), it remains to prove (2.8*a*) and (2.8*b*) for primitive $V \neq 1$.

To prove (2.8*a*), consider the double sum

$$\mu_1 := \sum_U \sum_W \psi\left(-\operatorname{Res}_\infty \frac{U(x)W(x)}{F(x)}\right) \psi(\alpha(W))\bar{\tau}(R(V, U)) , \tag{2.9}$$

where $W = W(x)$ ranges over monic polynomials of degree $D := \deg F$ over $GF(q)$ and $U = U(x)$ ranges over nonzero polynomials of degree $< D$ over $GF(q)$. Write $k = \deg U$,

$$W(x) = w_D x^D + w_{D-1}x^{D-1} + \cdots + w_0 , \quad (w_D = 1) , \tag{2.10}$$

and

$$\frac{x^k U(1/x)}{x^D F(1/x)} = a_0 + a_1 x + a_2 x^2 + \cdots . \tag{2.11}$$

Note that $a_0 \neq 0$ is the leading coefficient of $U(x)$. We have

$$\psi\left(\alpha(W) - \operatorname{Res}_\infty \frac{UW}{F}\right) = \psi\left(w_{D-1} + \sum_{i=0}^{k+1} a_{k+1-i} w_{D-i}\right) . \tag{2.12}$$

For fixed U, the sum over W in (2.9) thus vanishes unless $U(x) = -1$. When $U(x) = -1$, each member of (2.12) equals $\psi(a_1) = \psi(\alpha(F))$. Therefore

$$\mu_1 = q^{\deg F}\tau(-1)^{\deg V}\psi(\alpha(F)) . \tag{2.13}$$

On the other hand, by the proof of the last formula in [1, § 2] (here primitivity is used), we have

$$\mu_1 = \varepsilon_1(V)\sigma(F)\bar{\tau}(R(V, F')) \prod_{v|F} G(-\operatorname{ord}_v V)^{\deg v} . \tag{2.14}$$

Comparison of (2.13) and (2.14) yields (2.8*a*).

To prove (2.8*b*), consider the double sum

$$(2.15)\qquad \mu_2 := \sum_U \sum_Y \psi\left(-\operatorname{Res}_\infty \frac{U(x)\,Y(x)}{F(x)}\right) \psi(\beta(Y))\bar{\tau}(R(V,U))$$

where Y ranges over monic polynomials of degree $D+1$ over $GF(q)$ (with $D = \deg F$) and U ranges over nonzero polynomials of degree $< D$ over $GF(q)$. Write $k = \deg U$ and

$$(2.16)\qquad Y(x) = y_{D+1}x^{D+1} + y_D x^D + \cdots + y_0\,, \qquad (y_{D+1} = 1)\,.$$

In the notation of (2.11),

$$(2.17)\qquad \psi\left(\beta(Y) - \operatorname{Res}_\infty \frac{UY}{F}\right) = \psi\left(y_D^2/2 - y_{D-1} + \sum_{i=0}^{k+2} a_{k+2-i}y_{D+1-i}\right)\,.$$

For fixed U, the sum over Y in (2.15) vanishes unless $U(x) = 1$. When $U(x) = 1$, each member of (2.17) equals $\psi(a_2 + a_1 y_D + y_D^2/2)$ with

$$a_1 = -\,\alpha(F)\,, \qquad a_2 = \alpha(F)^2/2 + \beta(F)\,.$$

Therefore

$$(2.18)\qquad \mu_2 = q^D\psi(\beta(F)) \sum_{y \in GF(q)} \psi(y^2/2) = q^D\psi(\beta(F))\phi(2)G((q-1)/2)\,.$$

On the other hand, by the proof of the last formula in [1, §2], we have

$$(2.19)\qquad \mu_2 = \varepsilon_2(V)\sigma(F)\bar{\tau}(R(V,F')) \prod_{v|F} G(-\operatorname{ord}_v V)^{\deg v}\,.$$

Comparison of (2.18) and (2.19) yields (2.8*b*).

§3. Proof of Theorems 1.1, 1.1*a*, 1.1*b*

Let d denote the order of τ^c. The following lemma gives useful formulas for $P_n(a,b,c)$, $P_n(a,c)$, and $P_n(c)$ in the case $d \mid n$. The proof of (3.1*b*) is elementary but for (3.1) and (3.1*a*) we require the Hasse-Davenport product formula [7, (7)].

LEMMA 3.1. *Let d be the smallest positive integer such that $cd \equiv 0 \pmod{q-1}$. If $d \mid n$, then*

$$(3.1)\quad P_n(a,b,c) = \begin{cases} \dfrac{(-J(ad,bd))^{n/d}\tau(-1)^{c\binom{n}{2}}q^{n-n/d}}{G(c)^n}, & \text{if } ad \not\equiv 0 \pmod{q-1} \\ & \text{or } bd \not\equiv 0 \pmod{q-1} \\ \dfrac{q^{n-2n/d}\tau(-1)^{c\binom{n}{2}}}{G(c)^n}, & \text{if } ad \equiv bd \equiv 0 \\ & \pmod{q-1}, \end{cases}$$

$$(3.1a)\qquad P_n(a,c) = \frac{(-\bar{\tau}^{ad}(d)G(ad))^{n/d}\tau(-1)^{c\binom{n}{2}}q^{n-n/d}}{G(c)^n},$$

and

$$(3.1b)\qquad P_n(c) = \frac{(-\phi(2d)G((q-1)/2))^{n/d}\tau(-1)^{c\binom{n}{2}}q^{n-n/d}}{G(c)^n}.$$

Proof. By the Hasse-Davenport product formula [7, (7)],

$$(3.2)\qquad \prod_{j=0}^{d-1} G(a+jc) = -\bar{\tau}^{ad}(d)G(ad)\prod_{j=0}^{d-1} G(jc).$$

It follows from (1.4) and (3.2) that

$$(3.3)\qquad P_d(a,b,c) = \frac{-G(ad)G(bd)\bar{G}(ad+bd)q^{d-2}\tau(-1)^{c\binom{d}{2}}}{G(c)^d}.$$

Thus

$$(3.4)\qquad P_d(a,b,c) = \begin{cases} \dfrac{q^{d-2}\tau(-1)^{c\binom{d}{2}}}{G(c)^d}, & \text{if } \quad ad \equiv bd \equiv 0 \\ & \pmod{q-1} \\ \dfrac{-J(ad,bd)\tau(-1)^{c\binom{d}{2}}q^{d-1}}{G(c)^d}, & \text{otherwise}. \end{cases}$$

As $d \mid n$, we have $P_n(a,b,c) = P_d(a,b,c)^{n/d}$. Since

$$\tau(-1)^{cn(d-1)/2} = \tau(-1)^{c\binom{n}{2}},$$

(3.1) follows. The proof of (3.1a) is similar. If in place of (3.2) one uses the formula

$$(3.5)\qquad \phi(d) = \prod_{j=1}^{d-1} \frac{G(jc)}{\phi(2)G((q-1)/2)},$$

which is a consequence of quadratic reciprocity, then (3.1b) readily follows. □

For positive integers n, a, b, c, define the double sums

$$Y := \sum_Q \sum_P \tau(Q(0)^a Q(1)^b R(Q^c, P)) , \tag{3.6}$$

$$Y_1 := \sum_Q \sum_P \psi(\alpha(Q)) \tau(Q(0)^a R(Q^c, P)) , \tag{3.6a}$$

and

$$Y_2 := \sum_Q \sum_P \psi(\beta(Q)) \tau(R(Q^c, P)) , \tag{3.6b}$$

where here and in the sequel, P and Q range over monic polynomials over $GF(q)$ with

$$\deg P = n - 1 , \quad \deg Q = n . \tag{3.7}$$

In the next lemma, we evaluate Y, Y_1, and Y_2 in terms of the Selberg sums $S_n(a, b, c)$, $S_n(a, c)$, and $S_n(c)$, respectively.

LEMMA 3.2. *Assume that* $c \not\equiv 0 \pmod{q-1}$ *and that for all* j *with* $0 \leqslant j \leqslant n - 1$, $b + jc \not\equiv 0 \pmod{q-1}$. *Then*

$$Y = \begin{cases} \tau(-1)^{an + c\binom{n}{2}} S_n(a, b, c) G(c)^n / G(cn) , & \text{if } d \nmid n \\ \tau(-1)^{an + c\binom{n}{2}} \dfrac{G(c)^n}{qG(cn)} \{S_n(a,b,c) + (q-1) P_n(a, b, c)\} & \text{if } d \mid n , \end{cases} \tag{3.8}$$

$$Y_1 = \begin{cases} \tau(-1)^{c\binom{n}{2}} S_n(a, c) G(c)^n / G(cn) , & \text{if } d \nmid n \\ \tau(-1)^{c\binom{n}{2}} \dfrac{G(c)^n}{qG(cn)} \{S_n(a,c) + (q-1) P_n(a, c)\} , & \text{if } d \mid n , \end{cases} \tag{3.8a}$$

and

$$Y_2 = \begin{cases} \tau(-1)^{c\binom{n}{2}} S_n(c) G(c)^n / G(cn) , & \text{if } d \nmid n \\ \tau(-1)^{c\binom{n}{2}} \dfrac{G(c)^n}{qG(cn)} \{S_n(c) + (q-1) P_n(c)\} , & \text{if } d \mid n . \end{cases} \tag{3.8b}$$

Proof. Note that $d > 1$ by hypothesis. Write

$$Y = A + B , \tag{3.9}$$

where A is the sum over those Q which are not d^{th} powers, and B is the sum over those Q of the form $Q = W^d$ (for monic W with $\deg W = n/d$). Observe that Q is a d^{th} power if and only if $V = Q^c$ is a $(q-1)^{th}$ power. For those Q for which V is not a $(q-1)^{th}$ power, there can be a contribution to A only if Q is squarefree, since $L(t, V)$ is a polynomial of degree $(\deg F - 1)$. Thus

$$A = \sum_{Q \text{ squarefree}} \tau(Q^a(0)Q^b(1))\,\varepsilon(Q^c)\,.$$

By (2.8), it follows that

$$A = \tau(-1)^{an + c\binom{n}{2}} S_n(a,b,c)G^*(c)^n/G^*(cn)\,. \tag{3.10}$$

If $d \nmid n$, then Q cannot be a d^{th} power, so $Y = A$. Moreover, if $d \nmid n$, then $cn \not\equiv 0 \pmod{q-1}$, so $G^*(c)^n/G^*(cn) = G(c)^n/G(cn)$. This proves (3.8) in the case $d \nmid n$.

Suppose now that $d \mid n$. Then

$$B = \sum_W \tau(W^{ad}(0)\,W^{bd}(1)) \sum_P \tau(R(W^{cd}, P))$$

where W ranges over monic polynomials over $GF(q)$ of degree n/d. Thus B is the coefficient of $t^{n-1}z^{n/d}$ in

$$\sum_U \tau(U^{ad}(0)\,U^{bd}(1))L(t, U^{q-1})z^{\deg U}\,,$$

where U ranges over all monic polynomials over $GF(q)$. If $bd \equiv 0 \pmod{q-1}$, then $b + cj \equiv 0 \pmod{q-1}$ for some j, $0 \leqslant j \leqslant d-1$, which contradicts the hypothesis. Thus $bd \not\equiv 0 \pmod{q-1}$, so by (2.7),

$$B = (-J(ad, bd))^{n/d}\tau(-1)^{an}q^{n-n/d-1}(1-q)\,.$$

Since $G(cn) = -1$, it follows from (3.1) that

$$B = \tau(-1)^{an + c\binom{n}{2}} \frac{G(c)^n}{qG(cn)} P_n(a,b,c)\,(q-1)\,. \tag{3.11}$$

By (3.9)-(3.11), the proof of (3.8) is completed. The proofs of (3.8a) and (3.8b) follow similarly. $\square$

By reversing the order of summation in the double sums Y, Y_1, and Y_2, we can express them in terms of $S_{n-1}(a+c, b+c, c)$, $S_{n-1}(a+c, c)$, and $S_{n-1}(c)$, respectively, as the following lemma shows.

LEMMA 3.3. *Assume that* $c \not\equiv 0 \pmod{q-1}$ *and that for all* j *with* $0 \leqslant j \leqslant n-1$, $b + jc \not\equiv 0 \pmod{q-1}$. *Then*

$$(3.12)\qquad Y=\tau(-1)^{an+c\binom{n}{2}}S_{n-1}(a+c,b+c,c)G(a)G(b)G(c)^{n-1}\cdot\bar{G}(a+b+(n-1)c)/q\ ,$$

$$(3.12a)\qquad Y_1=\tau(-1)^{c\binom{n}{2}}S_{n-1}(a+c,c)G(a)G(c)^{n-1}\ ,$$

and

$$(3.12b)\qquad Y_2=\tau(-1)^{c\binom{n}{2}}S_{n-1}(c)G(c)^{n-1}\phi(2)G((q-1)/2)\ .$$

Proof. We have

$$(3.13)\qquad Y=\sum_P\sum_Q\tau(R(V,Q))\ ,$$

where

$$V=x^a(x-1)^bP^c\ .$$

By hypothesis, V is not a $(q-1)^{th}$ power, so $L(t,V)$ is a polynomial of degree $(\deg F-1)$. Thus we may restrict P to be squarefree and prime to $x(x-1)$ (so $\deg F=n+1$), as no other P contribute to Y.

Suppose that $a\not\equiv 0 \pmod{q-1}$. Then V is primitive and (3.13) yields

$$Y=\sum_P\varepsilon(V)\ ,$$

so (3.12) follows by (2.8).

Now suppose that $a\equiv 0\pmod{q-1}$. Then by (3.13) and (2.6),

$$Y=-\sum_P\varepsilon((x-1)^bP^c)\tau(R((x-1)^bP^c,x))\ ,$$

and again (3.12) follows by (2.8).

To prove (3.12*a*) and (3.12*b*), one proceeds similarly, using

$$(3.13a)\qquad Y_1=\sum_P\sum_Q\psi(\alpha(Q))\tau(R(x^aP^c,Q))$$

and

$$(3.13b)\qquad Y_2=\sum_P\sum_Q\psi(\beta(Q))\tau(R(P^c,Q))$$

in place of (3.13).

PROOF OF THEOREMS 1.1, 1.1*a*, 1.1*b*.

To prove Theorem 1.1, it suffices to prove that $S_n(a,b,c)=P_n(a,b,c)$ under the assumption

$$b + jc \not\equiv 0 \pmod{q-1} \quad \text{for all} \quad j \quad \text{with} \quad 0 \leqslant j \leqslant n-1 ,$$

in view of [10, Lemmas 2.1 and 2.2]. Assume also that

$$c \not\equiv 0 \pmod{q-1} ,$$

since the result has been proved in [5] for $c \equiv 0 \pmod{q-1}$.

Theorem 1.1 is clear for $n = 1$, so let $n > 1$ and assume as induction hypothesis that

$$S_{n-1}(a+c, b+c, c) = P_{n-1}(a+c, b+c, c) .$$

By (3.8) and (3.12), if $d \nmid n$,

$$\begin{aligned} S_n(a,b,c) &= P_{n-1}(a+c, b+c, c) \frac{G(a)G(b)G(cn)\bar{G}(a+b+(n-1)c)}{qG(c)} \\ &= P_n(a,b,c) , \end{aligned}$$

whereas

$$S_n(a,b,c) + (q-1)P_n(a,b,c) = qP_n(a,b,c) , \quad \text{if} \quad d \mid n .$$

Thus $S_n(a,b,c) = P_n(a,b,c)$ in both cases, proving Theorem 1.1. The proofs of Theorems 1.1*a* and 1.1*b* follow similarly, from (3.8*a*), (3.12*a*) and (3.8*b*), (3.12*b*) in place of (3.8), (3.12).

REFERENCES

[1] ANDERSON, G. W. The evaluation of Selberg sums. *Comptes Rendus Acad. Sci. Paris 311,* Série I (1990), 469-472.

[2] ANDERSON, G. W. A short proof of Selberg's generalized beta formula. *Forum Math. 3* (1991), 415-417.

[3] ASKEY, R. Some basic hypergeometric extensions of integrals of Selberg and Andrews. *SIAM J. Math. Anal. 11* (1980), 938-951.

[4] ASKEY, R. and D. RICHARDS. Selberg's second beta integral and an integral of Mehta. In *Probability, Statistics, and Mathematics,* T. W. Anderson *et al.,* eds., pp. 27-39, Academic Press, Boston, MA, 1989.

[5] AUTUORE, J. and R. EVANS. Evaluations of Selberg character sums. In *Analytic Number Theory,* B. C. Berndt *et al.,* eds., pp. 13-21, Birkhäuser, Boston, MA, 1990.

[6] CELNIKER, N., S. POULOS, A. TERRAS, C. TRIMBLE and E. VELASQUEZ. Is there life on finite upper half planes? (To appear.)

[7] EVANS, R. Identities for products of Gauss sums over finite fields. *Enseignement Math. 27* (1981), 197-209.

[8] —— A character sum for root system G_2. *Proc. Amer. Math. Soc.,* (to appear).

[9] EVANS, R., J. PULHAM and J. SHEEHAN. On the number of complete subgraphs contained in certain graphs. *J. Combin. Theory (Series B) 30* (1981), 364-371.

[10] EVANS, R. and W. ROOT. Conjectures for Selberg character sums. *J. Ramanujan Math. Soc. 3 (1)* (1988), 111-128.

[11] GASPER, G. and M. RAHMAN. *Basic hypergeometric series.* Cambridge, NY, 1990.

[12] GREENE, J. and D. STANTON. A character sum evaluation and Gaussian hypergeometric series. *J. Number Theory 23* (1986), 136-148.

[13] KOBLITZ, N. The number of points on certain families of hypersurfaces over finite fields. *Compositio Math. 48* (1983), 3-23.

[14] KOIKE, M. Hypergeometric series over finite fields and Apery numbers. (To appear.)

(Reçu le 3 janvier 1991)

Ronald J. Evans

Department of Mathematics
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0112 (USA)