[3] H. Davenport, *Indefinite quadratic forms in many variables*, Mathematika 3 (1956), pp. 81–101.
[4] — and H. Heilbronn, *On indefinite quadratic forms in five variables*, J. London Math. Soc. 21 (1946), pp. 185–193.
[5] — and K. F. Roth, *The solubility of certain Diophantine inequalities*, Mathematika 2 (1955), pp. 81–96.
[6] Jane Pitman, *Bounds for solutions of diagonal equations*, to appear in Acta Arith, 19 (1971) (DE).
[7] — and D. Ridout, *Diagonal cubic equations and inequalities*, Proc. Roy. Soc. A, 297 (1967), pp. 476–502.

THE UNIVERSITY OF ADELAIDE
Adelaide, South Australia

*Received on 8. 3. 1970*

ACTA ARITHMETICA
XVIII (1971)

# On Bombieri's estimate for exponential sums

by

J. H. H. Chalk and R. A. Smith (Toronto, Canada)

*In memory of H. Davenpor*

**1. Introduction.** In the course of an article [2] devoted mainly to the structure and interpretation of multiple exponential sums over finite fields, Bombieri included an estimate for the magnitude of certain special exponential sums "along a curve" (and, incidentally, generalized Weil's method [20] for similar sums "along a line"). For comparison purposes, it will be useful to have an abridged statement of this result (cf. [2], Theorem 6, p. 97). Thus, let $k = [q]$ denote the finite field of $q = p^a$ elements ($a \geqslant 1$) and characteristic $p$, $\sigma$ denote the absolute trace from $[q^m]$ to $[p]$, $e(x)$ denote $\exp(2\pi i x/p)$, $X$ a projective curve of degree $d_1$ defined over $k$ and embedded in projective $n$-space $\boldsymbol{P}^n$ over $k$, $X_m$ the set of points of $X$ defined over $[q^m]$, $R(X_0, X_1, \ldots, X_n)$ a homogeneous rational function in $\boldsymbol{P}^n$ defined over $k$ ($d_2$ being the degree of its numerator) and

$$\mathscr{S}_m(R, X) = \sum_{x \in X_m}{}' e\big[\sigma\big(R(x)\big)\big], \tag{1}$$

where "′" indicates that the poles of $R$ are omitted. Then

$$|\mathscr{S}_m(R, X)| \leqslant (d_1^2 - 3d_1 + 2d_1 d_2)\, q^{m/2} + d_1^2, \tag{2}$$

provided that

(A) for every homogeneous rational $h \in \bar{k}(X_0, \ldots, X_n)$, the function

$$R - (h^p - h) \tag{3}$$

does not vanish identically on any absolutely irreducible component of $X$.

This condition (A), which restricts the choice of $R$ not only in its behaviour over $k$ but also over the algebraic closure $\bar{k}$ of $k$, is stated (without details) to hold if[1]

(B) $p > d_1 d_2$ and $R$ is not constant on any such component of $X$.

[1] It seems likely that (2) continues to hold even if the restriction on $p$ in (B) is ignored.

Bombieri's methods belong to algebraic geometry and the principal tools (cf. [2], Theorem A (i), A (ii); pp. 87–88) are the "Artin conjecture" and the Riemann Hypothesis for the $L$-function defined by

$$L(t, R, X) = \exp\Big(\sum_{m=1}^{\infty} \mathscr{S}_m(R, X) t^m/m\Big), \tag{4}$$

which tell us that $L(t, R, X)$ is a *polynomial* in $t$ and that all its zeros have modulus $q^{-1/2}$, respectively (cf. A. Weil, [21], pp. 72–83). In this paper, we shall consider first one of the simplest cases of interest in (1); namely,

$$a = 1, \quad k = [p], \quad m = 1, \quad n = 2, \quad R \in k[X_0, X_1, X_2], \tag{5}$$

so that, by a slight change of notation,

$$\mathscr{S}_1(\mathscr{F}, X) = \sum_{\Psi(x,y,z)=0} e\big(\mathscr{F}(x, y, z)\big) \tag{6}$$

where now $\mathscr{F}$ and $\Psi$ are *forms* in $k[X, Y, Z]$ and the curve $X$ is defined in $\boldsymbol{P}^2$ by the equation $\Psi(x, y, z) = 0$. In fact, with a view to applications (cf. [17], [26]), we shall work with the affine form of (6),

$$S_2(f, \psi) = \sum_{\psi(x,y)=0} e\big(f(x, y)\big) \tag{7}$$

where $f$ and $\psi$ are polynomials in $k[X, Y]$ of degrees $d_2$ and $d_1$ respectively, and the sum on the right is over all pairs $(x, y) \in k^2$. Our methods stem from the arithmetic and analytic theory of Artin–Schreier extensions of function-fields of one variable over $k$, as developed by Hasse (cf. [9]; [10]; [11], Ia, § 8) in the early 1930's and provide an interesting and close parallel to those of Bombieri (cf. [2], § VI, pp. 93–99). The resulting estimate (Theorem 2)

$$|S_2(f, \psi)| \leqslant (d_1^2 - 3d_1 + 2d_1d_2)p^{1/2} + d_1^2 \tag{8}$$

is precisely the same as his (in the special case (5)) and holds, subject to the condition

$$\text{(C) } f(X, Y) \not\equiv a \big(\mathrm{mod}\, \psi_j(X, Y)\big) \text{ in } k[X, Y] \quad \forall a \in k \text{ and } \forall \text{ absolutely irreducible } \psi_j \mid \psi \text{ in } k[X, Y], \tag{9}$$

which is an alternative way of stating the condition (B) for our case, but without the restriction "$p > d_1d_2$". Since estimates of this kind lose their significance unless $p$ is large compared with $d_1$ and $d_2$, the coefficient of $p^{1/2}$ in (8) is the dominant one (and Bombieri [2], p. 99, remarks that the constant $d_1^2 - 3d_1 + 2d_1d_2$ in (2) cannot be improved but that the constant $d_1^2$ can be pared down to $(d_1 - 1)(d_2 - 1)/2$ ).

In a discussion of Bombieri's theorem, H. Heilbronn remarked that



estimates such as (8) were implicit in the literature and outlined the ideas, adding that Hasse's article [9] contained most of the relevant background material. With supplementary references, including Hasse's "Bericht ..." [11], Schmidt [16], Bombieri and Davenport [3], the books of Eichler [7] and Chevalley [6], and with (C) in mind as an economical way of excluding pairs $f$ and $\psi$ which violate (8), the first part of this paper is devoted to a detailed examination of the process by which Weil's theorem on the Riemann Hypothesis for algebraic function-fields may be applied to produce (8). In our case, the function-field is given by

$$L = K(u), \quad \text{where} \quad u^p - u - \zeta = 0, \quad \zeta = f(x, y) \in K$$

and $K$ is the function-field generated by $\psi(x, y) = 0$ over $k = [p]$. A condition somewhat analogous to (A) is implicit in Lemma 2, p. 196 and it is in fact a novel but quite minor extension of the result(2) of Bombieri and Davenport ([3], Lemma 4) expressed in the language of field-theory. It provides a valuable criterion, namely

$$\text{g.c.d.}\,\big(p, [\bar{k}K, \bar{k}(\zeta)]\big) = 1 \tag{10}$$

for judging whether $L = K(u)$ is a genuine extension of $K$ (and not just of $k$), when $\zeta$ is transcendental over $k$; i.e. it is a sufficient condition to ensure that the polynomial

$$U^p - U - \zeta \tag{11}$$

in $K[U]$ is irreducible over $\bar{k}K$ when $\zeta = f(x, y)$ is a non-constant element of $K$. But, as in Theorem 1, we shall arrange that the polynomial $\psi(x, Y)$ is irreducible over $\bar{k}(x)$, in which case $k$ *is* the exact field of constants of $K$ and of $L$. (For the "Artin conjecture", it is at least desirable to maintain a minimal field of constants; see e.g. [9], § 6, p. 52.) Then, of course, $\zeta = f(x, y)$ is a constant element of $K$ if and only if $f(x, y) \in k$ and condition (C) is enough (having been designed with this purpose!) to secure $f(x, y) \notin k$. Further preparations for the proof of Theorem 1 are listed in Lemma 1 where, at the expense of excluding the primes $p < d_1^2 d_2$, we ensure that $\zeta$ is a separating element of $K$ over $k$. Thus, reading $\psi$ for $F$ in Lemma 1 (as we may) it follows that, for $p > d_1^2 d_2$,

$$K/k(\zeta) \text{ is a finite separable extension, by (iv).}$$

Then since $[\bar{k}K\colon \bar{k}(\zeta)] \leqslant [K\colon k(\zeta)]$, $K$ being a simple extension of $k(\zeta)$, we have

$$[\bar{k}K\colon \bar{k}(\zeta)] \leqslant d_1^2 d_2 < p,$$

and Lemma 2 (iii) tells us that $L = K(u)$, where $u$ is a zero of the polynomial (11), is a cyclic extension of $K$ of degree $p$. In (v) of Lemma 1

(2) This was the subject of a brief correspondence with Davenport in 1968. Our version uses the same ideas, but permits greater freedom of choice for $f$ and $\psi$.

it is pure convenience to replace the bound on $p$ by $p < (d_1 d_2)^2$; for then it is slightly less troublesome to verify the inequality (12), which is precisely what is required in (29) (where the degree of the discriminant divisor of $L/K$ is being estimated), to give the proposed coefficient of $p^{1/2}$ in (8). But, although the small primes may need special treatment in the programme outlined above, it is economical to provide an alternative direct proof of (8) for them; see end of proof of Theorem 2.

In Section 3, we sketch the main features of Hasse's paper [9], pausing only to supplement his formulae where needed by references and computational details relevant to the constants in (8) (and suggest that the reader refer to the original paper, and the references given there for a comprehensive treatment). As with Bombieri's work, the "Artin conjecture" and Weil's theorem (which in our case refer to the $L$-functions and $\zeta$-functions in (20)) are the essential tools. It appears that even in our very special case where the Galois group $G(L/K)$ is cyclic, some class-field theory seems to be obligatory in proving the "Artin conjecture" when the genus of $K$ is not zero.

Theorem 2 is a straightforward deduction from Theorem 1 and provides a useful stepping-stone for lifting our estimates for exponential sums "along a curve" to exponential sums "over a hypersurface" (Theorem 3) in much the same way as Uchiyama [18] did for unrestricted multiple exponential sums. However, this is by no means as direct as in Uchiyama's case and some preliminary normalization (Lemmas 3, 4) of the hypersurface seems essential for the induction proof. The development, as given in Sections 5 and 6, has been designed to retain the flavour of the earlier work in Sections 2 and 3 on function-fields, but a similar normalization could be obtained by appealing to standard results in algebraic geometry on sections of varieties (e.g. [13], Lemma 2).

**2.** Throughout the remainder of this paper, $k = [p]$ will denote the finite field of $p$ (prime) elements. On reading $(X, Y)$ for $(X_1, X_2)$, the notation and definitions of Section 4, p. 203 relating to $(X_1, X_2, \ldots, X_n)$ apply here with $n = 2$. Thus, in particular,

$$f \equiv g \pmod h \text{ in } k[X, Y]$$
$$\Leftrightarrow f, g, h \text{ belong to } k[X, Y] \text{ and } f - g = h\lambda \text{ with } \lambda \in k[X, Y],$$

in accordance with the general definition.

LEMMA 1. *For any $F \in k[X, Y] - k[X] - k[Y] - k[X, Y^p]$ irreducible over $k(X)$, let $K = k(x, y)$ denote the algebraic function-field over $k$ generated by $F(x, y) = 0$. Then*

(i) *$K$ is a finite separable extension of $k(x)$,*

(ii) *the field of constants in $K$ is $k$ itself $\Leftrightarrow F(X, Y)$ is irreducible over $k_1(X)$, $\forall$ finite extensions $k_1/k$,*



(iii) *if $k$ is the (exact) field of constants of $K$ and $f \in k(X, Y)$ satisfies*

$$f \not\equiv a \pmod F, \quad \forall a \in k$$

*then $\zeta = f(x, y) \in K$ is transcendental over $k$ (i.e. $\notin k$),*

(iv) $[K\colon k(\zeta)] \leqslant d^2(F)\, d(f)$,

(v) *if $p > d^2(F)\, d^2(f)$ then $K$ is a (finite) separable extension of $k(\zeta)$ and moreover,* (iv) *can be strengthened to*

$$[K\colon k(\zeta)] \leqslant d(F)\, d(f). \tag{12}$$

Proof. Clearly (i) is a consequence of the hypotheses

$$[K\colon k(x)] \leqslant d(F) < \infty, \quad F \notin k[X, Y^p].$$

A well-known criterion for ensuring that the algebraic closure $\tilde{k}$ of $k$ in $K$ satisfies $\tilde{k} = k$ is given in (ii) (cf. Eichler [7], III, § 3.4, pp. 135–136 and III, § 6.1, p. 171). In fact, for (ii) it is enough to use the degree relations

$$[k_1 K\colon k(x)] = [k_1 K\colon k_1(x)][k_1(x)\colon k(x)] = [k_1 K\colon K][K\colon k(x)],$$
$$[k_1(x)\colon k(x)] = [k_1\colon k] \quad \text{(valid since } x \notin \tilde{k}),$$

and note that the condition

$$[k_1 K\colon k_1(x)] = [K\colon k(x)]$$

expresses the irreducibility of $F(X, Y)$ over $k_1(X)$, while

$$\tilde{k} = k \Leftrightarrow [k_1\colon k] = [k_1 K\colon K] \quad \forall \text{ finite extensions } k_1/k.$$

For (iii), we use the division algorithm in the polynomial domain $k(X)[Y]$ to produce $r \neq 0$ and $q$, both in $k[X, Y]$, and $s \neq 0$ in $k[X]$ such that

$$s(X)[f(X, Y) - a] = q(X, Y)F(X, Y) + r(X, Y),$$

identically in $k[X, Y]$ and with degrees (in $Y$) satisfying

$$d_Y(r) < d_Y(F).$$

Thus, *if* there exists $a \in k$ such that $\zeta = f(x, y) = a$, then $r(x, y)$ must vanish, since $f(x, y) - a = F(x, y) = 0$. But $r \notin k[X] \cup k[Y]$, since both $x$ and $y$ are transcendental over $k$. Hence $r(x, y) = 0$, which is incompatible with the definition of $F$.

In (iv) and (v) the special case when $f \in k[X]$ can be treated directly. Since, on general grounds, $\big[k(t)\colon k\big(f(t)\big)\big] = d(f)$ for any transcendental $t$ over $k$, we have

$$[K\colon k(\zeta)] = [K\colon k(x)]\big[k(x)\colon k\big(f(x)\big)\big] = d_Y(F) \cdot d(f)$$

without restriction on $p$. Otherwise, when $f \notin k[X]$, we first form the resultant $R(X, Z)$ of $F(X, Y)$ and $f(X, Y) - Z \in k[Z][X, Y]$ and observe

that it is not identically 0 in $k[X, Z]$. Moreover ($R$ being a linear combination of $F(X, Y)$ and $f(X, Y)-Z$), the substitution $(X, Y) \to (x, y)$ gives $R(x, \zeta) = 0$ and then, since neither of $x$ and $\zeta$ is algebraic over $k$, we have

$$R \in k[X, Z]-k[X]-k[Z].$$

Now

$$[K\colon k(\zeta)] \leqslant [K\colon k(x)][k(x, \zeta)\colon k(\zeta)],$$

where

$$[K\colon k(x)] = d_Y(F) \quad \text{and} \quad [k(x, \zeta)\colon k(\zeta)] \leqslant d_X(R) \leqslant d(R) \leqslant d(f)d(F),$$

since a resultant of any pair of polynomials $P, Q$ say is isobaric of weight $= d(P)d(Q)$. This completes the proof of (iv) (in place of resultants, one could equally well appeal to Bezout's theorem).

To complete (v), we may suppose that $f \in k[X, Y]-k[X]$ and, for $p > d^2(F)d(f)$, that $K$ is a finite separable extension of $k(\zeta)$. Then, by a standard theorem([3]) on primitive elements of finite separable extensions, there exists a $c \in k$ such that $K = k(z, t)$ with

$$t = x + cy.$$

If $c = 0$, there is nothing further to prove. Otherwise, we form the resultant $R^*(Z, T)$ of $F(T-cY, Y)$ and $f(T-cY, Y)-Z$; argue as for $R$ previously to obtain

(a) $R^*(Z, T) \in k[Z, T]-k[Z]-k[T]$,

(b) $R^*(\zeta, t) = 0$,

(c) $d_T(R^*(Z, T)) \leqslant d(f)d(F)$.

Then

$$[K\colon k(\zeta)] = [k(\zeta, t)\colon k(\zeta)] \leqslant d_T(R^*) \leqslant d(R^*) \leqslant d(f)d(F),$$

since the degrees of $f$ and $F$ are unaffected by the substitution

$$X \to T-cY.$$

LEMMA 2. *Let $x$ be a transcendental over $k$ and suppose that $K$ is a finite extension of $k(x)$. Let $\zeta \in K$ be any transcendental over $k$ which satisfies*

$$\text{g.c.d.}\,(p, [\bar{k}K\colon \bar{k}(\zeta)]) = 1,$$

*where $\bar{k}$ denotes the algebraic closure of $k$. Then*

(i) *the polynomial $P(U) = U^p - U - \zeta$ is irreducible over $\bar{k}K$,*

(ii) *if $u$ is a zero of $P(U)$, then*

$$[\bar{k}K(u)\colon \bar{k}K] = [K(u)\colon K] = p, \tag{13}$$

*and*

(iii) *$L = K(u)$ is a cyclic extension of $K$ of degree $p$.*

([3]) A condition such as $p > (d(f)d(F))^2$ arises at this stage if we follow the argument in van der Waerden [19], p. 126.



Proof. By hypothesis, $K$ is an algebraic function field of one variable over $k$. Hence, there exists $F(X, Z) \in k[X, Z]-k[X]-k[Z]$ with the property that

$$F(x, \zeta) = 0,$$

which gives $[k(x, \zeta)\colon k(\zeta)] < \infty$. By means of the degree relations

$$[K\colon k(x)] = [K\colon k(x, \zeta)][k(x, \zeta)\colon k(x)],$$

$$[K\colon k(\zeta)] = [K\colon k(x, \zeta)][k(x, \zeta)\colon k(\zeta)]$$

it follows therefore that $[K\colon k(\zeta)] < \infty$. We now observe (by means of degree relations for polynomials) that $\zeta$ itself is not expressible in the form

$$\zeta = (\lambda/\mu)^p-(\lambda/\mu) \quad \text{with } \lambda \text{ and } \mu \text{ in } \bar{k}[\zeta],\ (\lambda, \mu) = 1;$$

for, on rewriting it as

$$\mu^p \zeta = \lambda^p - \lambda\mu^{p-1}$$

and counting degrees (with obvious notation),

$$pd_\mu + 1 = \max\{pd_\lambda, pd_\mu + (d_\lambda - d_\mu)\},$$

where $d_\mu < d_\lambda$ and $p \nmid 1$; a contradiction. Hence $P(U)$ is irreducible over $\bar{k}(\zeta)$ and so

$$[\bar{k}(\zeta, u)\colon \bar{k}(\zeta)] = p.$$

By the Artin–Schreier theorem, we know that

$$[\bar{k}K(u)\colon \bar{k}K] = 1 \text{ or } p.$$

If this degree is 1, then $\bar{k}K(u) = \bar{k}K$, $u \in \bar{k}K$ and $\bar{k}(x, u) \subseteq \bar{k}K$. But, from

$$[\bar{k}K\colon \bar{k}(\zeta)] = [\bar{k}K\colon \bar{k}(\zeta, u)][\bar{k}(\zeta, u)\colon \bar{k}(\zeta)] = [\bar{k}K\colon \bar{k}(\zeta, u)]\cdot p \equiv 0 \bmod p$$

and our hypothesis for $[\bar{k}K\colon \bar{k}(\zeta)]$, we arrive at a contradiction. Hence

$$[\bar{k}K(u)\colon \bar{k}K] = p;$$

which says, simply, that $P(U)$ is irreducible in $\bar{k}K[U]$, as required. Since $P(U) \in K[U]$, we also have

$$[K(u)\colon K] = p$$

and (cf. [12], Theorem 11) $K(u)$ is a cyclic extension of $K$ of degree $p$.

**3.** THEOREM 1. *Let $f, \psi$ be given elements of $k[X, Y]$, subject to the conditions*

(i) *$\psi(X, Y)$ absolutely irreducible over $k$,*

(ii) *$f(X, Y) \not\equiv a \bmod \psi(X, Y)$, $\forall a \in k$.*

*Then, with* $d_1 = d(\psi)$, $d_2 = d(f)$,

$$|S_2(f,\psi)| \leqslant (d_1^2 - 3d_1 + 2d_1d_2)p^{1/2} + d_1^2, \tag{14}$$

*for all* $p \geqslant d_1^2 d_2^2$.

Remark. The condition on $p$ is convenient in the following proof; in fact, Theorem 1 holds for all $p$ (see e.g. (44)).

Proof. In view of Weil's estimate

$$|S_1(f(X),0)| \leqslant (d_2-1)p^{1/2}$$

the theorem holds when $\psi \in k[X] \cup k[Y]$. By Lemmas 1 and 2 and the remarks concerning them in Section 1, it follows that, for $p > d(f)d^2(\psi) = d_1^2 d_2$, $\zeta \in K$, the field $L = K(u)$ obtained by adjoining a root of the equation $u^p - u - \zeta = 0$ to $K$ is a (finite) cyclic separable extension of $K$ of degree $p$, whose (exact) field of constants is $k$ itself.

Let $(\zeta)$ denote the principal divisor in $K$ associated with the field element $\zeta = f(x,y) \in K$ and express $(\zeta)$ in the form

$$(\zeta) = \mathfrak{a}/\mathfrak{b}, \quad \text{where} \quad \text{g.c.d.}\ (\mathfrak{a},\mathfrak{b}) = 1,$$

$\mathfrak{a}$ being the integral divisor of zeros of $\zeta$ and $\mathfrak{b}$ the integral divisor of poles of $\zeta$. By Lemma 1 (iii), $\zeta$ is transcendental over $k$ and so has at least one pole in $K$; whence $\mathfrak{b}$ is not the unit divisor (1) in $K$. Let

$$\mathfrak{b} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}, \quad e_i \geqslant 1, \quad (\mathfrak{p}_i, \mathfrak{p}_j) = 1 \quad (i \neq j),$$

denote the decomposition of $\mathfrak{b}$ in $K$ as a product of powers of prime divisors in $K$. For later use, we note that

$$e_i \not\equiv 0 \pmod p, \quad i = 1, 2, \dots, r, \tag{15}$$

since

$$e_i \leqslant e_i \deg \mathfrak{p}_i \leqslant \deg \mathfrak{b} \leqslant [K\colon k(\zeta)] \quad \text{(cf. [6], Theorem 4, Corollary)},$$
$$\leqslant d_1^2 d_2, \quad \text{by Lemma 1(iv)},$$

and so, $e_i < p$, $\forall i$ under our present hypothesis on $p$. We can now follow Hasse's account of the local decomposition theory for cyclic fields ([9]; §§ 3, 6). Thus, for each prime divisor $\mathfrak{p}$ of $K$ which does not ramify in $L$, define $S_{\mathfrak{p}}(\zeta)$ to be the trace of $\zeta$ viewed as an element of the residue class field $\mathfrak{o}/\mathfrak{p}$, ($\mathfrak{o}$ being the local ring of elements of $K$ which are integral at $\mathfrak{p}$) and put

$$\chi(\mathfrak{p}) = \begin{cases} e\big(S_{\mathfrak{p}}(\zeta)\big), & \text{if } \mathfrak{p} \text{ is unramified in } L, \\ 0, & \text{if } \mathfrak{p} \text{ is ramified in } L. \end{cases} \tag{16}$$

On forming the infinite products

$$L(s,\chi^\nu) = \prod_{\mathfrak{p}} [1 - \chi^\nu(\mathfrak{p}) N\mathfrak{p}^{-s}]^{-1} \quad (\nu = 1, 2, \dots, p-1), \tag{17}$$



$$\zeta_K(s) = \prod_{\mathfrak{p}} [1 - N\mathfrak{p}^{-s}]^{-1}, \quad \text{over all } \mathfrak{p} \text{ in } K, \tag{18}$$

and

$$\zeta_L(s) = \prod_{\mathfrak{P}} [1 - N\mathfrak{P}^{-s}]^{-1}, \quad \text{over all } \mathfrak{P} \text{ in } L, \tag{19}$$

direct verification ([9], p. 51) gives

$$\zeta_L(s) = \zeta_K(s) \prod_{\nu=1}^{p-1} L(s,\chi^\nu) \quad (Rs > 1). \tag{20}$$

From the Riemann–Roch theorem for function-fields of one variable (and the functional equations for $\zeta_L$ and $\zeta_K$ consequent upon it), it is known that $\zeta_L(s)$ and $\zeta_K(s)$ admit analytic continuations into the whole complex $s$-plane and are meromorphic functions of $s$ there, whose singularities are simple poles at $s = 0$ and $s = 1$. The functional equation also shows that $\zeta_L(s)$ and $\zeta_K(s)$ have precisely $2G$ and $2g$ zeros, where $G$ and $g$ denote the genus of $L$ and $K$, respectively. It can also be established (cf. [9], pp. 51–52), that $L(s,\chi^\nu)$ is a polynomial in $p^{-s}$ of fixed degree $l$ say (i.e., independent of $\nu$), which must therefore satisfy, in view of the remark above and (20),

$$(p-1)l = 2G - 2g. \tag{21}$$

Hence

$$L(s,\chi^\nu) = \prod_{1 \leqslant i \leqslant l} [1 - \omega_i^{(\nu)} p^{-s}], \tag{22}$$

and so, on comparing the coefficients of $p^{-s}$ on both sides,

$$\sum_{\deg \mathfrak{p} = 1} \chi^\nu(\mathfrak{p}) = -\sum_{1 \leqslant i \leqslant l} \omega_i^{(\nu)} \tag{23}$$

for each $\nu = 1, 2, \dots, p-1$. Then, by Weil's theorem on the Riemann Hypothesis ([22]; a version is given in Eichler [7], p. 305), as applied to $\zeta_L(s)$, we have

$$|\omega_i^{(\nu)}| = p^{1/2}, \quad \forall\, i, \nu \tag{24}$$

so that, combining (23) with (21) and (24),

$$\Big|\sum_{\mathfrak{p} \in P} \chi(\mathfrak{p})\Big| \leqslant \frac{2G-2g}{p-1} \cdot p^{1/2}, \tag{25}$$

where $P$ denotes the set of all prime divisors $\mathfrak{p}$ of $K$ of degree 1 which do not ramify in $L$. Now (25) is our basic inequality and (14) is an elementary consequence. First, the Hurwitz genus formulae (a convenient version is given in Eichler, [7], p. 134; (9), (10)) gives

$$\frac{2G-2g}{p-1} = 2g - 2 + \frac{\deg_K(\mathrm{Disc}\, L/K)}{p-1} \tag{26}$$

and since (cf. Hasse [9], § 3, part (b)),

$$\text{Disc}L/K = \prod_{1\leqslant i\leqslant r} \mathfrak{p}_i^{(p-1)(e_i+1)}, \tag{27}$$

when $e_i \not\equiv 0 \pmod p$ for $i = 1, 2, \ldots, r$,

$$\begin{aligned}\deg_K(\text{Disc}L/K) &= (p-1)[(e_1+1)\deg\mathfrak{p}_1+\ldots+(e_r+1)\deg\mathfrak{p}_r]\\ &\leqslant 2(p-1)[e_1\deg\mathfrak{p}_1+\ldots+e_r\deg\mathfrak{p}_r]\\ &= 2(p-1)\deg\mathfrak{d}\\ &= 2(p-1)\deg(\zeta)_\infty\\ &= 2(p-1)[K\colon k(\zeta)] \quad \text{(cf. [6], Theorem 4, Corollary)} \qquad (28)\\ &\leqslant 2(p-1)d_1d_2, \qquad (29)\end{aligned}$$

if we apply the estimate in Lemma 1(v) to (28). Thus, for $p \geqslant (d_1d_2)^2$ we can combine (26) and (29) for insertion in (25):

$$\Big|\sum_{\mathfrak{p}\in P}\chi(\mathfrak{p})\Big| \leqslant [2g-2+2d_1d_2]p^{1/2} \leqslant [d_1^2-3d_1+2d_1d_2]p^{1/2}, \tag{30}$$

on using the classical bound $g \leqslant \frac{1}{2}(d-1)(d-2)$ for the genus.

Now, if $P^*$ consists of all the *finite* prime divisors of $P$, then

$$|P-P^*| \leqslant d_Y(\psi) \tag{31}$$

since any prime divisor in $k(x)$, and in particular the infinite prime $\infty_x$, splits into at most $d_Y(\psi)$ prime divisors in $K$. Moreover, if we write $\delta = d_Y(\psi)$, $\partial = d\big(c_\delta(X)\big)$ and

$$\psi(X, Y) = c_\delta(X)\,Y^\delta+\ldots+c_0(X),$$

then $c_\delta(x)$ has at most $\partial$ prime divisors in $k(x)$ and each of these splits into at most $\delta$ prime divisors in $K$. Thus, if $P_I^* \subseteq P$ denotes the set of finite prime divisors $\mathfrak{p}$ for which $y \in K$ is *integral* at $\mathfrak{p}$ (where $\psi(x, y) = 0$), then

$$|P^*-P_I^*| \leqslant \partial\delta.$$

For each $a \in k$, let $\mathfrak{p}_{a,i}$ $(i = 1, \ldots, s)$ denote the prime divisors of $K$ lying above the prime divisor of $k(x)$ corresponding to the polynomial $X-a \in k[X]$. Then as remarked above, $s \leqslant d_Y(\psi)$. Now let

$$\psi(X, Y) \equiv \psi(a, Y) \equiv (Y-b_1)^{e_1}\ldots(Y-b_s)^{e_s}\varphi_a(Y) \bmod (X-a) \tag{32}$$

denote the decomposition of $\psi(X, Y) \bmod (X-a)$ into distinct linear factors $Y-b_i$, where $b_i \in k$, and $\varphi_a(Y)$ satisfies $\varphi_a(b) \neq 0$ for any $b \in k$. Then, by the Kummer–Dedekind theorem (cf. [25], pp. 168–169), there exists a 1-1 correspondence between $\mathfrak{p}_{a,i} \in P_I^*$ and the pairs $(X-a, Y-b_i)$, $i = 1, \ldots, s$, given by

$$(x-a) = \mathfrak{p}_{a,1}^{e_1}\ldots\mathfrak{p}_{a,s}^{e_s}\mathfrak{a},$$



where $\deg\mathfrak{p}_{a,i} = 1$, $\forall\, i$ and $\mathfrak{a}$ has no finite prime divisor of degree 1. Note that $\mathfrak{p}_{a,i} \notin P_I^* \Rightarrow c_\delta(a) = \psi(a, b_i) = 0$ for all such $i$. Moreover, the general identity

$$\begin{aligned}F(X, Y) = \frac{F(X, Y)-F(a, Y)}{X-a}(X-a)+\\ +\frac{F(a, Y)-F(a, b)}{Y-b}(Y-b)+F(a, b),\end{aligned} \tag{33}$$

valid for arbitrary $F \in k[X, Y]$ and any $(a, b) \in k^2$, gives

$$F(x, y) \equiv F(a, b_i) \bmod \mathfrak{p}_{a,i} \quad (i = 1, \ldots, s), \tag{34}$$

and so

$$S_\mathfrak{p}(\zeta) = S_\mathfrak{p}\big(f(x, y)\big) = f(a, b) \in k, \tag{35}$$

whenever $(X-a, Y-b)$, or equivalently $(a, b)$, and a prime divisor $\mathfrak{p}$ of $K$ of degree 1 are related under the Kummer–Dedekind correspondence. Finally on applying these estimates to the difference between

$$\sum_{\mathfrak{p}\in P} e\big(S_\mathfrak{p}(\zeta)\big) \quad \text{and} \quad \sum_{\psi(a,b)=0} e\big(f(a, b)\big), \tag{36}$$

where the second sum is over *all* pairs $(a, b) \in k^2$, we obtain the bound

$$|P-P^*|+|P^*-P_I^*|+N\big(\psi(a, b) = c_\delta(a) = 0\big). \tag{37}$$

Hence by our estimate for the terms in (37), the sums in (36) differ by at most $\delta+\partial\delta+\partial\delta$, since $\psi(X, Y)$ and $c_\delta(X)$ are relatively prime in $k[X, Y]$. Since

$$d_1^2 \geqslant (\partial+\delta)^2 \geqslant \delta+2\partial\delta,$$

the result is complete.

In the next theorem we extend Theorem 1 to include the cases when $\psi$ is no longer absolutely irreducible and supply the additional argument to remove the restriction $p \geqslant d_1^2d_2^2$.

THEOREM 2. *Let $f$, $\psi$ be given elements of $k[X, Y]$ with $\psi$ not identically zero and suppose that they satisfy condition* (C) (see (9)). *Then*

$$|S_2(f, \psi)| \leqslant (d_1^2-3d_1+2d_1d_2)p^{1/2}+d_1^2 \tag{38}$$

*for all primes $p$, where $d_1 = d(\psi)$ and $d_2 = d(f)$.*

Proof. If $d_1 = 0$, then $\psi \in k-\{0\}$ and $S_2(f, \psi) = 0$. Otherwise let

$$\psi = \prod_{j=1}^{t}\psi_j \quad \text{in } k[X, Y] \tag{39}$$

where (4) the $\psi_j$ are the factors of $\psi$ which are irreducible in $k[X, Y]$ and, for convenience, $\psi_j$ for $j = 1, 2, \ldots, s$ where $s \leqslant t$ will denote those

(4) We may assume that the $\psi_j$ are distinct!

factors which are absolutely irreducible over $k$. We use the theorem of Bezout in the form

$$N\{(a,b)\in\bar{k}^2 \mid f(a,b)=F(a,b)=0\} \leqslant d(f)d(F), \tag{40}$$

where $f$ and $F$ are devoid of common factors in $k[X, Y]$. Thus

$$\Big|S_2(f,\psi)-\sum_{j=1}^{t} S_2(f,\psi_j)\Big| \leqslant \sum_{i\neq j} N\{(a,b)\in k^2 \mid \psi_i=\psi_j=0\} \leqslant \sum_{i\neq j}\delta_i\delta_j, \tag{41}$$

and

$$\Big|\sum_{i=s+1}^{t} S_2(f,\psi)\Big| \leqslant \sum_{i=s+1}^{t} N\{(a,b)\in k^2 \mid \psi_i=0\} \leqslant \sum_{i=s+1}^{t}\delta_i(\delta_i-1) \leqslant \sum_{i=s+1}^{t}[\delta_i^2+(2d_2-3)\delta_i] \tag{42}$$

where $\delta_j=d(\psi_j)$, since all zeros of $\psi_j$ for $j>s$ are multiple zeros and therefore singular. With Theorem 1 applied to each $\psi_j$ with $j\leqslant s$, these give

$$\begin{aligned}|S_2(f,\psi)| &\leqslant \Big|\sum_{j=1}^{s} S_2(f,\psi_j)\Big|+\Big|\sum_{j=s+1}^{t} S_2(f,\psi_j)\Big|+\sum_{i\neq j}\delta_i\delta_j \\ &\leqslant \sum_{j=1}^{t}\{\delta_j^2+(2d_2-3)\delta_j\}p^{1/2}+\sum_{j=1}^{t}\delta_j^2+\sum_{i\neq j}\delta_i\delta_j \\ &\leqslant \Big[\Big(\sum_{j=1}^{t}\delta_j\Big)^2+(2d_2-3)\sum_{j=1}^{t}\delta_j\Big]p^{1/2}+d_1^2 \\ &\leqslant [d_1^2+(2d_2-3)d_1]p^{1/2}+d_1^2,\end{aligned} \tag{43}$$

as required.

Now suppose that $p<d_1^2d_2^2$ and that $\psi$ is itself absolutely irreducible over $k$. Then

$$\begin{aligned}|S_2(f,\psi)| &\leqslant N\{(a,b)\in k^2 \mid \psi(a,b)=0\} \\ &\leqslant p+1+2gp^{1/2} \quad \text{(by the Riemann Hypothesis (5) for } K) \\ &= (p^{1/2}+2g)p^{1/2}+1 \\ &\leqslant (d_1^2-3d_1+d_1d_2+2)p^{1/2}+1 \\ &< (d_1^2-3d_1+2d_1d_2)p^{1/2}+d_1^2.\end{aligned} \tag{44}$$

Hence, we are now allowed to assume Theorem 1 for *all* primes $p$, and so in particular, (43) is true for *all* $p$.

(5) For a convenient reference, see [7], (23), pp. 299–307.



**4. Notation and definitions.** Capital Roman letters will denote independent indeterminates over $k$, while small Roman and Greek letters refer to algebraically dependent transcendentals over $k$, unless otherwise stated. In particular, if $X_1, X_2, \ldots, X_n$ are independent indeterminates over $k$, then for sake of brevity, we shall use the notation:

$$X=(X_1,\ldots,X_n),$$
$$X^i=(X_1,\ldots,\hat{X}_i,\ldots,X_n),$$

where $\hat{}$ signifies omission, $(X^n, a)=(X_1,\ldots,X_{n-1}, a)$, where $X^1=(X_2,\ldots,X_n)$ and $X^n=(X_1,\ldots,X_{n-1})$ are useful special cases of $X^i$ with $i=1$ and $n$. Similarly, for algebraically dependent transcendentals $x_1, x_2, \ldots, x_n$, we introduce the same notation for $x, x^i$, and $(x^n, a)$.

For the polynomial ring $k[X]$, we adopt the following definitions.

DEFINITION. (1) For any $f\in k[X]$,

$$f \textit{ contains } X_j \Leftrightarrow f\notin k[X^j].$$

(2) For any $f\in k[X]$, $d(f)$ denotes the total degree of $f$ and $d_V(f)$ denotes the degree of $f$ regarded as an element of $k[U][V]$, where $(U, V)$ is a permutation of $X$.

(3) $f\equiv g \pmod h$ in $k[X] \Leftrightarrow f, g, h$ belong to $k[X]$ and $f-g=\lambda h$ with $\lambda\in k[X]$.

Occasionally, it is convenient to use the Vinogradov symbol "$\ll$" in place of "$O$"; the implied constant will depend only on $n$ and at most on the degrees of the polynomials concerned.

**5.** The main theorem is an extension of Theorem 2 to the case of $n\geqslant 3$ indeterminates $X=(X_1, X_2, \ldots, X_n)$ with no attempt at precision in the matter of constants. In the course of the proof, we shall be working with a polynomial $\psi\in k[X]$, absolutely irreducible over $k$, and need an accurate form of the assertion that, for almost all $a\in k$, the sections $\psi(X_1, X_2, \ldots, X_{n-1}, a)=\psi(X^n, a)\in k[X^n]$ remain absolutely irreducible over $k$. As it stands, this is not quite true, as may be seen from the example

$$\psi(X)=X_1^2+X_2^2X_n, \quad n\geqslant 3, \tag{45}$$

where $\psi(X^n, a)$ is never absolutely irreducible over $k$, although $\psi(X)$ itself is. However, the difficulty can be circumvented by a preliminary linear non-singular transformation of $\psi$. In fact, *for* $n\geqslant 3$, a suitable permutation of $X_1, \ldots, X_n$ and an application of a shear of the type

$$X_n'=X_n+cX_{n-1}, \tag{46}$$

with an appropriately chosen $c\in k$, will be sufficient to ensure, for some $\eta$ transcendental over $k$, that

$$\psi(X^n, \eta)\in k[\eta][X^n]$$

is absolutely irreducible over $k(\eta)$. Then the hypotheses of Lemma 3 are fulfilled and the desired form of the assertion above may be concluded. The proof of Lemma 3 itself is entirely classical and depends upon the theory of resultant systems; one might note, in passing, that the existence of the absolutely irreducible section $\psi(X^n, \eta)$ of $\psi(X)$ is used solely as a device to avoid the possibility of the resultant system vanishing identically under the specializations considered.

LEMMA 3. *Suppose that $\psi(X)$ is absolutely irreducible over $k$ and that, for $\eta$ transcendental over $k$,*

$$\psi(X^n, \eta) \in k[\eta][X^n] \tag{47}$$

*is absolutely irreducible over $k(\eta)$. Then $\psi(X^n, a)$ is NOT absolutely irreducible over $k$ for at most $O_{n,d}(1)$ values of $a \in k$.*

One critical step in the proof of Theorem 3 concerns the number of zeros $x^n \in k^{n-1}$ of $\psi(x^n, a)$ and requires what is essentially a special case of the theorem of Lang and Weil ([13], Theorem 1) on the number of rational points on a variety, defined over $k$ (cf. [24], Proposition 2, p. 74):

COROLLARY. *For each $a \in k$ for which $\psi(X^n, a)$ is absolutely irreducible over $k$,*

$$N\{x^n \in k^{n-1} \mid \psi(x^n, a) = 0\} = p^{n-2} + O_{n,d}(p^{n-5/2}). \tag{48}$$

In order to realize the hypothesis of Lemma 3 in the manner described, we recall the classical argument of Zariski ([27], Lemma 5), as reproduced in [8], (pp. 81–83), for varieties defined over a field $k$ of characteristic 0. (For unrestricted characteristic, see e.g. [23], pp. 97–99 and references given there.) The modifications for the case of characteristic $p$ are relatively minor if $p$ is large and they are noted in our outline of the proof of Lemma 4.

LEMMA 4 ($n \geqslant 3$). *Suppose that $\psi(X)$ is absolutely irreducible over $k$ and contains both $X_1$ and $X_n$. Let $p > 2^d$, where $d = d(\psi)$. Then there exists $c \in k$ such that*

$$\varphi(X) = \psi(X^n, X_n + cX_{n-1})$$

*has the property that $\varphi(X^n, \zeta) \in k[\zeta][X^n]$ is absolutely irreducible over $k(\zeta)$ for some $\zeta$ transcendental over $k$.*

Proof of Lemma 3. Regard $\psi(X)$ as an element of $k[X_n][X^n]$ and put $d_n = d_{X^n}(\psi)$. Then, by the Emmy Noether theorem ([14]; a version is given in Perron, [15], Satz 140), we can assert, for each integer $l$ with $1 \leqslant l \leqslant d_n - 1$, the existence of a finite set of polynomials

$$\boldsymbol{R}_{l,\lambda}(X_n), \quad \lambda = 1, 2, \ldots, \Lambda(l) \tag{49}$$

in $k[X_n]$, where $\Lambda(l)$ and the degree of each $\boldsymbol{R}_{l,\lambda}$ in $k[X_n]$ are bounded in terms of $n$ and $d$, with the property:



If we regard $t$ as a variable element of some fixed algebraically closed field $K$ containing $k(\eta)$, then

$$\boldsymbol{R}_{l,\lambda}(t) = 0, \quad \lambda = 1, 2, \ldots, \Lambda(l) \tag{50}$$

is a necessary and sufficient condition for $\psi(X^n, t) \in k[t][X^n]$ to factorize in the form $\psi_1(X^n) \cdot \psi_2(X^n)$ with

$$d(\psi_1) = l, \quad d(\psi_2) = d_n - l \tag{51}$$

and $\psi_i \in k_t[X^n]$, $i = 1, 2$, where $k_t$ is some (necessarily finite) extension of $k(t)$; it being understood that $t$ does not take one of the finite set of values for which the coefficients $\theta_\lambda(t)$ of the terms of highest degree in $\psi(X^n, t)$ vanish simultaneously. Hence if $a \in k$, a factorization of $\psi(X^n, a)$ over some finite algebraic extension of $k$ will, apart from possibly $O_{n,d}(1)$ exceptions, entail the simultaneous vanishing of

$$\boldsymbol{R}_{l,\lambda}(a), \quad \lambda = 1, 2, \ldots, \Lambda(l) \tag{52}$$

for some $l$ with $1 \leqslant l \leqslant d_n - 1$. Moreover, by our hypothesis on $\psi(X^n, \eta)$, it is impossible for $\boldsymbol{R}_{l,\lambda}(t)$, $\lambda = 1, 2, \ldots, \Lambda(l)$ to vanish identically in $t$. Thus, there can be at most $O_{n,d}(1)$ values of $a \in k$ for which $\psi(X^n, a)$ splits, or reduces to a constant.

Outline of the proof of Lemma 4 (cf. [8], pp. 81–83). First, let $F$ denote any irreducible polynomial in $k'[X]$ containing both $X_1$ and $X_n$; $k'$ being any extension of $k$. Introduce algebraically independent indeterminates $\xi_2, \ldots, \xi_n$ over $k'$ and let $\Sigma = k'(\xi_1, \xi_2, \ldots, \xi_n) = k'(\xi)$ denote the function-field over $k'$ defined by the equation $F(\xi_1, \xi_2, \ldots, \xi_n) = 0$. Suppose that $p > d(F)$; then

$$F \text{ is absolutely irreducible over } k' \Leftrightarrow k' \text{ is algebraically closed in } k'(\xi). \tag{53}$$

We shall apply this criterion for absolute irreducibility in two cases:

$$(n, k', F) = \{n, k, \psi(X)\} \quad \text{and} \quad \{n-1, k(\zeta), \varphi(X^n, \zeta)\},$$

where $\zeta = \xi_n + c\xi_{n-1}$ for some $c \in k$. From the first case and our hypothesis for $\psi$, we have

$$k \text{ is algebraically closed in } k(\xi).$$

Also, $\zeta$ is clearly transcendental over $k$ and so, by Gauss' lemma, $\varphi(X^n, \zeta) \in k[\zeta][X^n]$ is irreducible over $k(\zeta)$. Hence by the second case, it follows that $\varphi(X^n, \zeta)$ is absolutely irreducible over $k(\zeta)$ if and only if

$$k(\zeta) \text{ is algebraically closed in } k(\zeta)(\xi_1, \xi_2, \ldots, \xi_{n-1}) = k(\xi). \tag{54}$$

Thus it remains to prove that for "large" $p$ there is a $c \in k$ such that $\zeta = \xi_n + c\xi_{n-1}$ satisfies (54).

Since $n-1 \geqslant 2$, we can define $\Sigma'$ as the field of elements of $\Sigma$ which are algebraically dependent over $k(\xi_{n-1}, \xi_n)$. Then, for any $a \in k$, we define $\Omega_a$ to be the field of those elements of $\Sigma$ which are algebraically dependent on $k(\xi_n + a\xi_{n-1})$. Then clearly,

$$k(\xi_{n-1}, \xi_n) \subseteq \Omega_a(\xi_{n-1}) \subseteq \Sigma'. \tag{55}$$

Since

$$\begin{aligned} d = d(\psi) &\geqslant [\Sigma\colon\ k(\xi_2, \ldots, \xi_n)] \\ &\geqslant [\Sigma'(\xi_2, \ldots, \xi_{n-2})\colon\ k(\xi_2, \ldots, \xi_n)] \\ &= [\Sigma'\colon\ k(\xi_{n-1}, \xi_n)], \end{aligned} \tag{56}$$

by our hypothesis concerning the algebraic independence of $\xi_2, \ldots, \xi_{n-2}$ over $k$, it follows that $\Sigma'/k(\xi_{n-1}, \xi_n)$ is a finite separable extension and therefore simple. Thus, there are at most $2^d$ fields $\Omega_a(\xi_{n-1})$ between $\Sigma'$ and $k(\xi_{n-1}, \xi_n)$ and since $p > 2^d$, there are two distinct elements $b, c$ of $k$ such that

$$\Omega_b(\xi_{n-1}) = \Omega_c(\xi_{n-1}),$$

i.e.,

$$\Omega_b(\xi_n + c\xi_{n-1}) = \Omega_c(\xi_n + b\xi_{n-1}). \tag{57}$$

Note that as $k$ is algebraically closed in $\Sigma$ it is certainly algebraically closed in the sub-field $\Omega_b$. Then the main part of the proof ([8], p. 82), which we omit as it is valid for fields $k$ of arbitrary characteristic, is the deduction:

(58) $k$ algebraically closed in $\Omega_b \Rightarrow k(\zeta)$ algebraically closed in $\Omega_b(\zeta)$.

The completion of the argument is now routine, for any element of $\Omega_b(\zeta)$ which is algebraic over $k(\zeta)$ is therefore in $k(\zeta)$. But any element of $\Omega_c$ is algebraic over $k(\zeta)$, and

$$\Omega_c \subseteq \Omega_c(\xi_n + b\xi_{n-1}) = \Omega_b(\zeta). \tag{59}$$

Hence any element of $\Omega_c$ is in $k(\zeta)$, i.e. $\Omega_c = k(\zeta)$ or $k(\zeta)$ is algebraically closed in $k(\xi)$, as required.

**6.** THEOREM 3. *For $n \geqslant 3$ let $f, \psi$ denote elements of $k[X]$, and suppose that*

$$f(X) \not\equiv c \bmod \psi_i(X) \tag{60}$$

*$\forall\, c \in k$ and $\forall$ absolutely irreducible factors $\psi_i(X)$ in $k[X]$ of $\psi(X)$. Then*

$$S_n(f, \psi) = \sum_{x \in k^n,\ \psi(x)=0} e\big(f(x)\big) \ll p^{n-3/2}. \tag{61}$$

**Remark.** The following proof proceeds by induction on $n$ from the case $n = 2$ (Theorem 2), and assumes the result

$$S_n(f, 0) \ll p^{n-1/2} \text{ when } \psi \text{ is identically zero in } k[X].$$



For $n = 1$, this is due to Weil [20] and the elementary inductive extension to general $n$ is due to Uchiyama [18].

Proof. By the lemma of Chalk and Williams [5],

$$|S_n(f, \psi)| \leqslant \sum_{j=1}^{l} |S_n(f, \psi_j)| + O_d(p^{n-2}),$$

where $l \leqslant d(\psi)$ and $\psi_j$ $(j = 1, 2, \ldots, l)$ are the distinct irreducible factors of $\psi(X)$ in $k[X]$. Moreover, if any $\psi_j$ is not absolutely irreducible over $k$, then[6] (cf. [1], Lemma 2 and Theorem 1, Corollary 2)

$$S_n(f, \psi_j) \ll \sum_{\psi_j(x)=0} 1 \ll p^{n-2}.$$

Thus, without loss of generality, we may henceforth assume that

(i) $\psi(X)$ is *itself* absolutely irreducible over $k$ and

(ii)

$$f(X) \not\equiv c \bmod \psi(X), \quad \forall c \in k. \tag{62}$$

This hypothesis and the desired conclusion (61) are clearly unaffected by the application of non-singular linear substitutions on $X$ and, in particular, by permutations of the $X_i$. From our remark about $S_n(f, 0)$ above, the conclusion is immediate in the cases when $f$ and $\psi$ can be rendered "disjoint", i.e., when, after a suitable permutation of the $X_i$,

$$f \in k[X_1, \ldots, X_r], \quad \psi \in k[X_{r+1}, \ldots, X_n], \quad \text{say}$$

and

$$\begin{aligned} S_n(f, \psi) &= S_r(f, 0) \cdot N\big((x_{r+1}, \ldots, x_n) \in k^{n-r} \mid \psi = 0\big) \\ &\ll p^{r-1/2} \cdot p^{n-r-1} = p^{n-3/2}. \end{aligned} \tag{63}$$

We may therefore assume that $f, \psi$ are not of this type and so by a suitable permutation of the $X_i$ $(1 \leqslant i \leqslant n)$ arrange that *both* $f, \psi$ contain $X_1$ and, as $\psi$ is absolutely irreducible over $k$ further ensure that $\psi$ contains $X_n$, unless $\psi$ is linear and of the form $X_1 + c$, where $c \in k$. By (62), the cases where $\psi$ is linear are a trivial consequence of the estimate for $S_{n-1}(f, 0)$ and are excluded henceforth. Hence, by Lemma 4, we know that a suitable shear of the type (46) will ensure that $\psi$ meets the requirements in the hypothesis of Lemma 3. Then, from its conclusion we have

$$|\mathcal{M}| \ll 1, \tag{64}$$

where

$$\mathcal{M} = \{a \in k \mid \psi(X^n, a) \in k[X^n] \text{ not absolutely irreducible over } k\} \tag{65}$$

---

[6] This also follows from [5], as was noted by K. S. Williams.

and from our reduction above we can express $f, \psi$ as elements of $k[X_1][X^1]$:

$$f(X) = f_0(X^1)X_1^e + \ldots + f_e(X^1), \quad e \geqslant 1, \tag{66}$$

$$\psi(X) = \psi_0(X^1)X_1^\delta + \ldots + \psi_\delta(X^1), \quad \delta \geqslant 1 \tag{67}$$

where neither of $f_0, \psi_0$ is identically zero in $k[X^1]$. Now, for a more useful form of our present hypotheses (i) and (ii) (cf. (62)) we introduce the resultant $R(X^1, Z)$ of $f(X)-Z$ and $\psi(X)$ which is obtained by eliminating $X_1$.

Then, by hypothesis (ii),

$$R(X^1, c) \text{ is NOT identically zero in } k[X^1], \quad \forall c \in k \tag{68}$$

or, equivalently, if we view $R(X^1, Z)$ as a polynomial with coefficients $R_t(X_n, Z)$ say, in $k[X_n, Z]$, then

$$\text{for each } c \in k,\ R_t(X_n, c) \text{ identically } 0 \text{ in } k[X_n]\ \forall t, \text{ is impossible.} \tag{69}$$

Consider the effect of the specialization

$$X_n \to a \quad (a \in k) \tag{70}$$

upon $f, \psi$ and note that the following sets

$$E = \{a \in k|\ \psi(X^n, a) \in k[X^1]\}, \tag{71}$$

$$F = \{a \in k|\ f(X^n, a) \in k[X^1]\} \tag{72}$$

(for which they become independent of $X_1$) are small, in the sense that

$$|E| \ll 1, \quad |F| \ll 1. \tag{73}$$

For, each of the sets $\{\psi_\mu^0(X_n)\}, \{f_\lambda^0(X_n)\}$ say, of coefficients of $\psi_0(X^1)$, $f_0(X^1)$, viewed now as polynomials with coefficients in $k[X_n]$, can vanish for at most $O(1)$ values of $a \in k$. We shall also need to know that $\psi(X^n, a)$ is not identically zero in $k[X^n]$ for any $a \in k$. This follows from the fact that $\psi(X)$ is irreducible over $k$ and that if it is regarded as a polynomial with coefficients $\theta_\nu(X_n)$ in $k[X_n]$, then the g.c.d. $\theta_\nu(X_n)$, taken over all $\nu$, is a unit in $k$ and so there can be no $a \in k$ for which $\theta_\nu(a) = 0, \forall \nu$. We collect our "small" sets together and introduce the notation,

$$H = E \cup F \cup \mathcal{N}, \quad G = k - H, \tag{74}$$

where, by (64), (73), we have

$$|H| \ll 1. \tag{75}$$

For our sum,

$$S_n(f, \psi) = \sum_{a \in k} \sum_{\substack{x^n \in k^{n-1} \\ \psi(x^n, a) = 0}} e\big(f(x^n, a)\big) \tag{76}$$



it is convenient to split the summation over $a \in k$ into two parts $\Sigma_1, \Sigma_2$ say according as $a \in H$ or $a \in G$, respectively. Then

$$\Sigma_1 \ll \sum_{a \in H} N\big(x^n \in k^{n-1}|\ \psi(x^n, a) = 0\big) \tag{77}$$

$$\ll p^{n-2}|H| \tag{78}$$

$$\ll p^{n-2}, \tag{78}$$

in view of (75) and our remark about the non-vanishing of $\psi$ under the specialization (70). For the remaining sum $\Sigma_2$ over $G$, two cases have to be distinguished and we define further sets

$$G_1 = \{a \in G|\ \psi(X^n, a)|[f(X^n, a) - c] \text{ in } k[X^n], \text{ for some } c \in k\}, \tag{79}$$

$$G_2 = \{a \in G|\ \psi(X^n, a) \nmid [f(X^n, a) - c] \text{ in } k[X^n], \forall c \in k\} \tag{80}$$

so that $G$ is the disjoint union of $G_1$ and $G_2$. Then

$$\Sigma_2 = \sum_{a \in G_1} + \sum_{a \in G_2} \tag{81}$$

and

$$\sum_{a \in G_2} = \sum_{a \in G_2} \sum_{\substack{x^n \in k^{n-1} \\ \psi(x^n, a) = 0}} e\big(f(x^n, a)\big) \ll p \cdot p^{n-5/2} \tag{82}$$

since our induction hypothesis applies for any $a \in G_2$ (when, of course, $a \notin \mathcal{N}$). The full force of our hypothesis is now required for the sum over the $a \in G_1$, i.e. if $a \in G$,

$$\psi(X^n, a)|\ [f(X^n, a) - c] \text{ in } k[X^n] \Leftrightarrow R_t(a, c) = 0, \forall t. \tag{83}$$

An essential step in the ensuing argument is the identification of the two sets:

$$S_1 = \{(x^n, a, z) \in k^{n-1} \times G_1 \times k|\ \psi(x^n, a) = f(x^n, a) - z = 0\}, \tag{84}$$

$$S_2 = \{(x^n, a, z) \in k^{n-1} \times G_1 \times k|\ \psi(x^n, a) = 0, R_t(a, z) = 0, \forall t\} \tag{85}$$

and this is a direct consequence of the definition of $G_1$ and (83). Then

$$\sum_{a \in G_1} = \sum_{\substack{(x^n, a) \in k^{n-1} \times G_1 \\ \psi(x^n, a) = 0}} e\big(f(x^n, a)\big) \tag{86}$$

$$= \sum_{(x^n, a, z) \in S_1} e(z)$$

$$= \sum_{(x^n, a, z) \in S_2} e(z) \tag{87}$$

$$= \sum_{(a, z) \in \mathcal{H}(G_1)} e(z) \Big\{ \sum_{\substack{x^n \in k^{n-1} \\ \psi(x^n, a) = 0}} 1 \Big\}, \tag{88}$$

on rearranging the order of summation in (87), and where, in general, $\mathscr{R}(S)$ denotes the set defined by

$$\mathscr{R}(S) = \{(a, z) \in k^2 |\ a \in S, R_t(a, z) = 0, \forall t\}. \tag{89}$$

For the inner sum over $x^n \in k^{n-1}$ in (88), we can apply the Corollary to Lemma 3, since $a \in G_1$ and, in particular, $a \notin \mathscr{N}$ so that $\psi(X^n, a)$ is absolutely irreducible over $k$. Hence

$$N\{x^n \in k^{n-1} |\ \psi(x^n, a) = 0\} = p^{n-2} + O(p^{n-5/2}) \tag{90}$$

and the implied constant in the $O$-symbol depends at most on $n$ and $d(\psi)$ (but not on $a$). Combining (88) and (90) and rearranging the terms, we get

$$\sum_{a \in G_1} -p^{n-2} \sum_{(a,z) \in \mathscr{R}(G_1)} e(z) \ll p^{n-5/2} |\mathscr{R}(k)|. \tag{91}$$

But, since not all of the polynomials $R_t(X_n, Z)$ are identically zero in $k[X_n, Z]$,

$$|\mathscr{R}(k)| \ll 1, \tag{92}$$

and so, by (91), it only remains to prove that

$$\sum_{(a,z) \in \mathscr{R}(G_1)} e(z) \ll p^{1/2}. \tag{93}$$

By definition of $H, G_1$ and $G_2$, we know that $\mathscr{R}(k)$ is the disjoint union of $\mathscr{R}(H), \mathscr{R}(G_1)$ and $\mathscr{R}(G_2)$. But, by (80) and (83)

$$\mathscr{R}(G_2) = \emptyset \tag{94}$$

and

$$\sum_{(a,z) \in \mathscr{R}(H)} e(z) \ll 1, \tag{95}$$

since if, for some $a \in H$, the polynomials $R_t(a, Z)$ are constant for all $t$ (i.e. the range of $z$ in the sum is unrestricted), the sum is zero and otherwise, the number of $z \in k$ with $R_t(a, z) = 0, \forall t$ is clearly bounded. From (93), (94) and (95), we have

$$\begin{aligned} \sum_{(a,z) \in \mathscr{R}(G_1)} e(z) &= \sum_{(a,z) \in \mathscr{R}(k)} e(z) - \sum_{(a,z) \in \mathscr{R}(G_2)} e(z) - \sum_{(a,z) \in \mathscr{R}(H)} e(z) \\ &= \sum_{(a,z) \in \mathscr{R}(k)} e(z) + O(1). \end{aligned} \tag{96}$$

Now, not all $R_t(X_n, Z)$ are identically zero in $k[X_n, Z]$ and so we may write

$$R_t(X_n, Z) = R(X_n, Z) R'_t(X_n, Z), \quad \forall t \tag{97}$$



where $R(X_n, Z)$ denotes the g.c.d. of the set of all the $R_t(X_n, Z)$ and is not identically zero in $k[X_n, Z]$. Then

$$\sum_{(a,z) \in \mathscr{R}(k)} e(z) = \sum_{\substack{(a,z) \in k^2 \\ R(a,z)=0}} e(z) + O(1), \tag{98}$$

since (cf. Bezout's theorem (40)), we have

$$N\{(a, z) \in k^2 |\ R'_t(a, z) = 0, \forall t\} \ll 1. \tag{99}$$

Finally, for the sum on the right of (98), we use Theorem 2 to complete our argument; it remains to confirm the hypothesis and for this we note that

$$\begin{aligned} &(Z - c) |\ R(X_n, Z) \text{ for some } c \in k \\ &\quad \Rightarrow (Z - c) |\ R_t(X_n, Z), \quad \forall t \\ &\quad \Rightarrow R_t(X_n, c) \text{ identically 0 in } k[X_n], \quad \forall t, \end{aligned}$$

contrary to (69).

## References


[1] B. J. Birch and D. J. Lewis, *p-adic forms*, J. Indian Math. Soc. 23 (1959), pp. 11–32.

[2] E. Bombieri, *On exponential sums in finite fields*, Amer. J. of Math. 88 (1966), pp. 71–105.

[3] — and H. Davenport, *On two problems of Mordell*, Amer. J. of Math. 88 (1966), pp. 61–70.

[4] J. H. H. Chalk and K. S. Williams, *The distribution of solutions of congruences*, Mathematika 12 (1965), pp. 176–192.

[5] — — *The distribution of solutions of congruences, Corrigendum and Addendum*, Mathematika 16 (1969), pp. 98–100.

[6] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, New York, Math. Surveys, No. VI, A. M. S. Publication 1951 (1963).

[7] M. Eichler, *Introduction to the Theory of Algebraic Numbers and Functions*, New York, London, 1966.

[8] W. V. D. Hodge and D. Pedoe, *Methods of Algebraic Geometry, II*, Cambridge 1952.

[9] H. Hasse, *Theorie der relativ-zyklischen algebraischen Funktionen-körpern, insbesondere bei endleichem Konstantenkörper*, Crelles Journal für Mathematik, 172 (1934), pp. 37–54.

[10] — *Über die Kongruenzzetafunktion*, Sitz. der Preuss. Akad. Wiss. Berlin, Math-Phys. Kl. XVII (1934), pp. 250–263.

[11] — *Bericht über neuere Untersuchungen und Probleme ans der Theorie der algebraischen Zahlkörper*, I, Ia, II, J. Ber. dt. Mat. Verein. 35 (1926), pp. 1–55; 36 (1927), pp. 233–311; Exg. bd. (1930a), pp. 1–204; reprinted: Würzburg–Wien 1965.

[12] S. Lang, *Algebra*, (Addison-Wesley, 1967), Ch. VIII, § 6.

[13] — and A. Weil, *Number of points of varieties in finite fields*, Amer. J. of Math. 76 (1954), pp. 819–827.

[14] E. Noether, *Ein algebraisches Kriterium für absolute Irreducibilität*, Math. Ann. 85 (1922), pp. 26–33.
[15] O. Perron, *Algebra, I*, de Gruyter, 3rd ed., 1951.
[16] F. K. Schmidt, *Analytische Zahlentheorie in Körpern der characteristik p*, Math. Zeitschr. 33 (1931), pp. 1–32.
[17] R. A. Smith, *The distribution of rational points on hypersurfaces defined over a finite field*, Mathematika 17(1970), pp. 328–332.
[18] S. Uchiyama, *On a multiple exponential sum*, Proc. Japan Acad. 32 (1956), pp. 748–749.
[19] B. van der Waerden, *Modern Algebra*, New York 1949, I, Ch. V, § 40.
[20] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci., U. S. A., 34 (1948), pp. 204–207.
[21] — *Sur les courbes algébriques et les variétés qui s'en déduisent*, Paris 1948.
[22] — *On the Riemann Hypothesis for function-fields*, Proc. Nat. Acad. Sci., U. S. A., 27 (1941), pp. 345–347.
[23] — *Sur les critères d'equivalence en géométrie algébrique*, Math. Annalen 128 (1954), pp. 95–127.
[24] — *Foundations of Algebraic Geometry*, New York, A. M. S. Colloq. Pub. 29 (1946).
[25] E. Weiss, *Algebraic Number Theory*, (McGraw–Hill, 1963), 4–9.
[26] K. S. Williams, *Pairs of consecutive residues of polynomials*, Canad. J. of Math. 19 (1967), pp. 655–666 (sec. (1.15)).
[27] O. Zariski, *Pencils on an algebraic variety and a new proof of a theorem of Bertini*, Trans. Amer. Math. Soc. 50 (1941), pp. 48–70.

UNIVERSITY OF TORONTO
Toronto, Canada

*Received on 8. 3. 1970*

ACTA ARITHMETICA
XVIII (1971)

# The multiplicity of partial coverings of space

by

L. Few (London)

**1.** Let $K$ be a convex body in $n$-dimensional space. Consider a system of translates of $K$ such that no point of space belongs to more than $h-1$ of the translates. This system is an $(h-1)$-fold packing. Let the proportion of space belonging to at least one of the bodies be $\delta$, and let

$$k = -\log(1-\delta). \tag{1}$$

We prove that, provided $n$ is sufficiently large, and

$$n4^{-n} < \delta < 1-e^{-n/6}, \tag{2}$$

there is such a system with $h-1 = [l]$, where

$$l = \frac{n\log 4(n+1) - 2ke - \log\delta - \frac{1}{2}\log n + n}{\log n - \log 2ke}, \tag{3}$$

and we also prove that the density of the system is greater than $2k$ and $\sim 2k$.

These results are illustrated by examples in § 7.

This paper uses methods of Erdös and Rogers [1], and the notation of that paper is used where convenient.

**2.** In this section we take $K$ to be a Lebesgue measurable set with finite positive measure $V$. Let $\Lambda$ be the lattice of all points with integral coordinates, and suppose that all the distinct translates of $K$ by the vectors of $\Lambda$ are disjoint.

Let the $N$ points $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_N$ be chosen at random in the cube $C$ of points $\boldsymbol{x}$ with

$$0 \leqslant x_i \leqslant 1 \quad (i = 1, 2, \ldots, n).$$

Consider the system of sets

$$K + \boldsymbol{x}_i + \boldsymbol{g} \quad (1 \leqslant i \leqslant N,\ \boldsymbol{g} \in \Lambda) \tag{4}$$

and, for $0 \leqslant h \leqslant N$, the set $E_h$ of points belonging to just $h$ of the sets (4). Then, given $K$ and $h$, the density $\delta(E_h)$ of the set $E_h$ is a function of