PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 114, Number 3, MARCH 1992

A CHARACTER SUM FOR ROOT SYSTEM G_2

RONALD EVANS

(Communicated by William Adams)

ABSTRACT. A character sum analog of the Macdonald–Morris constant term identity for the root system G_2 is proved. The proof is based on recent evaluations of Selberg character sums and on a character sum analog of Dixon's summation formula. A conjectural evaluation is presented for a related sum.

1. INTRODUCTION

Let $GF(q)$ denote the finite field of q elements, where q is a power of an odd prime p. Throughout, A, B, and C denote multiplicative characters on $GF(q)$. Let 1 and ϕ denote the trivial and quadratic characters on $GF(q)$, respectively. Define $A(0) = 0$, even if $A = 1$. Let $\operatorname{ord} C$ denote the order of C (e.g., $\operatorname{ord}\phi = 2$).

Define the Gauss and Jacobi sums $G(A)$, $J(A, B)$ over $GF(q)$ by

$$(1.1) \qquad G(A) = \sum_m A(m)\zeta^{T(m)}, \qquad J(A, B) = \sum_m A(m)B(1-m),$$

where the sums are over all $m \in GF(q)$, $\zeta = \exp(2\pi i/p)$, and T denotes the trace map from $GF(q)$ to $GF(p)$. For nonnegative integers n, define the n-dimensional Selberg character sum $L_n(A, B, C\phi)$ over $GF(q)$ by

$$(1.2) \qquad L_n(A, B, C\phi) = \sum_{\substack{F \\ \deg F = n}} A((-1)^n F(0))B(F(1))C\phi(D_F),$$

where the sum is over all monic polynomials F over $GF(q)$ of degree n, and where D_F denotes the discriminant of F.

Define

$$(1.3) \qquad R_n(A, B, C) = \prod_{j=0}^{n-1} \frac{G(C^{j+1})G(AC^j)G(BC^j)}{G(C)G(ABC^{n-1+j})}$$

Received by the editors September 17, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11L05, 11T21; Secondary 17B20, 33A30.

and

$$S_n(A, B, C) = q^{-n} R_n(A, B, C) \prod_{j=0}^{n-1} |G(ABC^{n-1+j})|^2$$
$$(1.4) \qquad = q^{-n} G(C)^{-n} \prod_{j=0}^{n-1} G(C^{j+1}) G(AC^j) G(BC^j) \overline{G}(ABC^{n-1+j}).$$

The generic Selberg character sum formula in Theorem 1.1 was conjectured in [5, (2.6); 2, (29)]. A proof of Theorem 1.1, based on the method of Anderson [1], is given in [4].

Theorem 1.1. *If*

$$(1.5) \qquad ABC^{n-1+j} \text{ is nontrivial for all } j, \qquad 0 \le j \le n-1$$

or

$$(1.6) \qquad AC^a \text{ is nontrivial for all } a, \qquad 0 \le a \le n-1$$

or

$$(1.7) \qquad BC^b \text{ is nontrivial for all } b, \qquad 0 \le b \le n-1,$$

then

$$(1.8) \qquad L_n(A, B, C\phi) = S_n(A, B, C).$$

Using Theorem 1.1 we prove a character sum analog of the Macdonald-Morris constant term identity for the root system G_2 [9, p. 994; 10, p. 45]. This analog, given in Theorem 1.2, was inspired by a pretty paper of Zeilberger [11].

Theorem 1.2. *Let*

$$(1.9) \qquad L = \sum_{\substack{F(0)=-1 \\ \deg F = 3}} B^2(F(1)) C\phi(D_F),$$

where the sum is over all monic cubic polynomials F over $GF(q)$ with constant term -1. Then

$$(1.10) \qquad L = q^2 - 2q + 3, \quad \text{if } B^2 = 1, \ C = \phi,$$
$$(1.11) \qquad L = (2 - 4/q) G(\overline{C})^3, \quad \text{if } B^2 = 1, \ \operatorname{ord} C = 3,$$
$$(1.12) \qquad L = (1 - 3/q) G(\overline{C})^3, \quad \text{if } B^2 = C^2, \ \operatorname{ord} C = 3,$$

and

$$(1.13) \qquad L = P(B, C) + P(B\phi, C) \quad \text{otherwise},$$

where

$$(1.14) \qquad P(B, C) = \frac{G(C^2) G(C^3) G(B^2) G(\overline{B}^2 \overline{C}^3) G(\overline{BC}^2) G(B^3 C^3)}{G(B) G(BC) G(C)^2}.$$

Note the completely direct analogy between $P(B, C)$ and the product of gamma functions in the Macdonald-Morris identity for G_2. The form of the sum L in (1.9) is suggested by identifying the polynomial $F(W)$ in (1.9) with $(W - x/y)(W - y/z)(W - z/x)$, where x, y, z are the variables in the constant term identity for G_2 in [11, Theorem, p. 880]. The form of the sum L is not directly analogous to the trigonometric integral [10, p. 46] or the beta integral [6, (1.7)] associated with G_2.

We remark that if B^2 is replaced by a nonsquare character in (1.9), then the resulting sum vanishes. This follows from (2.1) below and [5, (2.2)].

Our proof of Theorem 1.2 employs the character sum analog of Dixon's summation formula [11, p. 881] given in Theorem 1.3. A proof of this analog (and more general results) can be found in [7]; we give a different proof in the Appendix.

Theorem 1.3. *Define*

$$\delta(A) = \begin{cases} 0, & \text{if } A \neq 1, \\ 1, & \text{if } A = 1. \end{cases} \tag{1.15}$$

Then for all characters D, E, F *on* $GF(q)$,

$$\begin{aligned}(q-1)^{-1}\sum_A G(AD)G(AE)G(AF)\overline{G}(A\overline{D})\overline{G}(A\overline{E})\overline{G}(A\overline{F}) \\ = (q-1)q^2\delta(D^2E^2F^2) + Q(D, E, F) + Q(D\phi, E\phi, F\phi),\end{aligned} \tag{1.16}$$

where

(1.17)

$$Q(D, E, F) = DEF(-1)G(DE)G(DF)G(EF)G(D)G(E)G(F)/G(DEF).$$

Our proof of Theorem 1.2 also requires the evaluations of the Selberg sums $L_3(\overline{C}^2, 1, C\phi)$ and $L_3(\overline{C}, \overline{C}, C\phi)$ given in Theorem 1.4. These two Selberg sums are not covered by Theorem 1.1, but they can be evaluated by a suitable modification of the proof of [4, Theorem 1.1]. We omit the details.

Theorem 1.4. *If* $C^2 \neq 1$, *then*

$$\frac{L_3(\overline{C}^2, 1, C\phi)}{R_3(\overline{C}^2, 1, C)} = \frac{L_3(\overline{C}, \overline{C}, C\phi)}{R_3(\overline{C}, \overline{C}, C)} = 2 - q. \tag{1.18}$$

Inspired by Theorem 1.2, Greg Anderson suggested that the sum

$$Y(B, C) := \sum_{x, y \in GF(q)} B(x^2 - 4y)C(y^2 + 18y + 12xy - 4x^3 - 27) \tag{1.19}$$

has an elegant product formula. Since the discriminant of the polynomial $F(z) = z^3 - rz^2 + sz - 1$ is $r^2s^2 + 18rs - 4s^3 - 4r^3 - 27$, one sees via the transformation $x = r + s$, $y = rs$ that

$$L = Y(B, C\phi) + Y(B\phi, C\phi). \tag{1.20}$$

Thus the following conjecture implies Theorem 1.2.

Conjecture 1.5. *We have*

$$Y(B\phi, C\phi) = q^2 - 2q + 2 = (q^2 - 2q + 2)P(B, C), \quad \text{if } B = C = \phi, \tag{1.21}$$

$$Y(B\phi, C\phi) = (1 - 2/q)G(\overline{C})^3 = (2 - q)qP(B, C), \quad \text{if } \operatorname{ord} C = 3,\ B \in \{1, \phi, C\}, \tag{1.22}$$

and

$$Y(B\phi, C\phi) = P(B, C), \quad \textit{otherwise.} \tag{1.23}$$

For character sum analogs of Macdonald-Morris constant term identities connected with various other root systems, see [3]. For most root systems (e.g., $F_4, E_6, E_7, E_8, \ldots$), no analogs are known.

2. Proof of Theorem 1.2

By (1.2) and (1.9),

$$L = \frac{1}{q-1} \sum_A L_3(A, B^2, C\phi). \tag{2.1}$$

Define

$$d(A, B, C) = L_3(A, B, C\phi) - S_3(A, B, C). \tag{2.2}$$

Then by (2.1) and Theorem 1.1,

$$L = T + \frac{1}{q-1} \sum_{A \in \{1, \overline{C}, \overline{C}^2\}} d(A, B^2, C), \tag{2.3}$$

where

$$T = \frac{1}{q-1} \sum_A S_3(A, B^2, C). \tag{2.4}$$

By (2.4) and (1.4),

$$\begin{aligned} T &= \frac{1}{q-1} \sum_A S_3(A\overline{BC}^2, B^2, C) \\ &= \frac{G(C)G(C^2)G(C^3)G(B^2)G(B^2C)G(B^2C^2)}{(q-1)q^3G(C)^3} \sum_A \prod_{j=0}^{2} G(A\overline{B}C^{j-2})\overline{G}(ABC^j). \end{aligned} \tag{2.5}$$

Apply Theorem 1.3 with

$$D = \overline{BC}^2, \qquad E = \overline{BC}, \qquad F = \overline{B} \tag{2.6}$$

to obtain, for all characters B, C,

$$\begin{aligned} T = {} & \frac{G(C^2)G(C^3)G(B^2)G(B^2C)G(B^2C^2)}{q^3G(C)^2} \\ & \cdot \{(q-1)q^2\delta(B^6C^6) + Q(\overline{BC}^2, \overline{BC}, \overline{B}) + Q(\overline{B}\phi\overline{C}^2, \overline{B}\phi\overline{C}, \overline{B}\phi)\}. \end{aligned} \tag{2.7}$$

By definition (1.17),

$$\begin{aligned} & Q(\overline{BC}^2, \overline{BC}, \overline{B}) \\ & \quad = BC(-1)G(\overline{B}^2\overline{C}^3)G(\overline{B}^2\overline{C}^2)G(\overline{B}^2\overline{C})G(\overline{BC}^2)G(\overline{BC})G(\overline{B})/G(\overline{B}^3\overline{C}^3). \end{aligned} \tag{2.8}$$

Define

$$W(B, C) = G(\overline{B}^2\overline{C}^3)G(\overline{B}^2\overline{C}^2)G(\overline{B}^2\overline{C})G(\overline{BC}^2)G(\overline{BC})G(\overline{B})G(B^3C^3)/q. \tag{2.9}$$

By (2.8) and (2.9),

$$W(B, C) = Q(\overline{BC}^2, \overline{BC}, \overline{B}), \quad \text{if } B^3C^3 \neq 1. \tag{2.10}$$

Assume first that

$$B^2, \ B^2C, \text{ and } B^2C^2 \text{ are nontrivial.} \tag{2.11}$$

By (2.11), if $B^3C^3 = 1$, then

$$W(B, C) = -q^2 \quad \text{and} \quad Q(\overline{BC}^2, \overline{BC}, \overline{B}) = -q^3. \tag{2.12}$$

Hence (2.10) has the extension

$$(q-1)q^2\delta(B^3C^3) + Q(\overline{BC}^2, \overline{BC}, \overline{B}) = W(B, C). \tag{2.13}$$

Since $\delta(B^6C^6) = \delta(B^3C^3) + \delta(\phi B^3C^3)$, the expression in braces in (2.7) equals

$$W(B, C) + W(B\phi, C). \tag{2.14}$$

Again using (2.11), we thus obtain

$$T = P(B, C) + P(B\phi, C). \tag{2.15}$$

By (2.11) and Theorem 1.1, each summand $d(\overline{C}^a, B^2, C)$ in (2.3) vanishes. Thus $L = T$ and the result follows from (2.15) under the assumption (2.11).

Now drop the assumption (2.11). For brevity, set

$$R(a, b) = R(\overline{C}^a, \overline{C}^b, C), \tag{2.16}$$

$$U(a, b) = L_3(\overline{C}^a, \overline{C}^b, C\phi)/R(a, b), \tag{2.17}$$

$$V(a, b) = S_3(\overline{C}^a, \overline{C}^b, C)/R(a, b), \tag{2.18}$$

where $0 \leq a, b \leq 2$. Observe that $R(a, b)$, $U(a, b)$, $V(a, b)$ are symmetric in a, b. We proceed to evaluate these functions.

From (1.3),

$$R(0, 0) = G^2(C^2)/G(C^4), \tag{2.19}$$

$$R(1, 0) = G(\overline{C})G(C^2)/G(C), \tag{2.20}$$

$$R(2, 0) = R(2, 2) = R(2, 1) = -|G(C^2)|^2 G(C^3)G(\overline{C})/G^2(C), \tag{2.21}$$

$$R(1, 1) = -G(C^3)G^2(\overline{C})/G(C). \tag{2.22}$$

From (1.4),

$$V(0, 0) = \begin{cases} q^{-3}, & \text{if } C = 1, \\ q^{-2}, & \text{if } C = \phi, \\ q^{-1}, & \text{if } \operatorname{ord} C = 3 \text{ or } 4, \\ 1, & \text{if } \operatorname{ord} C > 4, \end{cases} \tag{2.23}$$

$$V(1, 0) = \begin{cases} q^{-3}, & \text{if } C = 1, \\ q^{-1}, & \text{if } \operatorname{ord} C = 2 \text{ or } 3, \\ 1, & \text{if } \operatorname{ord} C > 3, \end{cases} \tag{2.24}$$

$$V(2,0)=V(2,2)=V(1,1)=\begin{cases} q^{-3}, & \text{if } C=1, \\ q^{-2}, & \text{if } C=\phi, \\ q^{-1}, & \text{if ord } C>2, \end{cases} \tag{2.25}$$

$$V(2,1)=\begin{cases} q^{-3}, & \text{if } C=1, \\ q^{-1}, & \text{if } C\neq 1. \end{cases} \tag{2.26}$$

By [5, Theorem 4.1],

$$U(0,0)=\begin{cases} 4-3q, & \text{if } C=1, \\ -q^3+3q^2-5q+4, & \text{if } C=\phi, \\ q^2-3q+3, & \text{if ord } C=3, \\ q^{-1}, & \text{if ord } C=4, \\ 1, & \text{if ord } C>4. \end{cases} \tag{2.27}$$

We claim that

$$U(1,0)=\begin{cases} 4-3q, & \text{if } C=1, \\ 2-q, & \text{if } C=\phi, \\ q^2-3q+3, & \text{if ord } C=3, \\ 1, & \text{if ord } C>3. \end{cases} \tag{2.28}$$

The cases $C=1$, $C=\phi$ of (2.28) follow from [5, (2.13), (2.14)]. The case where $\operatorname{ord} C=3$ follows from (2.27), since by [5, Lemmas 2.1, 2.2],

$$U(1,0)=U(0,0) \quad \text{if ord } C=3.$$

The last case where $\operatorname{ord} C>3$ follows from (2.24) and Conjecture 1.1 (note that the hypothesis (1.5) of Theorem 1.1 holds with $A=\overline{C}$, $B=1$). Next we claim that

$$U(2,0)=U(2,2)=\begin{cases} 4-3q, & \text{if } C=1, \\ -q^3+3q^2-5q+4, & \text{if } C=\phi, \\ 2-q, & \text{if ord } C>2. \end{cases} \tag{2.29}$$

The first equality in (2.29) follows from [5, Lemmas 2.1, 2.2]. The cases $C=1$, $C=\phi$ of (2.29) follow from [5, (2.13), (2.14)], while the remaining case follows from Theorem 1.4. The same argument shows that

$$U(1,1)=\begin{cases} 4-3q, & \text{if } C=1, \\ (2-q)/q, & \text{if } C=\phi, \\ 2-q, & \text{if ord } C>2. \end{cases} \tag{2.30}$$

Finally, we claim that

$$U(2,1)=\begin{cases} 4-3q, & \text{if } C=1, \\ 2-q, & \text{if } C\neq 1. \end{cases} \tag{2.31}$$

The cases $C=1$, $C=\phi$ of (2.31) follow from [5, (2.13), (2.14)], while the cases where $C^2\neq 1$ follow from (2.30), since

$$U(2,1)=U(1,1) \quad \text{if ord } C>2 \tag{2.32}$$

by [5, Lemmas 2.1, 2.2].

For $0 \le a, b \le 2$, set

$$d(a, b) = \{U(a, b) - V(a, b)\}R(a, b), \tag{2.33}$$

so that by (2.2),

$$d(a, b) = d(\overline{C}^a, \overline{C}^b, C). \tag{2.34}$$

From (2.19)–(2.31), we obtain the following evaluation of $d(a, b)$:

$$d(0, 0) = \begin{cases} -(4 - 3q - q^{-3}), & \text{if } C = 1, \\ -(-q^3 + 3q^2 - 5q + 4 - q^{-2}), & \text{if } C = \phi, \\ (q^2 - 3q + 3 - q^{-1})G^3(\overline{C})/q, & \text{if ord}\, C = 3, \\ 0, & \text{if ord}\, C > 3; \end{cases} \tag{2.35}$$

$$d(1, 0) = \begin{cases} -(4 - 3q - q^{-3}), & \text{if } C = 1, \\ -(2 - q - q^{-1}), & \text{if } C = \phi, \\ (q^2 - 3q + 3 - q^{-1})G^3(\overline{C})/q, & \text{if ord}\, C = 3, \\ 0, & \text{if ord}\, C > 3; \end{cases} \tag{2.36}$$

$$d(2, 0) = d(2, 2) = \begin{cases} -(4 - 3q - q^{-3}), & \text{if } C = 1, \\ -(-q^3 + 3q^2 - 5q + 4 - q^{-2}), & \text{if } C = \phi, \\ -(2 - q - q^{-1})G(C^3)G^3(\overline{C})/q, & \text{if ord}\, C > 2; \end{cases} \tag{2.37}$$

$$d(1, 1) = \begin{cases} -(4 - 3q - q^{-3}), & \text{if } C = 1, \\ -(2 - q - q^{-1})\phi(-1), & \text{if } C = \phi, \\ -(2 - q - q^{-1})G(C^3)G^3(\overline{C})C(-1)/q, & \text{if ord}\, C > 2; \end{cases} \tag{2.38}$$

and

$$d(2, 1) = \begin{cases} -(4 - 3q - q^{-3}), & \text{if } C = 1, \\ -(2 - q - q^{-1}), & \text{if } C = \phi, \\ -(2 - q - q^{-1})G(C^3)G^3(\overline{C})/q, & \text{if ord}\, C > 2. \end{cases} \tag{2.39}$$

We now evaluate L from (2.3), using (2.7), (2.8), and (2.35)–(2.39), and Theorem 1.2 follows.

3. Appendix

Here we give a proof of Theorem 1.3. Let H denote the left side of (1.16). First suppose that $DE = 1$. Then

$$\begin{aligned} H &= \frac{1}{q-1} \sum_A |G(AE)|^2 |G(A\overline{E})|^2 G(AF)\overline{G}(A\overline{F}) \\ &= \begin{cases} M - (q+1)G(EF)\overline{G}(E\overline{F}), & \text{if } E^2 = 1, \\ M - qG(\overline{E}F)\overline{G}(\overline{EF}) - qG(EF)\overline{G}(E\overline{F}), & \text{if } E^2 \ne 1, \end{cases} \end{aligned} \tag{3.1}$$

where

$$M = \frac{q^2}{q-1} \sum_A G(AF)\overline{G}(A\overline{F}). \tag{3.2}$$

By (1.1),

$$M = \frac{q^2}{q-1} \sum_t \sum_u \sum_A AF(t)\overline{A}F(u)\zeta^{T(t-u)} = q^2(q-1)\delta(F^2). \tag{3.3}$$

Using (3.3) in (3.1), we easily deduce (1.16) in the case $DE = 1$.

By symmetry, it remains to prove (1.16) in the case

$$DE \neq 1, \qquad DF \neq 1, \qquad EF \neq 1. \tag{3.4}$$

By (1.1),

(3.5)

$$\begin{aligned} H &= \frac{1}{q-1} \sum_{t,u,v} \sum_{x,y,z\neq 0} \sum_A A\left(\frac{tuv}{xyz}\right) D(tx)E(uy)F(vz)\zeta^{T(t+u+v-x-y-z)} \\ &= \frac{1}{q-1} \sum_{t,u,v} \sum_{x,y,z} \sum_A A(tuv)D(txy)E(uyz)F(vzx)\zeta^{T(y(t-1)+z(u-1)+x(v-1))}, \end{aligned}$$

where the last equality results from replacing t by ty, u by uz, and v by vx. By (3.4), it follows that

$$\begin{aligned} H = &\frac{1}{q-1} G(DE)G(DF)G(EF) \\ &\times \sum_{t,u,v} \sum_A A(tuv)\overline{DE}(1-t)\overline{EF}(1-u)\overline{DF}(1-v)D(t)E(u)F(v). \end{aligned} \tag{3.6}$$

Thus,

(3.7)

$$\begin{aligned} &H/\{G(DE)G(DF)G(EF)\} \\ &\quad = \sum_{t,v\neq 0} \overline{DE}(1-t)\overline{EF}(1-1/(tv))\overline{DF}(1-v)D(t)\overline{E}(tv)F(v) \\ &\quad = \sum_{t,v\neq 0} \overline{DE}(1-t/v)\overline{EF}(1-1/t)\overline{DF}(1-v)D(t/v)\overline{E}(t)F(v) \\ &\quad = \sum_{t,v} EF(v)DF(t)\overline{EF}(t-1)\overline{DF}(1-v)\overline{DE}(v-t) \\ &\quad = EF(-1) \sum_{t,v\neq 0} \overline{DF}\left(\frac{1+v}{t}\right)\overline{EF}\left(\frac{1+t}{v}\right)\overline{DE}(v-t) \\ &\quad = EF(-1)\{J(\overline{DEF}, DE)J(E, \overline{DE}) + J(\overline{DEF}\phi, DE)J(E\phi, \overline{DE})\}, \end{aligned}$$

where the last equality follows from [2, (28)]. Since $DE \neq 1$, we can apply the formula [8]

$$J(A, B) = G(A)G(\overline{AB})A(-1)/G(\overline{B}), \quad \text{if } B \neq 1 \tag{3.8}$$

to express all of the Jacobi sums in (3.7) in terms of Gauss sums. Then (1.16) readily follows.

Acknowledgments

We are grateful for helpful comments from Dave Bressoud, John Greene, and especially Greg Anderson.

REFERENCES

1. G. W. Anderson, *The evaluation of Selberg sums*, C. R. Acad. Sci. Paris Sér. I Math. **311** (1990), 469–472.
2. R. J. Evans, *Identities for products of Gauss sums over finite fields*, Enseign. Math. (2) **27** (1981), 197–209.
3. ——, *Character sum analogues of constant term identities for root systems*, Israel J. Math. **46** (1983), 189–196.
4. ——, *The evaluation of Selberg character sums*, Enseign. Math. (to appear).
5. R. J. Evans and W. A. Root, *Conjectures for Selberg character sums*, J. Ramanujan Math. Soc. **3** (1988), 111–128.
6. F. G. Garvan, *A beta integral associated with the root system* G_2, SIAM J. Math. Anal. **19** (1988), 1462–1474.
7. J. Greene, *The Bailey transform over finite fields* (to appear).
8. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Math., vol. **84**, Springer-Verlag, New York, 1982.
9. I. G. Macdonald, *Some conjectures for root systems*, SIAM J. Math. Anal. **13** (1982), 988–1007.
10. W. G. Morris, *Constant term identities for finite and affine root systems*, Ph.D. thesis, Univ. of Wisconsin, Madison, 1982.
11. D. Zeilberger, *A proof of the* G_2 *case of Macdonald's root system—Dyson conjecture*, SIAM J. Math. Anal. **18** (1987), 880–883.

DEPARTMENT OF MATHEMATICS 0112, UNIVERSITY OF CALIFORNIA AT SAN DIEGO, LA JOLLA, CALIFORNIA 92093