

Pacific Journal of Mathematics

SOME AVERAGES OF CHARACTER SUMS

HERBERT WALUM

SOME AVERAGES OF CHARACTER SUMS

H. WALUM

Let χ and ψ be nonprincipal characters mod p . Let f be a polynomial mod p and let a_1, \dots, a_p be complex constants. We will assume $a_j = a_k$ for $j \equiv k(p)$, and thus have a_n defined for all n . Define

$$(1) \quad S = \sum_r a_r \chi(f(r))$$

and

$$(2) \quad J_n(c) = \sum_r \psi(r) \chi(r^n - c),$$

where the variables of summation run through a complete system of residues mod p .

The averages in question are

$$(3) \quad A_1 = \sum_{a=1}^{p-1} |J_n(a)|^2$$

and

$$(4) \quad A_2 = \Sigma |S|^2,$$

where the sum in (4) is over the coefficients mod p of certain fixed powers of the variables in f . Exact formulae for A_1 will be obtained in all cases, and for A_2 in an extensive class of cases.

Specifically, the following theorems are true.

THEOREM I. *Let $f(r) = yr^{m_1} + xr^{m_2} + g(r)$ and assume $(m_2 - m_1, p - 1) = 1$. Let the sum in (4) be over all x and y mod p . If g has a nonzero constant term and neither m_1 nor m_2 is zero, then*

$$(5) \quad A_2 = p(p - 1) \sum_{r=1}^{p-1} |a_r|^2 + p^2 |a_0|^2.$$

Otherwise,

$$(6) \quad A_2 = p(p - 1) \sum_{r=1}^{p-1} |a_r|^2.$$

THEOREM II. *Let $d = (n, p - 1)$, $\psi(t) = e^{2\pi i (r \text{ ind } (t)/s)}$, where, naturally, $s | (p - 1)$, $(r, s) = 1$ and $g^{\text{ind } (t)} \equiv t(p)$ for g a primitive root mod p . If $ds \nmid (p - 1)$, then $A_1 = 0$. If $ds | (p - 1)$ and $\psi \chi^n$ is nonprincipal, then $A_1 = p(p - 1)d$. If $ds | (p - 1)$ and $\psi \chi^n$ is principal, then $A_1 = p(p - 1)(d - 1) - (p - 1)$.*

The following is an immediate consequence of the first theorem.

Received November 21, 1963 and in revised form June 16, 1964. Research done under the auspices of the National Science Foundation.

THEOREM III. *Let f be as in Theorem I, and assume $|\alpha_r| = 1$, $r = 1, \dots, p$. Then there exist x_0, y_0, x_1 and y_1 depending on χ , such that the S , as in (1), for x_0 and y_0 satisfies $|S| < \sqrt{p}$ and the S , for x_1 and y_1 , satisfies $\sqrt{(p-2)} < |S|$.*

Proof of Theorem II. Our principal device is the fact that a function which is periodic mod p has a unique expansion by means of the characters mod p [2]. That is if $h(r) = h(s)$ for $r \equiv s(p)$, then for $n \not\equiv 0(p)$

$$(7) \quad h(n) = \sum_{\theta} b_{\theta} \theta(n),$$

where θ runs through the characters mod p . b_{θ} is given by

$$(8) \quad (p-1)b_{\theta} = \sum_r h(r) \bar{\theta}(r).$$

Regarding $J_n(c)$ as a periodic function mod p of c , and expanding $J_n(c)$ in the form (7), we obtain, by standard methods,

$$(9) \quad J_n(c) = \sum_{\rho^n = \psi \chi^n} \pi(\bar{\rho}, \chi) \rho(c)$$

where $\pi(\alpha, \beta)$ is a Jacobi sum [1]

$$(10) \quad \pi(\alpha, \beta) = \sum_r \alpha(r) \beta(1-r).$$

The sum in (9) is over all characters ρ which satisfy the indicated condition.

The expansion (7) has a Parseval identity

$$(11) \quad \sum_{t=1}^{p-1} |h(t)|^2 = (p-1) \sum_{\theta} |\alpha_{\theta}|^2.$$

Thus we can evaluate A_1 by means of (11) and (9) when we know the value of $|\pi(\alpha, \beta)|^2$. Now [1] $|\pi(\alpha, \beta)|^2 = p$ when $\alpha \neq \varepsilon$, $\beta \neq \varepsilon$ and $\alpha\beta \neq \varepsilon$, where ε is the principal character. If $\alpha = \varepsilon$ or $\beta = \varepsilon$, then $|\pi(\alpha, \beta)|^2 = 1$. If $\alpha\beta = \varepsilon$ with $\alpha \neq \varepsilon$ or $\beta \neq \varepsilon$, then $|\pi(\alpha, \beta)|^2 = p$. By hypothesis, χ is nonprincipal. Thus $|\pi(\bar{\rho}, \chi)|^2$ is p unless $\bar{\rho} = \varepsilon$ or $\bar{\rho}\chi = \varepsilon$. If $\bar{\rho} = \varepsilon$, then $\bar{\rho} = \varepsilon$ and $\psi\chi^n$ is principal. If $\bar{\rho}\chi = \varepsilon$, then $\rho = \chi$ and $\rho^n = \psi\chi^n$ implies $\psi = \varepsilon$ which is excluded by hypothesis. Let N be the number of solutions of $\rho^n = \psi\chi^n$. If $\psi\chi^n$ is nonprincipal then $|\pi(\bar{\rho}, \chi)|^2 = p$ for all N of the ρ and $A_1 = p(p-1)N$. If $\psi\chi^n$ is principal, then $|\pi(\bar{\rho}, \chi)|^2 = p$ for $N-1$ of the ρ and $|\pi(\bar{\rho}, \chi)|^2 = 1$ for $\rho = \varepsilon$. Thus, in this case, $A_1 = (p-1)(p(N-1) + 1) = Np(p-1)^2$.

N , the number of solutions of $\rho^n = \psi\chi^n$, is the number of solutions of $s^n = \psi$. It is a standard lemma from the theory of cyclic groups of order k that $a^n = b$ has (n, k) or 0 solutions according to whether

or not order $b \mid k/(n, k)$. Also, N is the number of solutions of $x^n = \psi(g)$, for x , in $(p - 1) - st$ roots of unity. From either description of N , it follows that $N = d$ or $N = 0$ according as $ds \mid (p - 1)$ or $ds \nmid (p - 1)$, and the theorem follows.

Proof of Theorem I. Referring to the hypotheses of Theorem I,

$$|S|^2 = \sum_{r,s} a_r \bar{a}_s \chi(yr^{m_1} + xr^{m_2} + g(r)) \bar{\chi}(ys^{m_1} + xs^{m_2} + g(s))$$

and thus,

$$(12) \quad A_2 = \sum a_r \bar{a}_s \sum \chi(yr^{m_1} + xr^{m_2} + g(r)) \chi(ys^{m_1} + xs^{m_2} + g(s)) = T_1 + T_2.$$

T_1 is the sum of the terms in (12) such that $r \not\equiv 0$ and $s \not\equiv 0$. T_2 is the sum of the terms in (12) such that $r \equiv 0$ or $s \equiv 0$. T_1 can be written

$$(13) \quad T_1 = \sum_{r \not\equiv 0, s} a_r \bar{a}_s \chi^{m_1}(r/s) A(r^{m_2-m_1}, r^{-m_1}g(r); s^{m_2-m_1}, s^{-m_1}g(s))$$

where

$$A(a, b; c, d) = \sum_{y+cx+d \not\equiv 0} \chi\left(\frac{y+ax+b}{y+cx+d}\right).$$

Now,

$$A(a, b; c, d) = \sum_x \sum_{y \not\equiv 0} \chi\left(\frac{y+x(a-c)+(b-d)}{y}\right).$$

Except when $(a-c)x + (b-d) \equiv 0(p)$,

$$\sum_{y \not\equiv 0} \chi\left(\frac{y+(a-c)x+(b-d)}{y}\right) = -1.$$

Also, $(a-c)x + (b-d) \equiv 0(p)$ when $x \equiv ((b-d)/(a-c))(p)$ or when $a \equiv c$ and $b \equiv d$. Thus, if $a \not\equiv c$ or $b \not\equiv d$, then

$$A(a, b; c, d) = -(p-1) + p - 1 = 0.$$

If $a \equiv c$ and $b \equiv d$, then

$$A(a, b; c, d) = p(p-1).$$

In view of this (13) becomes the sum over all r and s such that $r \not\equiv 0 \not\equiv s$ and $r^{m_2-m_1} = s^{m_2-m_1}$, $r^{-m_1}g(r) = s^{-m_1}g(s)$. Since $(m_2 - m_1, p - 1) = 1$, we have $r \equiv s$. Thus the sum in (13) is over those r and s such that $r \not\equiv 0 \not\equiv s$ and $r \equiv s$. Thus

$$T_1 = p(p-1) \sum_{r=1}^{p-1} |a_r|^2.$$

Now

$$\begin{aligned}
 (14) \quad T_2 &= \sum_{r \neq 0} a_r \bar{a}_0 \sum_{x,y} \chi(yr^{m_1} + xr^{m_2} + g(r)) \bar{\chi}(g(0)) \\
 &\quad + \sum_{s \neq 0} a_0 \bar{a}_s \sum_{x,y} \chi(g(0)) \bar{\chi}(ys^{m_1} + xs^{m_2} + g(s)) \\
 &\quad + |a_0|^2 \sum_{x,y} \chi(g(0)) \bar{\chi}(g(0)) = p^2 |a_0|^2 |\chi(g(0))|^2,
 \end{aligned}$$

except when $m_1 = 0$ or $m_2 = 0$.

Thus, if $g(0) \equiv 0$,

$$A_2 = p(p-1) \sum_{r \neq 0} |a_r|^2$$

and if $g(0) \not\equiv 0$, then

$$A_2 = p(p-1) \sum_{r \neq 0} |a_r|^2 + p^2 |a_0|^2,$$

when $m_1 = 0$ or $m_2 = 0$, then $\chi(g(0))$ in (14) must be changed to $\chi(y + g(0))$ or $\chi(x + g(0))$, and A_2 is given by (6).

REFERENCES

1. H. Davenport, and H. Hasse, *Die Nullstellen der Kongruenzetafunktionen in gewissen zyklischen Fallen*, Journal für Math. (Crelle) **172** (1934), S. 151-182.
2. M. J. Delsarte, *Essai sur l'application de la theorie des fonctions periodiques a l'arithmetique*, Annales Scientifiques L'Ecole Normale Superieure, series 3, **62** (1945), 185-204.

OHIO STATE UNIVERSITY

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. SAMELSON

Stanford University
Stanford, California

R. M. BLUMENTHAL

University of Washington
Seattle, Washington 98105

*J. DUGUNDJI

University of Southern California
Los Angeles, California 90007

RICHARD ARENS

University of California
Los Angeles, California 90024

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON

* * *

AMERICAN MATHEMATICAL SOCIETY
CHEVRON RESEARCH CORPORATION
TRW SYSTEMS
NAVAL ORDNANCE TEST STATION

Larry Armijo, <i>Minimization of functions having Lipschitz continuous first partial derivatives</i>	1
Edward Martin Bolger and William Leonard Harkness, <i>Some characterizations of exponential-type distributions</i>	5
James Russell Brown, <i>Approximation theorems for Markov operators</i>	13
Doyle Otis Cutler, <i>Quasi-isomorphism for infinite Abelian p-groups</i>	25
Charles M. Glennie, <i>Some identities valid in special Jordan algebras but not valid in all Jordan algebras</i>	47
Thomas William Hungerford, <i>A description of $\text{Mult}_i(A^1, \dots, A^n)$ by generators and relations</i>	61
James Henry Jordan, <i>The distribution of cubic and quintic non-residues</i>	77
Junius Colby Kegley, <i>Convexity with respect to Euler-Lagrange differential operators</i>	87
Tilla Weinstein, <i>On the determination of conformal imbedding</i>	113
Paul Jacob Koosis, <i>On the spectral analysis of bounded functions</i>	121
Jean-Pierre Kahane, <i>On the construction of certain bounded continuous functions</i>	129
V. V. Menon, <i>A theorem on partitions of mass-distribution</i>	133
Ronald C. Mullin, <i>The enumeration of Hamiltonian polygons in triangular maps</i>	139
Eugene Elliot Robkin and F. A. Valentine, <i>Families of parallels associated with sets</i>	147
Melvin Rosenfeld, <i>Commutative F-algebras</i>	159
A. Seidenberg, <i>Derivations and integral closure</i>	167
S. Verblunsky, <i>On the stability of the set of exponents of a Cauchy exponential series</i>	175
Herbert Walum, <i>Some averages of character sums</i>	189