ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 3, Number 1, Winter 1973

ON THE REPRESENTATION OF POLYNOMIALS OVER FINITE FIELDS AS SUMS OF POWERS AND IRREDUCIBLES

WILLIAM A. WEBB

I. **Introduction.** There are a number of results known concerning the expression of an integer as the sum of a certain number of primes and kth powers [2], [3], [4]. In this paper, we prove several of these results, specifically those found in [4], for polynomial rings over finite fields.

A Hardy-Littlewood like method is used. The use of the Riemann hypothesis simplifies the proofs and enables us to obtain better error terms than those obtained in [4].

II. **Notation and preliminary results.** In general we follow the notation used in [5] and [6].

$GF[q, x]$ is the ring of polynomials over the finite field with q elements, $q = p^\beta$, p a prime.

$\mathcal{K}_{1/x}$ is the completion of the field of rational functions over $GF(q)$, with respect to ν, the degree valuation.

$\mathcal{P}_j = \{t \in \mathcal{K}_{1/x} : \nu(t) > j\}$.

$\mathcal{P}_0 = \mathcal{P}$.

$E(a) = \lambda(\alpha)$ where λ is a fixed nonprincipal character on $GF(q)$ and α is the coefficient of $1/x$ in a, where $a \in \mathcal{K}_{1/x}$.

$\int dp$ is the Haar integral on $\mathcal{P}$.

All capital letters represent elements of $GF[q, x]$.

$\deg K = \deg P_i = nk$ $(k \geqq 2)$.

$\deg A_i = n$.

P_i and A_i are primary, that is, have leading coefficient 1.

P_i are irreducible.

$\delta_i \in GF(q)$ are such that $\sum \delta_i = \operatorname{sgn} K =$ leading coefficient of K.

$\sum'$ denotes a sum over primary polynomials.

$f(t) = \sum'_{\deg P = nk} E(Pt)$.

$g(t) = \sum'_{\deg A = n} E(A^k t)$.

The main theorem we prove is

THEOREM 1. *If $p > k$, and $N_1(K)$ is the number of representations of K in the form*

Received by the editors February 20, 1970 and, in revised form, May 10, 1971.
AMS (MOS) subject classifications (1970). Primary 10J10, 10J15, 12C05; Secondary 10B35, 10J05.

$$K = \delta_1 P_1 + \delta_2 P_2 + \delta_3 A^k \tag{1}$$

then $N_1(K) = \mathfrak{S}_1\, q^{(k+1)n}/(nk)^2 + O(q^{(k+1-1/2^k)n})$ *where* $\mathfrak{S}_1 = c > 0$ *is defined by* (11).

III. **Proof of the main theorem.** Just as in the usual Hardy-Littlewood method $N_1(K) = \int_{\mathcal{P}} f(\delta_1 t) f(\delta_2 t) g(\delta_3 t) E(-Kt)\, d\rho$.

We must divide $\mathcal{P}$ in major and minor arcs. We use a primordial subdivision of $\mathcal{P}$ with respect to $2(k-1)n$. G/H is primordial if $\deg G < \deg H \leqq (k-1)n$, $(G, H) = 1$, and H is primary. $\mathcal{U}_{G/H} = \{t \in \mathcal{P} : \nu(t - G/H) > h + (k-1)n\}$.

The set of all such $\mathcal{U}_{G/H}$ is the primordial subdivision. For a more complete discussion, see [5].

The major arcs M are all those $\mathcal{U}_{G/H}$ with $\deg H < n$. The minor arcs $\mathcal{M}$ are all those $\mathcal{U}_{G/H}$ with $\deg H \geqq n$.

Now

$$\begin{aligned} N_1(K) &= \int_M f(\delta_1 t) f(\delta_2 t) g(\delta_3 t) E(-Kt)\, d\rho \\ &\quad + \int_{\mathcal{M}} f(\delta_1 t) f(\delta_2 t) g(\delta_3 t) E(-Kt)\, d\rho \\ &= T_1 + T_2. \end{aligned} \tag{2}$$

We first estimate the integral over the minor arcs. By Lemma 5 of [6], if $t \in \mathcal{M}$,

$$|g(t)| = O(q^{\,n(1-1/2^{k-1}+\epsilon)}) \tag{3}$$

for any $\epsilon > 0$. Thus

$$\begin{aligned} |T_2| &= \left| \int_{\mathcal{M}} f(\delta_1 t) f(\delta_2 t) g(\delta_3 t) E(-Kt)\, d\rho \right| \\ &= O\left(|g(\delta_3 t)| \int_{\mathcal{M}} |f(\delta_1 t) f(\delta_2 t)|\, d\rho \right) \\ &= O\left(q^{n(1-1/2^k)} \int_{\mathcal{P}} |f(\delta_1 t) f(\delta_2 t)|\, d\rho \right) \quad \text{for } \epsilon < 1/2^k \\ &= O\left(q^{n(1-1/2^k)} \left(\int_{\mathcal{P}} |f(\delta_1 t)|^2\, d\rho \right)^{1/2} \left(\int_{\mathcal{P}} |f(\delta_2 t)|^2\, d\rho \right)^{1/2} \right) \\ &= O\left(q^{n(1-1/2^k)} \left(\int_{\mathcal{P}} \sum_{P_1, P_2}{}' E(\delta(P_1 - P_2)t)\, d\rho \right) \right) \\ &= O(q^{n(1-1/2^k)} \pi(kn)) \end{aligned}$$

since

$$\int E(\delta(P_1 - P_2)t)\,d\rho = \begin{cases} 1 & \text{if } P_1 = P_2, \\ 0 & \text{otherwise.} \end{cases}$$

$\pi(r) =$ number of primary irreducibles of degree r. Trivially $\pi(r) \leqq q^r$. Thus

$$|T_2| = O(q^{(k+1-1/2^k)n}). \tag{4}$$

Next, we estimate the integral over the major arcs. Hence, we hereafter assume $\deg H < n$, $t \in \mathcal{U}_{G/H}$ so $t = G/H + y$ where $\nu(y) > h + (k-1)n$. By equation (12) of [**6**],

$$g(\delta t) = \begin{cases} 0 & \text{if } \nu(y) \leqq kn, \\ q^{n-h}E(x^{nk}\delta y)S(\delta G, H) & \text{if } \nu(y) > kn, \end{cases}$$

where $S(G, H) = \sum_{\deg R<h} E(R^k G/H)$. Thus

$$\begin{aligned} T_1 &= \sum_{\substack{G/H \text{ primordial} \\ \deg H<n}} \int_{\mathcal{U}_{G/H}} f(\delta_1 t)f(\delta_2 t)g(\delta_3 t)E(-Kt)\,d\rho \\ &= \sum_{\substack{G/H \text{ primordial} \\ \deg H<n}} q^{n-h}S(\delta_3 G, H)E(-KG/H) \\ &\quad \cdot \int_{\{y\,:\,\nu(y)>kn\}} f(\delta_1(G/H+y))f(\delta_2(G/H+y))\,E(\delta_3 x^{nk}y)E(-Ky)\,d\rho \\ &= \sum_{\substack{G/H \text{ primordial} \\ \deg H<n}} q^{n-h}S(\delta_3 G, H)E(-KG/H) \\ &\quad \cdot \sum_{P_1}{}' \sum_{P_2}{}' E((\delta_1 P_1 + \delta_2 P_2)G/H) \\ &\qquad\qquad \cdot \int_{\{y:\nu(y)>kn\}} E((\delta_1 x^{nk} + \delta_2 x^{nk} + \delta_3 x^{nk} - K)y)\,d\rho. \end{aligned}$$

But since $\nu((\delta_1 x^{nk} + \delta_2 x^{nk} + \delta_3 x^{nk} - K)y) > -nk + 1 + nk = 1$, the integral is just q^{-kn}. Thus

$$\begin{aligned} T_1 = &\sum_{\substack{G/H \text{ primordial} \\ \deg H<n}} q^{n-kn-h}S(\delta_3 G, H)E(-KG/H) \\ &\cdot \sum_{P}{}' E(\delta_1 PG/H) \sum_{P}{}' E(\delta_2 PG/H) \end{aligned} \tag{5}$$

where again P represents a primary, irreducible polynomial of degree nk.

Now

$$\sum_P{}' E(\delta PG/H) = \sum_{\deg L<\deg H;\ (L,H)=1} E(\delta LG/H)\pi(nk, H, L) \tag{6}$$

where $\pi(nk, H, L)$ is the number of primary, irreducible polynomials of degree nk which are $\equiv L \pmod H$. Since the Riemann hypothesis holds for the function fields considered here,

$$\pi(nk, H, L) = q^{nk}/nk\,\Phi(H) + O(q^{nk/2}) \tag{7}$$

where $\Phi(H)$ is the number of residue classes (mod H) which are prime to H.

By Theorem 6.1 of [5],

$$\sum_{\deg L<\deg H;\ (L,H)=1} E(\delta LG/H) = \mu(H) \tag{8}$$

where μ is the natural analog of the Möbius function.

Therefore, by (6), (7), and (8),

$$\sum_P{}' E(\delta_1 PG/H) \sum_P{}' E(\delta_2 PG/H) = \mu^2(H)\left(\frac{q^{2nk}}{(nk)^2\Phi^2(H)} + O\left(\frac{q^{3nk/2}}{nk\Phi(H)}\right)\right). \tag{9}$$

Hence, by (5) and (9),

$$T_1 = \frac{q^{n+nk}}{(nk)^2} \sum_{G/H \text{ primordial};\ \deg H<n} q^{-h}\frac{\mu^2(H)}{\Phi^2(H)} S(\delta_3 G, H)E(-KG/H)$$
$$+ O\left(\frac{q^{n+nk/2}}{nk} \sum_{G/H \text{ primordial};\ \deg H<n} q^{-h}\frac{\mu^2(H)}{\Phi(H)} \cdot S(\delta_3 G, H)E(-KG/H)\right).$$

We will now assume $k \geqq 3$; the case $k = 2$ is easily handled (see Theorem 2).

Let

$$A(H) = q^{-h} \sum_{(G,H)=1} S(\delta_3 G, H)E(-KG/H)$$

where the sum is over a reduced residue system (mod H).

Since $\deg H < n$, $\Phi(H) < q^n$, so

$$T_1 = \left(\frac{q^{(k+1)n}}{(nk)^2} + O\left(\frac{q^{(2+k/2)n}}{nk}\right)\right) \sum_{\deg H<n}{}' A(H)\frac{\mu^2(H)}{\Phi^2(H)}. \tag{10}$$

Let $\mathfrak{S}_1$ be the singular series

$$\mathfrak{S}_1 = \sum_H{}' A(H)\mu^2(H)/\Phi(H) \tag{11}$$

where the summation is over all primary polynomials.

By an argument which is similar to that used in [1, Theorem 8.5, p. 258] we may show that

$$S(A, P) \leqq (d-1)|P|^{1/2} \tag{12}$$

where $d = (k, |P| - 1)$.

Since $A(H)$ and $S(G, H)$ are also multiplicative, we are able to obtain

$$A(H) = O(|H|^{-1/k}\Phi(H)). \tag{13}$$

This implies that $\mathfrak{S}_1$ is absolutely convergent and

$$\sum_{\deg H \geqq n}{}' A(H)\mu^2(H)/\Phi^2(H) = O(q^{-n/(k+1)}). \tag{14}$$

Now, since δG runs over a reduced system (mod P) as G does,

$$\begin{aligned} A(P) &= |P|^{-1} \sum_{(G,\,P)=1}\ \sum_{\deg R < \deg P} E(R^k G/P)E(-KG/P) \\ &= |P|^{-1} \sum_{\deg R < \deg P} \left(\sum_{\deg G < \deg P} E((R^k - K)G/P - 1) \right) \end{aligned}$$

where the inner sum is now over a complete system (mod P) including zero.

By Theorems 3.4 and 3.7 of [5],

$$\sum_{\deg G < \deg P} E((R^k - K)G/P) = \begin{cases} q^{\deg P} & \text{if } P \mid R^k - K, \\ 0 & \text{if } P \nmid R^k - K. \end{cases}$$

Letting $\psi_P(K)$ be the number of R such that $\deg R < \deg P$ and $P \mid R^k - K$, we have

$$\begin{aligned} A(P) &= q^{-\deg P}(\psi_P(K)(q^{\deg P} - 1) + (q^{\deg P} - \psi_P(K))(-1)) \\ &= \psi_P(K) - 1. \end{aligned} \tag{15}$$

Now, since A is multiplicative and $\mathfrak{S}$ is absolutely convergent, by (15),

$$\begin{aligned} \mathfrak{S}_1 &= \sum_H{}' A(H)\frac{\mu^2(H)}{\Phi^2(H)} = \sum_{H \text{ square-free}} \prod_{P \mid H} \frac{(\psi_P(K) - 1)}{(|P| - 1)^2} \\ &= \prod_P{}' \left(1 + \frac{\psi_P(K) - 1}{(|P| - 1)^2} \right) \end{aligned} \tag{16}$$

where the product is over all primary irreducible polynomials.

Since $\psi_P(K) \leqq k$, $\sum_P' 1/(|P| - 1)^2$ converges, and no factor in (16) is zero,

$$\mathfrak{S}_1 = c > 0. \tag{17}$$

Hence, by (10), (11), and (14), we have

$$T_1 = \mathfrak{S}_1 q^{(k+1)n}/(nk)^2 + O(q^{(k+1-1/(k+1))n}). \tag{18}$$

By (2), (4), and (18),

$$N_1(K) = \mathfrak{S}_1 q^{(k+1)n}/(nk)^2 + O(q^{(k+1-1/2^k)n}).$$

This completes the proof of Theorem 1.

In an entirely similar manner we may prove the following theorem.

THEOREM 2. *Let $N_2(K)$ and $N_3(K)$ be respectively the number of representations of K in the forms*

$$K = \delta_1 P_1 + \cdots + \delta_s P_s + \delta_{s+1} A_1^2 + \cdots + \delta_{s+r} A_r^2 \tag{19}$$

and

$$K = \delta_1 P + \delta_2 A_1^2 + \delta_3 A_2^2 + \delta_4 B^k \tag{20}$$

where $\deg K = nk = \deg P_i$, $\deg A_i = nk/2$, $\deg B = n$, *and* $\sum \delta_i =$ sgn K. *Then*

$$N_2(K) = \mathfrak{S}_2 q^{(r+2s-2)n}/(2n)^s + O(q^{(r+2s-2-1/2^k)n}) \tag{21}$$

provided $p > 2$ *and* $r + 2s > 4$; *and*

$$N_3(K) = \mathfrak{S}_3 q^{(k+1)n}/nk + O(q^{(k+1-1/2^k)n}) \tag{22}$$

provided $p > k$.

$\mathfrak{S}_2$ and $\mathfrak{S}_3$ are singular series similar to $\mathfrak{S}_1$ and both are positive constants.

In all of the results it was assumed that the degree of each of the summands is the same as the degree of K. If the degree of the summands is unrestricted, the problems change considerably and are generally much easier. However, if the degree of K is not a multiple of k we must allow summands of degree at least $([\deg K/k] + 1)k$. We may do this without changing the results significantly.

REFERENCES

1. R. Ayoub, *An introduction to the analytic theory of numbers,* Math. Surveys, no. 10, Amer. Math. Soc., Providence, R. I., 1963. MR 28 #3954.

2. S. Chowla, *The representation of a number as a sum of four squares and a prime,* Acta Arith. 1 (1963), 115–122.

3. T. Estermann, *Proof that every large integer is the sum of two primes and a square,* Proc. London Math. Soc. (2) 42 (1936), 501–516.

4. H. Halberstam, *On the representation of large numbers as sums of squares, higher powers, and primes,* Proc. London Math. Soc. (2) 53 (1951), 363–380. MR 13, 112.

5. D. R. Hayes, *The expression of a polynomial as a sum of three irreducibles,* Acta Arith. 11 (1966), 461–488. MR 34 #1306.

6. W. Webb, *Waring's problem in* $GF[q, x]$, Acta Arith. (to appear).

WASHINGTON STATE UNIVERSITY, PULLMAN, WASHINGTON 99163