# Pacific Journal of Mathematics

# STRICTLY LOCAL SOLUTIONS OF DIOPHANTINE EQUATIONS

MARVIN J. GREENBERG

Vol. 51, No. 1

November 1974

# STRICTLY LOCAL SOLUTIONS OF DIOPHANTINE EQUATIONS

## MARVIN J. GREENBERG

For any system f of Diophantine equations, there exist positive integers C(f), D(f) with the following properties: For any nonnegative integer n, for any prime p, if v is the p-adic valuation, and if a vector x of integers satisfies the inequality

$$v(f(x)) > C(f)n + v(D(f))$$

then there is an algebraic p-adic integral solution y to the system f such that

$$v(x-y) > n \; .$$

This theorem is proved by techniques of algebraic geometry in the more general setting of Noetherian domains of characteristic zero. When f is just a single equation, the method of Birch and McCann gives an effective determination of C(f)and D(f).

Let R be a Noetherian integral domain, K its field of fractions. We will consider *Henselian discrete valuation rings*  $R_v$  (see [4]) containing R, where v is the valuation normalized so that  $v(R_v)$  is the set of nonnegative integers (plus  $\infty$ ). If  $f = (f_1, \dots, f_r)$  is a system of r polynomials in s variables with coefficients in R, and x is an s-tuple with coordinates in an extension ring of R, we set  $f(x) = (f_1(x), \dots, f_r(x))$ . We define the valuation of an r-tuple (or s-tuple) to be the minimum of the valuations of its components.

THEOREM. Assume R has characteristic zero. For each system f of polynomials with coefficients in R, there exists an integer  $C(f) \ge 1$  and an element  $D(f) \ne 0$  in R with the following property: For any Henselian discrete valuation ring  $R_v$  containing R, and any nonnegative integer n, if an s-tuple x with components in R satisfies the inequality

(1) 
$$v(f(x)) > C(f)n + v(D(f))$$

then there is a zero y of f in  $R_v$  such that

$$v(x-y) > n$$
.

In particular, if R is the ring of algebraic integers in a number field, and we take n = 0, S = set of primes dividing D(f), then we recover Greenleaf's theorem [3] to the effect that if  $p \notin S$ , then every zero of  $f \mod p$  may be refined to an actual zero of f in the p-adic integers — in fact, to an actual zero of f in the *algebraic* p-adic integers. The theorem above strengthens Greenleaf's result by giving information about the exceptional primes  $p \in S$  and by providing a precise linear estimate of how close the actual zero y is to the approximate zero x. The hypothesis that R have characteristic zero is required by Greenleaf's counterexample ([3], p. 30).

*Proof.* Let fR[X] be the ideal in the polynomial ring  $R[X_1, \dots, X_s]$  generated by  $f_1(X), \dots, f_r(X)$ , and let V be the algebraic set in affine s-space over K which is the locus of zeroes of f.

Step 1. We may assume fR[X] is equal to its own radical. For let g be a system of polynomials generating the radical, and suppose the mth power of the radical is contained in fR[X]. If C(g), D(g)are invariants for g, set

$$C(f) = mC(g)$$
,  $D(f) = D(g)^m$ .

Then inequality (1) implies that for any polynomial  $h \in fR[X]$ , say  $h = h_1 f_1 + \cdots + h_r f_r$ , we have

$$egin{aligned} v(h(x)) &\geq \min_i \left[ v(h_i(x)) + v(f_i(x)) 
ight] \ &\geq \min_i v(f_i(x)) = v(f(x)) > C(f)n + v(D(f)) \ . \end{aligned}$$

In particular, for  $h = g_j^m$ , with  $g_j$  in g, we get

$$mv(g_j(x)) > m[C(g)n + v(D(g))]$$
 for all j

so that there is a zero y of g in  $R_v$  such that

$$v(x-y) > n$$
.

Since y is also a zero of f, we have found the invariants for f.

Step 2. Granted that fR[X] is its own radical, we may further assume fR[X] is a prime ideal. Otherwise, it is an intersection of finitely many prime ideals, so by induction on the number of these, we may assume fR[X] is the intersection of two ideals generated by systems g, g' for which invariants C(g), C(g'), D(g), D(g') have already been found. We set

$$egin{aligned} C(f) &= \max\left(2C(g),\,2C(g')
ight) \ D(f) &= D(g)^2D(g')^2 \ . \end{aligned}$$

Then for each  $g_i \in g$  and  $g'_j \in g'$ , we have  $g_i g'_j \in fR[X]$ , so that as before, inequality (i) implies

$$v(g_i(x)) + v(g'_i(x)) \ge v(f(x)) > C(f)n + v(D(f))$$
.

Suppose that for one index j,  $v(g'_i(x)) < 1/2 v(f(x))$ . Fixing that j and letting i vary, we get  $v(g_i(x)) > 1/2 v(f(x))$  for all indices i, so that

$$v(g(x)) > rac{1}{2} \left[ C(f) n \, + \, v(D(f)) 
ight] \, .$$

By definition of C(f) and D(f), the term on the right is at least as big as C(g)n + v(D(g)), so that there is a zero y of g — a fortiori of f — in  $R_v$  such that v(x - y) > n. If, on the other hand,  $v(g'(v)) \ge$ 1/2 v(f(x)), the same argument gives a zero y of g' — a fortiori of f — in  $R_v$  such that v(x - y) > n.

Step 3. Assuming fR[X] is a prime ideal, we proceed by induction on the dimension m of the irreducible K-variety V. If V is empty, let D(f) be any nonzero constant in fR[X], and let C(f) = 1. Then the inequality (1) is never satisfied for any n, v, and x, so the theorem is vacuously true. Assume now that V is nonempty and the theorem established in dimensions less than m. Let J be the Jacobian matrix of f,  $\Delta$  the system of minors  $\Delta_{(i)(j)}$  of order s - mtaken from J. Since the characteristic is zero, the locus of common zeros of  $\Delta$  and f is a proper K-closed subset of V (the singular locus); by inductive hypothesis, there are invariants C', D' for the system  $\Delta$  plus f.

If (i) is a collection of s - m indices  $\leq r, f_{(i)}$  the corresponding system of s - m polynomials taken out of f, let  $V_{(i)}$  be the algebraic set of zeros of  $f_{(i)}$  and let  $W_{(i)}$  be the union of the K-irreducible components of  $V_{(i)}$  which have dimension m and are different from V. Let  $g_{(i)}$  be a system of generators for the ideal of  $W_{(i)}$  in R[X]; by inductive hypothesis, there are invariants  $C_{(i)}, D_{(i)}$  for the system  $g_{(i)}$  plus f (since  $V \cap W_{(i)}$  is its locus). The results of Zariski (Trans. A.M.S. 62 (1947), pp. 14 and 28-29) tell us that if x is a point of  $V_{(i)}$  such that for some (j)

$$\Delta_{(i)(j)} \neq 0$$

then x lies on exactly one component of  $V_{(i)}$ , that component having dimension m.

We now set

$$C(f) = C' + \max \{C', C_{(k)} \text{ all } (k)\}$$
  
 $D(f) = (D')^2 \prod_{(k)} D_{(k)}$ 

so that  $v(D(f)) \ge v(D') + \max \{v(D'), v(D_{(k)}) \text{ all } (k)\}$ . Assuming inequality (1), we then have three possibilities:

I.  $v(\varDelta(x)) > C'n + v(D')$ . By inductive hypothesis, there is a singular zero y of f in  $R_v$  such that v(x - y) > n.

II. For some (i),  $v(g_{(i)}(x)) > C_{(i)}n + v(D_{(i)})$ . By inductive hypothesis, there is a zero y of f in  $R_v$  (lying on  $V \cap W_{(i)}$ ) such that v(x - y) > n.

III. For some (i) and (j),

$$v(\mathcal{A}_{(i)(j)}(x)) \leq C'n + v(D')$$

and for every (k), there is a polynomial  $\gamma_{(k)}$  in the system  $g_{(k)}$  for which

$$v(\gamma_{(k)}(x)) \leq C_{(k)}n + v(D_{(k)})$$
.

By Hensel's Lemma, there is a zero y of the system  $f_{(i)}$  in  $R_{y}$  such that

 $v(y - x) > \max \{C'n + v(D'), C_{(k)}n + v(D_{(k)}) \text{ all } k\}$ .

In that case  $g_{(k)}(y) \neq 0$ , for all (k), since

$$v(\gamma_{(k)}(y)) = v(\gamma_{(k)}(x))$$
.

Thus  $y \notin W_{(k)}$  for any (k). As we also have

$$\Delta_{(i)(j)}(y) \neq 0$$

y must lie on V, so y is a zero of f.

Note 1. In the last part of the above argument we used a version of Hensel's Lemma which is a strengthening of Lemma 2, p. 63 of [2]. It says that if  $R_v$  is a Henselian discrete valuation ring with maximal ideal m, F a system of r polynomials in s variables with coefficients in  $R_v$ ,  $r \leq s$ , J its Jacobian matrix,  $x \in R_v^s$ ,  $a \in R_v$  so that

$$F(x) \equiv 0 \qquad (\bmod a e^2 \mathfrak{m})$$

where e = D(x), D being a minor of order r taken from J, then there exists  $y \in R_v^s$  such that F(y) = 0 and

$$y \equiv x \pmod{aem}$$
.

(Since h = v(a) is an arbitrary integer, we have applied this lemma by taking  $F = f_{(i)}$  and

$$h = \max \{C'n + D', C_{(k)}n + D_{(k)} \text{ all } k\} - v(A_{(i)(j)}(x))$$

in part III above.) The idea for proving this stronger Hensel's Lemma is the same as in [2], pp. 63-64, reducing to the case r = s, applying Taylor's formula to F(aeX), obtaining F(aeX) = aeJ(0)H(X), and if  $y' \in \mathfrak{m}^s$  is zero of H as in Lemma 1 of [2], then y = aey' is the zero we seek. Note 2. Birch and McCann [1] proved the special case of the theorem where R is a unique factorization domain, and f is a single polynomial (in several variables). Their method has the advantage of providing an effective (but impractical) method of calculating D(f) when f is a single polynomial. If f involves s variables, they use the notation  $D_s(f)$  because their invariant is constructed by induction on s. They omit the definition of  $C_s(f) = C(f)$ , which can be given inductively on s as follows: If s = 1,  $C_i(f) = d(f)$ , where d(f) is the degree of f. If s > 1, denote by  $f_i$  the polynomial f regarded as having coefficients in  $R[X_i]$  and involving the other s - 1 variables. Then

$$C_{s}(f) = \max_{1 \leq i \leq s} \{C_{s-1}(f_{i}) + d(D_{s-1}f_{i})\}$$

with  $d(D_{s-1}f_i)$  being the degree in  $X_i$  of  $D_{s-1}f_i \in R[X_i]$ .

The proof by Birch and McCann then goes by induction on s. However, there is an error in the inductive step (their equation  $D_{n-1}(\phi) = g_1(a_1)$  does not always hold, as is shown by the polynomial  $f(X_1, X_2) = X_2^2 - X_1^2$ , with  $a_1 = 0$ , where  $g_1(a_1) = 0$  while  $D_1(\phi) = 1$ ). This error can be rectified by proving the following result and its corollary, since the inequality in the corollary is all they really need for their argument.

SPECIALIZATION THEOREM. Let R be a unique factorization domain of characteristic zero. Given  $f \in R[X_0, X_1, \dots, X_s]$  and  $a_0 \in R$ . Denote by a bar the specialization obtained by substituting  $a_0$  for  $X_0$ . Let  $f_0$  be f regarded as a polynomial in the variables  $X_1, \dots, X_s$  with coefficients in  $R[X_0]$ . Let  $D_s f_0 \in R[X_0]$  and  $D_s \overline{f_0} \in R$  be the invariants defined by Birch-McCann. If

 $\overline{D_s f_{\scriptscriptstyle 0}} 
eq 0$ 

then  $\overline{D_s f_0}$  is divisible by  $D_s \overline{f_0}$  and they have the same irreducible factors.

COROLLARY. For any valuation v nonnegative on R,

$$v(D_s ar{f}_{\scriptscriptstyle 0}) \leqq v(\overline{D_s f_{\scriptscriptstyle 0}})$$
 .

2. Proof of the specialization theorem and the main theorem for the invariant of Birch-McCann. Recall how  $D_s(f)$  is defined: For any polynomial g in one variable, A(g) is the leading coefficient of g, d(g) is its degree, and

$$rg = g/(g, g')$$

where (g, g') is the greatest common divisor of g and its derivative g'. Thus rg is the primitive polynomial having the same roots as g but all taken with multiplicity one.  $\Delta(g)$  is the discriminant of g; if g has the linear factorization

$$g(X) = A(g) \prod_{i=1}^{d} (X - \alpha_i)$$

then

$$arDelta(g) = A^{\scriptscriptstyle 2(d-1)} \prod_{i < j} (lpha_i - lpha_j)^{\scriptscriptstyle 2}$$
 .

Suppose f is a polynomial in s variables  $X_1, \dots, X_s$  and  $g_i$  is a polynomial in  $X_i$  only. Let  $d(g_i) = d_i$ , and let  $\alpha_{ij}$ , with  $1 \leq j \leq d_i$ , be the roots of  $g_i$  counted with their multiplicities. Then the *eliminant*  $E(Z) = E(f; g_1, \dots, g_s)(Z)$  is the polynomial in Z of degree  $d(E) = \prod d_i$  given by

$$E(Z) = \prod_{i} A(g_{i})^{d(E)d(f)/d_{i}} \prod_{(j)} \{Z - f(lpha_{1j_{1}}, \cdots, lpha_{sj_{s}})\}$$

Inductively,  $D_s(f)$  is then defined as follows: If s = 1,  $D_1(f) = A(f)^{(d-1)d^2} \Delta(rf)^d$ . If s > 1, set  $g_i = D_{s-1}(f_i)$ , where  $f_i$  has been defined before as f regarded as a polynomial in the s - 1 variables other than  $X_i$ ; let E be  $E(f; g_1, \dots, g_s)$ . Then

$$D_s(f) = egin{cases} \prod_i \, D_{\scriptscriptstyle 1}(g_i) \{A(E)^{d(E)} E(0)\}^{d(g_i)} & ext{if} \; E(0) 
eq 0 \ \prod_i \, D_{\scriptscriptstyle 1}(g_i) D_{\scriptscriptstyle 1}(E)^{d(g_i)} & ext{if} \; E(0) = 0 \ . \end{cases}$$

We will prove the Specialization Theorem by induction on s.

Case s = 1. Let  $f_0(X_1) = A(f_0)X_1^d + \cdots$ , and let  $(rf_0)(X_1) = A(rf_0)X_1^\delta + \cdots$ , so that  $\delta \leq d$  and  $A(rf_0)$  divides  $A(f_0)$ . Since by hypothesis  $\overline{D_1 f_0} \neq 0$ , we have  $\overline{A(f_0)} \neq 0$ , so  $\overline{A(f_0)} = A(\overline{f_0})$  and  $\overline{f_0}$  has the same degree d in  $X_1$ . Also  $\overline{d(rf_0)} = d(\overline{rf_0}) \neq 0$ , so  $\overline{rf_0}$  has the same degree  $\delta$  and only simple roots, but may not be primitive. Let c be the greatest common divisor of the coefficients of  $\overline{rf_0}$ ; then  $\overline{rf_0} = c(r\overline{f_0})$ . Now  $d(\overline{rf_0})$  is homogeneous of degree  $2(\delta - 1)$  in the coefficients of  $\overline{rf_0}$ . Thus

$$\overline{D_1f_0}=A(\overline{f_0})^{(d-1)d^2} \varDelta(c(r\overline{f_0}))^d=c^{2d\,(\,\delta-1)}D_1\overline{f_0}\;.$$

The theorem then follows from the fact that c divides  $A(\overline{f_0})$  which divides  $A(\overline{f_0})$  which divides  $D_1\overline{f_0}$ .

To carry out the induction, we will need to strengthen our result for s = 1 with the following lemma.

LEMMA 1. Let g, h be polynomials in one variable Y which satisfy

$$g = c_1^{k_1} \cdots c_s^{k_s} h$$

with each  $c_i$  dividing h, and  $k_i \ge 1$ . Then  $D_1g$  and  $D_1h$  satisfy the same type of relationship:

$$D_1g = C_1^{m_1} \cdots C_t^{m_t} D_1h$$

with each  $C_i$  dividing  $D_1h$ .

*Proof.* Let e = degree h,  $\gamma_i = \text{degree } c_i$ , so that degree  $g = \varepsilon = e + \sum_i k_i \gamma_i$ , and

$$A(g) = A(c_1)^{k_1} \cdots A(c_s)^{k_s} A(h)$$
.

Since each  $c_i$  divides h, g, and h have the same irreducible factors, so that rg = rh. Hence

$$D_{\scriptscriptstyle 1}g = A(g)^{\scriptscriptstyle(\mathfrak{c}-1)\mathfrak{c}^2} arDelta(rg)^{\scriptscriptstyle arepsilon} = (\prod_i A(c_{\scriptscriptstyle arphi})^{k_i})^{\scriptscriptstyle(\mathfrak{c}-1)\mathfrak{c}^2} A(h)^{\scriptscriptstyle(\mathfrak{c}-1)\mathfrak{c}^2} arDelta(rh)^{\scriptscriptstyle arepsilon} \; .$$

Now  $D_1h = A(h)^{(e-1)e^2} \varDelta (rh)^e$ , and if we write  $(\varepsilon - 1)\varepsilon^2 = (e-1)e^2 + m$ we get

$$D_{\scriptscriptstyle 1}g = (\prod_i A(c_i)^{k_i})^{(arepsilon-1)arepsilon^2} A(h)^{{}^m\!arepsilon}(rh)^{arepsilon-arepsilon} D_{\scriptscriptstyle 1}h \; .$$

Since  $A(c_i)$ , A(h),  $\Delta(rh)$  each divide  $D_1h$ , the lemma is proved.

The inductive step: By definition,

$$egin{aligned} D_s f_0 &= \sum\limits_{i=1}^s D_1(g_i) M^{d(g_i)} \ D_s \overline{f_0} &= \sum\limits_{i=1}^s D_1(g_i^*) M^{*d(g_i^*)} \end{aligned}$$

where  $g_i = D_{s-1}f_{0i}$ ,  $f_{0i}$  being  $f_0$  regarded as a polynomial in the variables  $X_j$  with  $j \neq i, j \geq 1$  (so that the coefficients of  $f_{0i}$  are polynomials in  $X_0$  and  $X_i$ );  $g_i^* = D_{s-1}(\overline{f_0})_i$  is defined similarly. Also,

$$M = egin{cases} A(E)^{d(E)} E(0) & ext{if} \ E(0) 
eq 0 \ D_1(E) & ext{if} \ E(0) = 0 \end{cases}$$

where  $E = E(f_0; g_1, \cdots, g_s)$ ; and

$$M^* = egin{cases} A(E^*)^{d(E^*)}E^*(0) & ext{if} \ E^*(0) 
eq 0 \ D_1(E^*) & ext{if} \ E^*(0) = 0 \end{cases}$$

where  $E^* = E(\overline{f_0}; g_1^*, \dots, g_s^*)$ . Our hypothesis is  $\overline{D_s f_0} \neq 0$ , so that  $\overline{D_i(g_i)} \neq 0$  for all *i* and  $\overline{M} \neq 0$ .

Since  $\overline{g_i} \neq 0$  (because  $\overline{A(g_i)}$ , which is a factor of  $\overline{D_1g_i}$ , is not zero), and  $\overline{f_{0i}} = (\overline{f_0})_i$ , the inductive hypothesis provides us with  $c_i \in R[X_i]$ such that

$$\overline{g_i} = c_i g_i^*$$

with each irreducible factor of  $c_i$  being a factor of  $g_i^*$ . By Lemma 1,

$$D_1\overline{g_i} = C_i D_1 g_i^*$$

with each irreducible factor of  $C_i$  dividing  $D_1g_i^*$ . The step n = 1 already proved yields

$$\overline{D_{\scriptscriptstyle 1}g_{\scriptscriptstyle i}}=B_iD_{\scriptscriptstyle 1}\overline{g_{\scriptscriptstyle i}}$$

with each irreducible factor of  $B_i$  dividing  $D_i \overline{g_i}$ . Combining gives

$$\overline{D_{\scriptscriptstyle 1}g_{\scriptscriptstyle i}}=B_iC_iD_{\scriptscriptstyle 1}g_i^*$$

so that  $\overline{D_1g_i}$  and  $D_1g_i^*$  have the same irreducible factors.

The condition  $\overline{A(g_i)} \neq 0$  implies  $d(g_i) = d(\overline{g_i})$ , and since  $g_i^*$  divides  $\overline{g_i}, d(\overline{g_i}) \geq d(g_i^*)$ . As

$$\overline{D_sf_0}=\prod\limits_{i=1}^s\overline{D_1g_i}\ ar{M}^{d(g_i)}$$

the theorem will be proved if we can show  $M^*$  divides  $\overline{M}$  and they have the same irreducible factors.

 $\overline{M}$  is the specialization of M and is given by the same formula as M with the specialization  $\overline{E}$  of E taking the place of E. Now the function E, like  $\Delta$ , commutes with specialization, so we have

$$\overline{E}\,=\,E(\overline{f_{\scriptscriptstyle 0}};\,\overline{g_{\scriptscriptstyle 1}},\,\cdots,\,\overline{g_{\scriptscriptstyle s}})\,=\,E(f_{\scriptscriptstyle 0};\,c_{\scriptscriptstyle 1}g_{\scriptscriptstyle 1}^*,\,\cdots,\,c_{\scriptscriptstyle s}g_{\scriptscriptstyle s}^*)\;.$$

Notice also that if  $E(0) \neq 0$  so  $M = A(E)^{d(E)}E(0)$ ,  $\overline{M} \neq 0$  implies  $\overline{A(E)} \neq 0$ , so  $\overline{A(E)} = A(\overline{E})$ , and  $\overline{E(0)} \neq 0$ , so  $\overline{E}(0) \neq 0$ . On the other hand, if E(0) = 0, then  $M = D_1(E)$ , and  $\overline{M} \neq 0$  implies again  $\overline{A(E)} \neq 0$ , so again  $\overline{A(E)} = A(\overline{E})$  and  $d(E) = d(\overline{E})$ .

The problem reduces to examining the relation between  $\overline{E} = E(\overline{f}_0; c_1g_1^*, \dots, c_sg_s^*)$  and  $E^* = E(\overline{f}_0; g_1^*, \dots, g_s^*)$  given that every root of  $c_i$  is a root of  $g_i^*$ .

Note first that  $A(E^*) = \prod_i A(g_i^*)^{\delta_i d(\overline{f}_0)}$ , where  $\delta_i = \prod_{j \neq i} d(g_j^*)$ . If  $\varepsilon_i = \prod_{j \neq i} (d(g_j^*) + d(c_j))$ , then write  $\varepsilon_i = \delta_i + \gamma_i$ , so that

$$A(ar{E}) = A(E^*) \prod A(c_i)^{arepsilon_i d(ar{f}_0)} A(g_i^*)^{arphi_i d(ar{f}_0)}$$

Since every irreducible factor of  $c_i$  is an irreducible factor of  $g_i^*$ , every irreducible factor of  $A(c_i)$  is an irreducible factor of  $A(g_i^*)$ , so the above expression shows that  $A(\bar{E})$  and  $A(E^*)$  have the same irreducible factors.

Thus in the case where  $M = A(E)^{d(E)}E(0)$ , we are reduced to proving that  $\overline{E}(0)$  is divisible by  $E^*(0)$  and they have the same irreducible factors. This will follow from the formula

$$E(f; gh, g_2, \dots, g_s) = E(f; g, g_2, \dots, g_s)E(f; h, g_2, \dots, g_s)$$

whose proof is an easy exercise. From this formula we see that the constant term of  $E(f; g_1, g_2, \dots, g_s)$  is just a product of the constant terms of the various  $E(f; p_1, p_2, \dots, p_s)$ , where  $p_i$  runs through the irreducible factors of  $g_i$  for each  $i = 1, \dots, s$ . Hence  $\overline{E}(0)$  is divisible by  $E^*(0)$  with the same irreducible factors.

Consider finally the case where  $M = D_1(E)$ . Since  $\overline{E}$  is divisible by  $E^*$  with the same irreducible factors, it follows from Lemma 1 that  $D_1(\overline{E})$  is divisible by  $D_1(E^*)$  with the same irreducible factors. The proof for the case s = 1 showed that  $\overline{D_1(E)}$  is divisible by  $D_1(\overline{E})$ with the same irreducible factors.

Thus in both cases  $\overline{M}$  is divisible by  $M^*$  with the same irreducible factors.

Having demonstrated the Specialization Theorem, we can now prove that the Birch-McCann invariant  $D_s(f)$  and the other invariant  $C_s(f)$  defined inductively by

$$egin{aligned} C_{\scriptscriptstyle 1}(f) &= d(f) \quad ext{if} \quad s = 1 \ C_{\scriptscriptstyle s}(f) &= \max_{1 \leq i \leq s} \left\{ C_{\scriptscriptstyle s-1}(f_i) + d(D_{\scriptscriptstyle s-1}f_i) 
ight\} \end{aligned}$$

satisfy our main theorem, if R is a unique factorization domain.

*Proof.* For s = 1 this is Birch-McCann's Theorem with  $\underline{Z}$  and  $o_p$  replaced by R and  $R_v$ . The proof goes over word-for-word because v has a unique extension to the algebraic closure of the field of fractions of  $R_v$  (as follows from Nagata, *Local Rings*, statement (30.5), p. 105). Notice also that in this case (s = 1), the zero y = b is unique.

For s > 1, we proceed by induction on s. Take  $f \in R[X_0, X_1, \dots, X_s]$ ,  $a \in R^{s+1}$ , and let  $\overline{f_0}(X_1, \dots, X_s) = f(a_0, X_1, \dots, X_s)$ , and similarly denote throughout by a bar the result of substituting  $a_0$  for  $X_0$ . Now  $D_s f_0 \in R[X_0]$  so can be written  $g_0(X_0)$ . Suppose

$$v(f(a)) > C_s(\overline{f_0})n + v(D_s\overline{f_0})$$
.

Then the inductive hypothesis gives us a zero  $b \in R^s_v$  of  $\overline{f_0}$  such that  $v(a_i - b_i) > n$  for  $i = 1, \dots, s$ ; hence  $(a_0, b_1, \dots, b_s)$  is the required zero for f. Otherwise

$$v(f(a)) \leq C_s(\overline{f_0})n + v(D_s\overline{f_0})$$
.

In this inequality we propose to replace  $C_s(\overline{f_0})$  by  $C_s(f_0)$  and  $D_s\overline{f_0}$  by  $\overline{D_sf_0} = g_0(a_0)$ . If  $g_0(a_0) = 0$ , we get infinity on the right side. So

suppose  $g_0(a_0) \neq 0$ . Then by the corollary to the Specialization Theorem,  $v(D_s\overline{f_0}) \leq v(\overline{D_sf_0}) = v(g_0(a_0))$ . We need

Addendum to Specialization Theorem. Under the same hypotheses,  $C_s(\overline{f_0}) \leq C_s(f_0)$ .

Proof by induction on s: For s = 1,  $C_1$  is just the degree in the variable  $X_1$ , which stays the same or decreases under specialization. Assume the result for s - 1. Then  $C_{s-1}(\overline{f_{0i}}) \leq C_{s-1}(f_{0i})$  for all  $i = 1, \dots, s$ . In the notation of the proof of the Specialization Theorem,  $\overline{D_{s-1}f_{0i}} = \overline{g_i} = c_i g_i^* = c_i D_{s-1}\overline{f_{0i}}$ , so that

$$d(D_{s-1}\overline{f_{0i}}) \leqq d(\overline{g_i}) = d(g_i) = d(D_{s-1}f_{0i})$$
 .

So by definition of  $C_s$ ,  $C_s(\overline{f_0}) \leq C_s(f_0)$ , proving the addendum.

We have thus obtained, arguing with respect to any other variable  $X_i$  as we have for  $X_0$ , the inequality

$$(2) v(f(a)) \leq C_s(f_i)n + v(g_i(a_i))$$

for all  $i = 0, 1, \dots, s$ . Combining with our hypothesis (1) on v(f(a)), with a = x, we obtain

$$(3) \qquad \qquad [C_{s+1}(f) - C_s(f_i)]n + v(D_{s+1}f) < v(g_i(a_i))$$

for all  $i = 0, 1, \dots, s$ , where by definition of  $C_{s+1}(f)$ , the coefficient of n in the left side is nonnegative, hence

$$(4)$$
  $v(D_{s+1}f) < v(g_i(a_i))$ 

for all  $i = 0, 1, \dots, s$ .

Arguing exactly as in Birch-McCann, we next show that inequality (4) implies that for every root  $\alpha = (\alpha_0, \dots, \alpha_s)$  of  $(g_0, \dots, g_s)$  such that  $v(\alpha - \alpha) > v(M)$  — and there exist such roots by (4) and the theorem for 1 variable applied s + 1 times — we must have  $f(\alpha) = 0$ . Thus E(0) = 0, and hence  $M = D_1(E)$ .

By definition of  $C_{s+i}$ , the coefficient of n in inequality (3) is at least equal to  $d(g_i)$ , and by definition of  $D_{s+i}$ , we have  $v(D_{s+i}f) \ge v(D_ig_i)$  for all i. So we can apply the theorem for one variable to obtain a unique zero  $\alpha_i$  of  $g_i$  such that  $v(a_i - \alpha_i) > n$ , for each  $i = 0, 1, \dots, s$ .

Applying the definition of  $D_{s+1}$  again and using inequality (4), we obtain

$$d(g_i)v(M) + v(D_{\scriptscriptstyle 1}g_i) < v(g_i(a_i))$$

for all i, hence by the theorem for one variable again there is a

unique zero  $\beta_i$  of  $g_i$  in  $R_v$  such that  $v(a_i - \beta_i) > v(M)$  for each i. Define

$${\gamma}_{\scriptscriptstyle i} = egin{cases} lpha_i & ext{if} \;\; n \geqq v(M) \ eta_i & ext{if} \;\; n \leqq v(M) \;. \end{cases}$$

Then, as remarked before, we must have  $f(\gamma) = 0$ , which proves the theorem.

### References

1. B. J. Birch and K. McCann, A criterion for the p-adic solubility of Diophantine equations, Quart. J. Math., Oxford, (2), 18 (1967), 59-63.

2. M. J. Greenberg, Rational points in Henselian discrete valuation rings, Publications Mathématiques, No. **31** (1966), I.H.E.S., 59-64.

3. N. Greenleaf, Irreducible subvarieties and rational points, Amer. J. Math., 87 (1965), 25-31.

4. M. Raynaud, Anneaux Locaux Henséliens, Lecture Notes in Mathematics 169, Springer-Verlag, 1970.

Received November 20, 1972.

UNIVERSITY OF CALIFORNIA, SANTA CRUZ

## PACIFIC JOURNAL OF MATHEMATICS

## EDITORS

RICHARD ARENS (Managing Editor) University of California Los Angeles, California 90024 J. DUGUNDJI\* Department of Mathematics University of Southern California Los Angeles, California 90007

D. GILBARG AND J. MILGRAM Stanford University Stanford, California 94305

#### ASSOCIATE EDITORS

E. F. BECKENBACH

University of Washington Seattle, Washington 98105

R. A. BEAUMONT

B. H. NEUMANN

K. Yoshida

### SUPPORTING INSTITUTIONS

F. WOLF

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 NAVAL WEAPONS CENTER

\* C. R. DePrima California Institute of Technology, Pasadena, CA 91109, will replace J. Dugundji until August 1974.

Printed in Japan by Intarnational Academic Printing Co., Ltd., Tokyo, Japan

# Pacific Journal of MathematicsVol. 51, No. 1November, 1974

Zvi Arad, $\pi$ -homogeneity and $\pi'$ -closure of finite groups Ivan Baggs, A connected Hausdorff space which is not contained in a maximal	1
connected space	11
Eric Bedford, <i>The Dirichlet problem for some overdetermined systems on the unit</i> ball in $C^n$	19
R. H. Bing, Woodrow Wilson Bledsoe and R. Daniel Mauldin, <i>Sets generated by rectangles</i>	27
Carlo Cecchini and Alessandro Figà-Talamanca, <i>Projections of uniqueness for</i> $L^{p}(G)$	37
Gokulananda Das and Ram N. Mohapatra, <i>The non absolute Nörlund summability of</i> <i>Fourier series</i>	49
Frank Rimi DeMeyer, <i>On separable polynomials over a commutative ring</i>	57
Richard Detmer, <i>Sets which are tame in arcs in</i> $E^3$	67
William Erb Dietrich, Ideals in convolution algebras on Abelian groups	75
Bryce L. Elkins, <i>A Galois theory for linear topological rings</i>	89
William Alan Feldman, A characterization of the topology of compact convergence	100
on C(X)	109
Hillel Halkin Gershenson, A problem in compact Lie groups and framed	101
cobordism	121
Samuel R. Gordon, <i>Associators in simple algebras</i>	131
Marvin J. Greenberg, <i>Strictly local solutions of Diophantine equations</i>	143
Jon Craig Helton, <i>Product integrals and inverses in normed rings</i>	155
Domingo Antonio Herrero, Inner functions under uniform topology	167
Jerry Alan Johnson, <i>Lipschitz spaces</i>	177
Marvin Stanford Keener, Oscillatory solutions and multi-point boundary value functions for certain nth-order linear ordinary differential equations	187
John Cronan Kieffer, A simple proof of the Moy-Perez generalization of the Shannon-McMillan theorem	203
Joong Ho Kim, <i>Power invariant rings</i>	207
Gangaram S. Ladde and V. Lakshmikantham, <i>On flow-invariant sets</i>	215
Roger T. Lewis, Oscillation and nonoscillation criteria for some self-adjoint even order linear differential operators	221
Jürg Thomas Marti, On the existence of support points of solid convex sets	235
John Rowlay Martin, <i>Determining knot types from diagrams of knots</i>	233
James Jerome Metzger, Local ideals in a topological algebra of entire functions	241
characterized by a non-radial rate of growth	251
K. C. O'Meara, Intrinsic extensions of prime rings	257
Stanley Poreda, A note on the continuity of best polynomial approximations	271
Robert John Sacker, <i>Asymptotic approach to periodic orbits and local prolongations</i> of maps	273
Eric Peter Smith, <i>The Garabedian function of an arbitrary compact set</i>	289
Arne Stray, Pointwise bounded approximation by functions satisfying a side condition	301
John St. Clair Werth, Jr., Maximal pure subgroups of torsion complete abelian	
<i>p</i> -groups	307
Robert S. Wilson, On the structure of finite rings. II	317
Kari Ylinen, The multiplier algebra of a convolution measure algebra	327