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: §3. Proof of Theorems 1.1, 1.1a, 1.1b
DOI: https://doi.org/10.5169/seals-58741

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

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

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

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

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

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

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

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

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

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

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*

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

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

and

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

Proof. We have

$$Y = \sum_P \sum_Q \tau(R(V, Q)) \ , \tag{3.13}$$

where

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

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),

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

and again (3.12) follows by (2.8).

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

$$Y_1 = \sum_P \sum_Q \psi(\alpha(Q)) \tau(R(x^a P^c, Q)) \tag{3.13a}$$

and

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

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).