ACTA ARITHMETICA
XXV (1974)

On a theorem of MacCluer

by

MICHAEL FRIED (Stony Brook, N. Y.)

1. Introduction. Let $F = \boldsymbol{F}(q)$ be the finite field with q elements. In [6] C. MacCluer proved a theorem which says (roughly) that a polynomial map on a finite field that is "almost" one-one, is actually one-one. More precisely, let $f(y) \in F[y]$ satisfy (called *exceptional* in [6] and *virtually one-one* in [4]):

(1.1) $\varphi(y, z) = \dfrac{f(y)-f(z)}{y-z}$ has *no* absolutely irreducible factors over F

(that is, every irreducible factor of $\varphi(y, z)$ reduces over $\overline{F}$, a fixed algebraic closure of F).

Assume in addition that

(1.2) the function field $F(y)$ is tamely ramified over $F(f(y))$.

Then MacCluer showed that

(1.3) $f(y)$ is a one-one (and therefore onto map) of the field F into itself.

Actually, it turned out (by much deeper methods) that for $f \in F[y]$ satisfying (1.1) and (1.2), f is indeed very special: a composition of cyclic and Chebychev polynomials (see Theorem 1 of [4]).

R. Lidl and C. Wells in [5] introduced polynomial mappings (in many variables) from $F^m \to F^m$ that generalize the properties of cyclic and Chebychev polynomials in that they often produce one-one mappings.

Let R be either a finite field or the ring of integers of a number field, and let $\mathrm{Res}(R)$ be the collection of field extensions of residue class fields of R. In fact, in [5] it is conjectured that if

(1.4) H: $(y_1, \ldots, y_n) = \boldsymbol{y} \to (h_1(\boldsymbol{y}), \ldots, h_n(\boldsymbol{y}))$ is a polynomial mapping with $h_i \in R[\boldsymbol{y}]$ for $i = 1, \ldots, n$

and if

(1.5) H: $F^n \to F^n$ is one-one for infinitely many fields $F \in \mathrm{Res}(R)$,

then

(1.6) H is a composite of the generalized cyclic and Chebychev polynomials of Wells and Lidl.

Actually, as example 1 of [4] shows, this was already wrong for $n = 1$, $R = \boldsymbol{F}(q)$ because of wild ramification (condition (1.2) does not hold). In Section 2 the notion of virtually one-one is extended to all H as in (1.4). Let $f(y) = \dfrac{f_1(y)}{f_2(y)}$ be a rational function, with $f_i(y) \in R[y]$ for $i = 1, 2$. Then, we may formally add ∞ to F, in order to ask if

(1.7) $f(y)$: $F \dot{\cup} \infty \to F \dot{\cup} \infty$ is a virtually one-one map.

This is equivalent to H being virtually one-one where

(1.8) $H = \big(h_1(y_1, y_2), h_2(y_1, y_2)\big) = \big(y_2 f_1(y_1), y_2 f_2(y_1)\big)$.

In fact, if f satisfies (1.7) then f is one-one (Proposition 1). But

(1.9) $H(y_1^{(1)}, y_2^{(1)}) = H(y_1^{(2)}, y_2^{(2)})$ for $\boldsymbol{y}^{(1)}, \boldsymbol{y}^{(2)} \in F^2$ and $y_2^{(1)} = y_2^{(2)} = 0$.

If $y_2^{(1)} \cdot y_2^{(2)} \neq 0$, the ratios of the coordinates in (1.9) are equal so that

$$\frac{f_1(y_1^{(1)})}{f_2(y_1^{(1)})} = \frac{f_1(y_1^{(2)})}{f_2(y_1^{(2)})}.$$

From (1.7) this implies that $y_1^{(1)} = y_1^{(2)}$, and therefore from (1.9) that $y_2^{(1)} = y_2^{(2)}$. Thus H is nearly (but not quite) one-one. So MacCluer's theorem does not hold in the many variable case.

In this paper we generalize MacCluer's theorem to show that a polynomial map (as in (1.4)) that is virtually one-one, finite and surjective, is actually a one-one mapping (Theorem 1). Proposition 1 generalizes Mac Cluer's Theorem in another direction. The observation for treating wild ramification was made by S. Cohen in [1]. For the notions of finite and surjective morphisms we refer the reader to [10], pp. 243–245. The f satisfying (1.7), of prime degree, are classified in [4] and [9].

2. Generalizations of MacCluer's theorem. Throughout F denotes a finite field, with order $|F|$. Let H be a polynomial mapping as given in (1.4). Let $\Gamma_H \overset{\text{def}}{=}$ Graph of H so that over any field $F \in \mathrm{Res}(R)$,

(2.1) $\Gamma_H(F) = \big\{(y_1, \ldots, y_n;\ h_1(\boldsymbol{y}), \ldots, h_n(\boldsymbol{y})) \big|\ \boldsymbol{y} \in F^n\big\}$.

We assume that

(2.2) $\text{trans.dim.}\, F\big(h_1(\boldsymbol{y}), \ldots, h_n(\boldsymbol{y})\big) = n$,

and that

(2.3) $F(\boldsymbol{y})$ is a separable extension of $F(\boldsymbol{x})$ where we have introduced the variables $x_i = h_i(\boldsymbol{y})$, for $i = 1, \ldots, n$.

Without condition (2.2) it is unlikely that H could give a one-one mapping. In fact, the image set would be of lower dimension (say $k < n$) and therefore would have roughly $|F|^k$ rational points over the finite field F (see proof of Lemma 2).

Let $\{z_i\}_1^n$ be new variables, algebraically independent over $F(\boldsymbol{y})$. Let S be the affine algebraic set in F^{2n} defined by the ideal

$$I_S = (h_1(\boldsymbol{y}) - h_1(\boldsymbol{z}), h_2(\boldsymbol{y}) - h_2(\boldsymbol{z}), \ldots, h_n(\boldsymbol{y}) - h_n(\boldsymbol{z})) \quad \text{in} \quad F[\boldsymbol{y}; \boldsymbol{z}].$$

We let Ω_H be the normal closure of $F(\boldsymbol{y})$ over $F(\boldsymbol{x})$. Let Δ be the affine algebraic subset of F^{2n} defined by the ideal

$$I_\Delta = (y_1 - z_1, y_2 - z_2, \ldots, y_n - z_n) \quad \text{in} \quad F[\boldsymbol{y}; \boldsymbol{z}].$$

LEMMA 1. *The irreducible components of S are all of dimension n and include Δ with multiplicity one.*

Proof. We denote the fields conjugate to $F(\boldsymbol{y}) = F(\boldsymbol{y}^{(1)})$ over $F(\boldsymbol{x})$ by $F(\boldsymbol{y}^{(i)})$, $i = 1, \ldots, l$ where $l = [F(\boldsymbol{y}) : F(\boldsymbol{x})]$. The irreducible components of S have generic points in $\tilde{\Omega}^{2n}$, (where $\tilde{\Omega}$ is some universal domain containing Ω_H) given by $(\boldsymbol{y}^{(1)}; \boldsymbol{y}^{(i)})$. Also, $(\boldsymbol{y}^{(1)}; \boldsymbol{y}^{(i)})$ and $(\boldsymbol{y}^{(1)}; \boldsymbol{y}^{(j)})$ define the same irreducible component of S if and only if $F(\boldsymbol{y}^{(i)})$ is conjugate to $F(\boldsymbol{y}^{(j)})$ over $F(\boldsymbol{y}^{(1)})$. Clearly the transcendence dimension of the generic point (and therefore the dimension of the algebraic set defined by it) is n.

The generic point of Δ is $(\boldsymbol{y}^{(1)}; \boldsymbol{y}^{(1)})$. In order to show that Δ is a component of multiplicity one, we have only to show that

$$(I_\Delta)^2 \not\ni I_S. \tag{2.4}$$

From (2.3) there exist i and j such that

$$\frac{\partial}{\partial y_i}(h_j(\boldsymbol{y}) - h_j(\boldsymbol{z}))\Big|_{(\boldsymbol{y}^{(1)};\boldsymbol{y}^{(1)})} = \frac{\partial}{\partial y_i^{(1)}}(h_j(\boldsymbol{y}^{(1)})) \tag{2.5}$$

in not identically zero. However, for $f \in (I_\Delta)^2$, the expression

$$\frac{\partial f}{\partial y_i}\Big|_{(\boldsymbol{y}^{(1)};\boldsymbol{y}^{(1)})}$$

is identically zero, thus demonstrating (2.4). ■

LEMMA 2. *Let H be a polynomial mapping as given in* (1.4) *such that* (2.2) *and* (2.3) *hold. In the notation above assume that*

(2.6) *S has an absolutely irreducible component defined over F and distinct from Δ.*

Then there exist constants C, B, ε with $0 < C < 1$, $\varepsilon > 0$, $B > 0$ (all independent of $|F|$) such that

(2.7) *the image of the polynomial mapping H excludes at least $C|F|^n - B|F|^{n-\varepsilon}$ elements of F^n.*

Proof. Let V^n be an absolutely irreducible variety over the finite field F, of dimension n. Then V^n has $|F|^n + O(|F|^{n-\varepsilon})$ rational points for some constant $\varepsilon > 0$ (independent of $|F|$). This is well known, but we point out that this fact can be reduced to the case of curves by Bertini's Theorem. For many curves the elementary argument of Davenport applies (see [2]: in general we use the celebrated Riemann hypothesis for curves over finite fields). Let V be the absolutely irreducible component of S hypothesized in (2.6). Since $V \cap \Delta$ is an algebraic set of dimension $n-1$, it has $O(|F|^{n-1})$ rational points. Thus $V - \Delta$ has $|F|^n + O(|F|^{n-\varepsilon})$ rational points. Let $(\boldsymbol{y}^{(1)}; \boldsymbol{y}^{(j)})$ (as in the proof of Lemma 1) be a generic point of V, where $\boldsymbol{y}^{(j)}$ has t conjugates over $F(\boldsymbol{y}^{(1)})$. Then there are at least $\frac{1}{t}|F|^n + O(|F|^{n-\varepsilon})$ elements of F^n which occur as the second n-tuple of rational points of $V - \Delta$. Since H maps each of these elements onto elements which are the image by H of at least two elements of F^n, the image of H must exclude at least $\frac{1}{t}|F|^n + O(|F|^{n-\varepsilon})$ elements of F^n. Taking $C = 1/t$, the proof of the lemma is concluded. ∎

Definition. If H is a polynomial mapping (as in (1.4)) satisfying (2.2) and (2.3) and such that

(2.8) S has, excluding Δ, no absolutely irreducible components defined over F;

then we say H is a *virtually one-one mapping over F.*

Theorem 1. *Let H be a polynomial mapping that is virtually one-one finite and surjective over F. Then H: $F^n \to F^n$ is a one-one mapping.*

Proof. We use the notation of Lemma 1. Let $\boldsymbol{x}_0$ be a place of $F(\boldsymbol{x})$ and let $\boldsymbol{p}$ be a prime of Ω_H extending $\boldsymbol{x}_0$, with decomposition group $D(\boldsymbol{p})$. Let $\hat{F}$ be the algebraic closure of F in Ω_H, and (as in [1]):

$$G(\Omega_H/F(\boldsymbol{x})) \overset{\text{def}}{=} \{\tau \in G(\Omega_H/F(\boldsymbol{x})) \mid \tau \text{ restricted to } \hat{F} \text{ is the Frobenius element in } G(\hat{F}/F)\}. \tag{2.9}$$

Let $\tau(\boldsymbol{p}) \in D(\boldsymbol{p})$ map onto the Frobenius element by the residue class map (that is, $\tau(\boldsymbol{p})$ generates $G(F(\boldsymbol{p})/F)$ where $F(\boldsymbol{p})$ is the residue class field of $\boldsymbol{p}$). All of this, including the existence of $\tau(\boldsymbol{p})$, is classical in the one variable case. See [8] (pp. 69–82) for the several variable case.

Suppose that we have the relation

$$\hat{G}\big(\Omega_H/F(\boldsymbol{x})\big) = \bigcup_{i=1}^{l} \hat{G}\big(\Omega_H/F(\boldsymbol{y}^{(i)})\big). \tag{2.10}$$

Then $\tau(\boldsymbol{p}) \in \hat{G}\big(\Omega_H/F(\boldsymbol{y}^{(i)})\big)$ for some i. Therefore $\tau(\boldsymbol{p})$ fixes $\boldsymbol{p}(\boldsymbol{y}^{(i)})$ (the value of the place $\boldsymbol{p}$ on $\boldsymbol{y}^{(i)}$) which implies that $\boldsymbol{p}(\boldsymbol{y}^{(i)}) \in F^m$. Thus, $H\big(\boldsymbol{p}(\boldsymbol{y}^{(i)})\big) = \boldsymbol{x}_0$, and $\boldsymbol{x}_0$ is an image point under H. In other words, H is onto (and therefore one-one) map.

Note that condition (2.8) implies that if $\tau(\boldsymbol{p}) \in \hat{G}\big(\Omega_H/F(\boldsymbol{y}^{(1)})\big)$, then $\tau(\boldsymbol{p})(\boldsymbol{y}^{(i)}) \neq \boldsymbol{y}^{(i)}$ for $i \neq 1$ since $(\boldsymbol{y}^{(1)}; \boldsymbol{y}^{(i)})$ is the generic point for an irreducible component of S which is acted on nontrivially by the Frobenius element. Thus $\hat{G}\big(\Omega_H/F(\boldsymbol{y}^{(1)})\big)$ has no intersection with $\hat{G}\big(\Omega_H/F(\boldsymbol{y}^{(i)})\big)$ for $i \neq 1$, and the right side of (2.10) has order $l\big|\hat{G}\big(\Omega_H/F(\boldsymbol{y}^{(1)})\big)\big|$. This is also the order of the left side of (2.10), as $F(\boldsymbol{y}^{(1)})/F(\boldsymbol{x})$ is a regular extension of degree l. Since the right side of (2.10) is *a priori* contained in the left side, and their orders are the same, we have proved that (2.10) holds. From the previous argument we are done. ■

The next proposition is proved in a similar manner, and it offers still another generalization of MacCluer's Theorem.

PROPOSITION 1. *Let $h(x, y) \in F[x, y]$ be an irreducible polynomial, and suppose $F(x, y^{(1)})$ is separable over $F(x)$, where $\{y^{(i)}\}_1^l$ are the zeros of $h(x, y)$. Assume also that*

(2.11) *each orbit of the representation of $G\big(\Omega_h/F(y^{(1)})\big)$ on $y^{(2)}, \ldots, y^{(l)}$ breaks up into smaller orbits under the action of $G\big(\overline{F}\cdot\Omega_h/\overline{F}(y^{(1)})\big)$ (where $\Omega_h = F(x, y^{(1)}, \ldots, y^{(l)})$ and $\overline{F}$ is a fixed algebraic closure of F).*

Then,

(2.12) *for each $x_0 \in F \dot{\cup} \infty$, there exists (a unique) $y_0 \in F \dot{\cup} \infty$ such that $h(x_0, y_0) = 0$.*

References

[1] S. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. 17 (1970), pp. 259–273.

[2] H. Davenport, *On Character Sums in finite fields*, Acta Math. 71 (1939), pp. 99–121.

[3] M. Fried, *On a conjecture of Schur*, Mich. Math. Journal 17 (1970), pp. 41–55.

[4] — *Arithmetical properties of function fields (II)*, Acta Arith. 25 (1974), pp. 225–258.

[5] R. Lidl and C. Wells, *Chebychev polynomials in several variables*, Crelle, 1972.

[6] C. MacCluer, *On a conjecture of Davenport and Lewis concerning exceptional polynomials*, Acta Arith. 12 (1967), pp. 289–299.

[7] C. Wells (with the aid of W. Nobauer), *Bibliography of Literature on Representable Mappings of an Algebraic Structure Into Itself*. Dept. of Math. Case Western Reserve University.

[8] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. II, 1960.

Added in proof

[9] M. Fried and D. J. Lewis, *Solution spaces to Diophantine problems,* Bull. Amer. Math. Soc., to appear.
[10] M. Mumford, *Introduction to Algebraic Geometry,* Harvard Notes.

Received on 24. 4. 1972 (384)