EXPONENTIAL SUMS RELATED TO POLYNOMIALS OVER THE GF(p)

STEPHAN R. CAVIOR¹

1. Let k denote the finite field GF(p), and let $f(x) = a_r x^r + \dots + a_0$ be a polynomial function over k . We define

$$(1) \quad M(f) = \sum_{a \pmod{p}} e^{2\pi i/p \cdot f(a)},$$

where p is an odd prime.

Some years ago L. Carlitz and S. Uchiyama [1, pp. 37-39] proved that

$$(2) \quad |M(f)| \leq (r-1) \cdot p^{1/2}.$$

This result has raised some questions about the distribution of values of the M -function, and in particular, the question whether $M(f)$ can equal an integral multiple of $p^{1/2}$. The object of this paper is to determine which polynomial functions satisfy the equality

$$(3) \quad |M(f)| = p^{1/2}.$$

2. First we prove

THEOREM 1. *Let $R(\zeta)$ denote the cyclotomic field generated by $\zeta = e^{2\pi i/p}$, where p is an odd prime, and let α be an integer in $R(\zeta)$. Then*

$$(4) \quad |\alpha| = p^{1/2}$$

if and only if

$$(5) \quad \alpha = \pm \zeta^s \cdot \sum_{r \pmod{p}} \zeta^{r^2} \quad (0 \leq s \leq p-1).$$

By a well-known property of the Gauss sum, it is obvious that (4) holds if (5) holds.

To prove the converse, we first suppose that α, β are integers in $R(\zeta)$ such that

$$(6) \quad |\alpha| = |\beta| = p^{1/2}.$$

Then

$$(7) \quad \alpha \cdot \bar{\alpha} = p, \quad \beta \cdot \bar{\beta} = p,$$

Received by the editors January 3, 1963.

¹ Supported by National Science Foundation grant G16485.

and since $(1-\zeta)$ is a prime ideal of $R(\zeta)$ such that $(p) = (1-\zeta)^{p-1}$, (4) implies

$$(8) \quad \begin{aligned} (\alpha \cdot \bar{\alpha}) &= (\alpha)^2 = (1-\zeta)^{p-1}, \\ (\beta \cdot \bar{\beta}) &= (\beta)^2 = (1-\zeta)^{p-1}. \end{aligned}$$

Consequently

$$(9) \quad \alpha = \epsilon(1-\zeta)^{(p-1)/2}, \quad \beta = \epsilon'(1-\zeta)^{(p-1)/2},$$

where ϵ, ϵ' are units. We note immediately that

$$(10) \quad \eta = \frac{\alpha'}{\alpha}$$

is a unit, and we note by (6) that $|\eta| = 1$.

Since η is a unit, it satisfies some polynomial $h(x)$ with integer coefficients, and since $|\eta| = 1$, we have

$$(11) \quad \eta \cdot \bar{\eta} = 1.$$

If we set

$$(12) \quad \eta^{(i)} = T^{(i)}(\eta) \quad (1 \leq i \leq p-1),$$

where $T^{(i)}$ is the automorphism of $R(\zeta)$ defined by

$$(13) \quad T^{(i)}: \zeta \rightarrow \zeta^i \quad (1 \leq i \leq p-1),$$

it is clear from Galois theory that

$$(14) \quad \eta^{(i)} \cdot \bar{\eta}^{(i)} = 1 \quad (1 \leq i \leq p-1).$$

Since (12) comprises all the roots of $h(x)$, we see from (14) that the conjugates of η are unimodular. Therefore we know [2, Theorem 910, p. 223] that η must be a root of unity; i.e.,

$$(15) \quad \eta = \pm \zeta^s \quad (0 \leq s \leq p-1).$$

We have already noted that

$$(16) \quad \left| \sum_{r \pmod{p}} \zeta^{r^2} \right| = p^{1/2}.$$

Therefore, if $\alpha \in R(\zeta)$ and $|\alpha| = p^{1/2}$, we conclude that

$$(17) \quad \alpha = \pm \zeta^s \cdot \sum_{r \pmod{p}} \zeta^{r^2} \quad (0 \leq s \leq p-1).$$

This completes the proof of the theorem.

3. We now prove

THEOREM 2. *The total number T of polynomial functions f over k such that $|M(f)| = p^{1/2}$ is given by*

$$(18) \quad T = \frac{2p \cdot p!}{2^{(p-1)/2}}.$$

Suppose f is a polynomial function such that

$$(19) \quad M(f) = \sum_{r \pmod{p}} \zeta^{r^2}.$$

Using the identity

$$\sum_{r \pmod{p}} \zeta^{r^2} = 1 + 2 \cdot \sum_{\chi(a)=1} \zeta^a,$$

we note that by putting

$$\sum_{r \pmod{p}} \zeta^{r^2} = a_0 + a_1 \zeta + \cdots + a_{p-1} \zeta^{p-1},$$

we have

$$\begin{aligned} a_0 &= 1, \\ a_i &= \begin{cases} 2 & (\chi(i) = 1), \\ 0 & (\text{otherwise}), \end{cases} \quad (1 \leq i \leq p-1). \end{aligned}$$

Therefore if a is a fixed number in k such that $\chi(a) = 1$, there are precisely two numbers b_0, b_1 in k such that $f(b_0) = f(b_1) = a$; furthermore, there is a unique number c in k such that $f(c) = 0$. This last statement is in fact a necessary and sufficient condition for a function f to satisfy (19), so the number of such functions is

$$(20) \quad \binom{p}{2} \binom{p-2}{2} \cdots \binom{3}{2} = \frac{p!}{2^{(p-1)/2}},$$

where the symbols in (20) are binomial coefficients.

Suppose now that g is a function such that

$$(21) \quad M(g) = \pm \zeta^s \cdot \sum_{r \pmod{p}} \zeta^{r^2} \quad (1 \leq s \leq p-1).$$

Since the field $R(\zeta)$ must have an automorphism which maps the right member of (19) onto its negative, it is obvious that we can rewrite (21) in the form

$$(22) \quad M(g) = \sum_{r \pmod{p}} \zeta^{m(r)},$$

where $m(r)$ is a quadratic polynomial in r . Using the properties of a quadratic polynomial over k and the earlier combinatorial argu-

ments, we find that the number of functions g that satisfy (21) is also given by (20). Finally, since there are $2p$ sums in (5), we conclude that

$$T = \frac{2p \cdot p!}{2^{(p-1)/2}}.$$

This completes the proof of the theorem.

REFERENCES

1. L. Carlitz and S. Uchiyama, *Bounds for exponential sums*, Duke Math. J. **24** (1957), 37-41.
2. E. Landau, *Vorlesungen über Zahlentheorie*, Vol. 3, S. Hirzel, Leipzig, 1927.

STATE UNIVERSITY OF NEW YORK, BUFFALO