Rational Maps and Images of Rational Points of Curves over Finite Fields

ROBERT M. GURALNICK

Abstract. We give a survey and some new results about covers of curves related to images of rational points. In particular, we discuss exceptional covers and exceptional polynomials and pairs of covers which have the same image on rational points. Our approach uses group theoretic translations of these problems. A variant of this problem is to study extensions of a number field with the same degree one primes.

Dedicated to the memory of
my good friend, colleague and collaborator Dennis Estes.

1. Introduction

This paper is based to a large extent on a talk given at the May 2001 All Ireland Algebra Days Conference in Belfast. We wish to thank the organizers of the conference and in particular Martin Mathieu for their support, encouragement and hospitality. We would also like to thank Mike Fried for many interesting conversations on these topics.

Let k be a field of characteristic $p \geq 0$. For convenience, we assume that k is perfect and often a finite field. Let X, Y be smooth projective curves and $f : X \to Y$ a separable branched covering of degree n defined over k. We make the blanket assumption that all such covers are geometric – i.e. the degree remains the same after passing to $\bar{k}$, the algebraic closure of k. This is always the case if f is a polynomial or a rational function or if there is a totally ramified rational point.

Key words and phrases. Rational point, value set, curve, finite field, exceptional polynomials, Davenport pair, Kronecker equivalence, coverings of curves.

The author was supported in part by NSF grant DMS-9970305. The author would also like to thank the organizers of the All Ireland Algebra Days Conference.

Let $X(k)$ and $Y(k)$ denote the set of k-rational points on X and Y. Let $\mathcal{V}_k(f) := f(X(k)) \subseteq Y(k)$. In this article, we will consider various properties of f related to $\mathcal{V}_k(f)$. We will attack these problems by translating many of these questions to group theoretic properties of certain Galois groups. We try to classify the groups with such properties and then determine when such groups can act on curves with the desired properties. Fried [12], [13] has used this approach to good effect.

For the rest of the introduction, assume that k is finite. One concept that has been of interest in this field for well over a hundred years has been the study of permutation polynomials – polynomials which are bijective on rational points. If k is sufficiently large (compared to the degree of the polynomial), then permutation polynomials in fact are bijective on rational points for infinitely many extensions and are called exceptional polynomials. See [26] for some specific types of bounds.

Much progress has been made recently about exceptional polynomials. See §3 for a survey about the classification of indecomposable exceptional polynomials – in particular, we know all the indecomposable exceptional polynomials except those of degree $p^a, a > 2$. In fact, much work had been done in trying to prove the Carlitz conjecture about exceptional polynomials over finite fields of odd characteristic – i.e. that there are no such polynomials of even degree. This is an easy consequence of the classification mentioned above.

A generalization of this is the concept of a Davenport pair of polynomials – see [5]. These are two polynomials f, g over k so that $\mathcal{V}_f(k') = \mathcal{V}_g(k')$ for infinitely many extensions k'/k. If we take $g = x$, then (f, x) a Davenport pair is equivalent f being exceptional. If $\mathcal{V}_f(k') = \mathcal{V}_g(k')$ for all k', then the pair (f, g) is called a strong Davenport pair. See [5] for some recent results on Davenport pairs and strong Davenport pairs of polynomials. There is an obvious analog for pairs of maps $f_i : X_i \to Y, i = 1, 2$.

A special case of what we shall prove is:

Theorem 1.1. *Let k be a finite field of cardinality q. For $i = 1, 2$, let $f_i : X_i \to Y$ be rational maps of curves X_i, Y all defined over k and assume that there is a point $y \in Y(k)$ that is totally ramified in each cover.*

(1) *If* (f_1, f_2) *is a Davenport pair with* f_i *of degree* n_i*, then* $\gcd(n_1, q-1) = \gcd(n_2, q-1)$*; and*
(2) *If* (f_1, f_2) *is a strong Davenport pair, then* $n_1' = n_2'$*, where* n_i' *is the largest prime to* p *integer dividing* n_i*.*

If the f_i are polynomials, this is proved in [5]. If f_1 is an exceptional cover from X_1 to Y over k, then we can take f_2 to be the identity map on Y. This yields the Carlitz-Wan conjecture (see [15], [20], [7]):

Corollary 1.2. *Let* k *be a finite field of cardinality* q*. Let* $f : X \to Y$ *be rational map of curves defined over* k *and assume that there is a point* $y \in Y(k)$ *that is totally ramified. If* f *is exceptional of degree* n*, then* $\gcd(n, q-1) = 1$.

This is a much weaker result than the classification of exceptional polynomials. See [20] and [7] for proofs of the corollary. Lenstra was the first to observe that if one is interested in only the degrees of exceptional polynomials, then there is an easy proof of the corollary. The classification of exceptional polynomials depends upon the classification of finite simple groups. The theorem and corollary above do not depend on any deep facts.

If f is not bijective, then using Chebotarev density and some classical and recent results about derangements (i.e. fixed point free permutations) in finite permutation groups, one can show that f usually cannot be very close to being bijective on rational points. We will recall some results in [27] regarding this situation and discuss briefly some ongoing work.

Here is a brief summary of what is in the paper. In the next section, we give a summary of various arithmetic properties of covers of curves and their group theoretic analogs. We then discuss exceptional polynomials and describe the current state of the classification of them. After a few group theoretic preliminaries, we prove various results about Davenport pairs of covers in which at least one has a totally ramified rational point. In particular, we consider the case when there is a common totally ramified point and both covers are indecomposable.

We also interpret an old result [17] which yields (with no assumption on ramification):

Theorem 1.3. *Let* $f_i : X_i \to Y$ *be defined over a finite field* k*. Assume that* f_i *has degree* n *and the geometric monodromy group is* S_n*.*

If (f_1, f_2) is a strong Davenport pair, then f_1 and f_2 are equivalent over k (and in particular X_1 and X_2 are isomorphic over k).

In the final section, we mention some results about $\mathcal{V}_k(f)$ when f is not an exceptional map. By Chebotarev density, this is closely related to questions about derangements (fixed point free permutations).

We remark that many of these questions can be considered in a more general setting – including varieties rather than curves and number fields. See [17], [16] and [33] for examples.

2. A Dictionary

In this section, we introduce the basic set up to translate arithmetic and geometric properties of the cover to group theoretic properties.

We first recall some group theoretic notation. Let A be a group and Ω a transitive G-set. We say A is primitive on Ω if it preserves no nontrivial partition of Ω. This is equivalent to saying that the stabilizer A_ω of a point $\omega \in \Omega$ is a maximal subgroup of A.

Another notion that we will use if that of exceptionality. Suppose that G is normal in A and also acts transitively on Ω. We say that (A, G, Ω) is exceptional if A and G have no common orbits on $\Omega \times \Omega$ other than the diagonal. If $\omega \in \Omega$, this is equivalent to saying that A_ω and G_ω have no suborbit in common other than the common fixed point ω. If A/G is cyclic, this is easily seen to be equivalent to the fact that if aG generates A/G, then every element in the coset aG has a (unique) fixed point. See [15] or [27].

Let k be a perfect field of characteristic $p \geq 0$. Let $\bar{k}$ denote the algebraic closure of k. If X is a curve defined over k, let $X(k)$ denote the set of k-rational points of X. Let $f : X \to Y$ be a separable cover of degree n defined over k with f geometric. This is equivalent to consider the extension of function fields $k(X)/k(Y)$, a separable extension of degree n. The geometric hypothesis just means that k is algebraically closed in $k(X)$.

We need to introduce some groups into this picture. We can consider the Galois closure of this extension – it corresponds to some curve Z defined over some finite Galois extension k'/k. Since we will be considering pairs of covers, we will consider such a Z but only assume that $k'(Z)/k(Y)$ is a finite Galois extension and $k'(Z)$ contains $k(X)$ but may be larger than the Galois closure. Let $A = \mathrm{Gal}(k'(Z)/k(Y)), G = \mathrm{Gal}(k'(Z)/k'(Y)$, and $H := H_f =$

$\mathrm{Gal}(k'(Z)/k(X)$. A is called the arithmetic monodromy group and G the geometric monodromy group. Note the following:

$|A:H| = n$ and $\Omega := \Omega_f$ is the A-set A/H;

G is transitive on Ω or equivalently, $A = GH$ (this is the geometric cover hypothesis);

$A/G = \mathrm{Gal}(k'/k)$ and in particular G is a normal subgroup of A.

The next few results gives the correspondence between some arithmetic/geometric properties and group theoretic properties.

We say f is arithmetically indecomposable if f cannot be written as a composition of covers over k. We say f is geometrically indecomposable if f cannot be written as a composition of covers over the algebraic closure of k (or equivalently k'). One obviously has:

Lemma 2.1. (1) *f is arithmetically indecomposable if and only if A is primitive on Ω.*
(2) *f is geometrically indecomposable if and only if G is primitive on Ω.*

Let $y \in Y(k)$. Let $z \in Z$ be any point over y. The stabilizer D_y in G of y is called the decomposition group of z. We will abuse notation and call this the decomposition group of y – this is well defined up to conjugacy in A. Note that $A = GD$ since $y \in Y(k)$ and so D_y has fixed field k in its action on the residue field of z. Let I_y be the subgroup of D_y which does act trivially on the residue field. So $I_y \leq G \cap D_y$. We note the following well known facts (see [35], [36] and [18]):

Lemma 2.2. (1) *D_y is the local Galois group – i.e. it is the Galois group after completing at z;*
(2) *I_y is cyclic modulo its normal Sylow p-subgroup and if k is procyclic, then D_y/I_y is cyclic;*
(3) *$y \in Y(k)$ is totally ramified in the cover $f : X \to Y$ if and only if I_y is transitive on Ω; and*
(4) *the number of elements in $X(k)$ over $y \in Y(k)$ is the number of common (D_y, I_y) orbits on Ω.*

Suppose that $y \in Y(k)$ is not a branch point. This is equivalent to saying that $I_y = 1$. Thus, $D_y \cong \mathrm{Gal}(k''/k)$, where k'' is the residue field at z (a point over y). In particular, if k is procyclic (eg., k is finite), then D_y is cyclic. As noted above, $A = GD_y$ and so D_y is generated by some element in the coset aG where aG is a generator for A/G. If (A, G, Ω) is exceptional, then clearly D_y has a unique fixed point for any $y \in Y(k)$ that is not a branch point. Thus, there is a unique point in $X(k)$ mapping to y. If $y \in Y(k)$ is a branch point, then still $D_y = \langle b \rangle I_y$ where $b \in aG$. Thus, $D_y\omega = I_y\omega$ where ω is the fixed point of b. Thus, D_y and I_y have the common orbit $I_y\omega$. It is straightforward to see that this is the unique common orbit. This analysis applies equally well to any extension field ℓ/k linearly disjoint from k'/k (since (A, G, Ω) remains unchanged). So we have shown:

Lemma 2.3. *If k is procyclic and (A, G, Ω) is exceptional, then f is a bijection from $X(\ell) \to Y(\ell)$ for every finite extension field ℓ with* $\gcd(|\ell : k|, |A/G|) = 1$.

The converse is not true for general fields – for example, $X(k)$ and $Y(k)$ can be both be empty (take $k = \mathbb{R}$). However, if k is finite and is sufficiently large, then every cyclic subgroup D of A with $A = GD$ occurs as a decomposition group (this is a weak version of the Chebotarev density theorem). Alternatively, one can use the fact that given an absolutely irreducible variety V over a finite field k, then for every sufficiently large extension field ℓ over k, $V(\ell)$ is nonempty to prove the well known (see [12], [15], [6]):

Lemma 2.4. *Assume that k is finite. (A, G, Ω) is exceptional if and only if f is a bijection from $X(\ell) \to Y(\ell)$ for every finite extension field ℓ with* $\gcd(|\ell : k|, |A/G|) = 1$.

3. EXCEPTIONAL COVERS

In this section, we give a survey of the classification results for exceptional covers and polynomials with a totally ramified point. Keep the notation from the previous section.

We say that f is an exceptional cover if the one dimensional variety

$$\{(x_1, x_2) | x_i \in X, f(x_1) = f(x_2)\}$$

has no absolutely irreducible components defined over k other than the diagonal. If k is finite, this is equivalent to f being bijective for infinitely many extensions of k or indeed being bijective for k sufficiently large. See [6], [15], [12], [13].

Lemma 3.1. *$f : X \to Y$ is exceptional over k if and only if A and G have no common orbits on $\Omega \times \Omega$ other than the diagonal, i.e. if and only if (A, G, Ω) is exceptional.*

In [24], all triples (A, G, Ω) satisfying the following conditions were determined:

(1) A is primitive and faithful on Ω with $|\Omega| = n$;
(2) (A, G, Ω) is exceptional;
(3) G contains a transitive subgroup I with I/P cyclic for P a Sylow p-subgroup of I; and
(4) n is not a power of p.

If in addition, we assume that A/G is cyclic, this result was obtained in [15]. In [21], a fairly comprehensive result about the triples (A, G, Ω) satisfying (1), (2) and (4) was obtained (again with the assumption that A/G is cyclic). We expect a similar result to hold if we drop the assumption that A/G is cyclic (there are a few more families of examples without that assumption and the method of proof will be quite different). By a result of Guralnick and Stevenson [25], these group theoretic possibilities will occur for some cover $f : X \to Y$ (over some finite field of characteristic p if A/G is cyclic).

If $p \geq 5$, the only such examples occur for n prime with A/N cyclic of order dividing $n - 1$ with N normal of order n.

If $p = 2$ or 3, there are some additional families of degree $n = p^a(p^a - 1)/2$ for $1 < a$ with a odd.

In [22] and [28], all the possibilities for polynomials in these latter two cases were determined and in particular were shown to be variants of known families (see [31], [8], [30]) except for one new family in characteristic 2. It was also determined over which fields the polynomials can be defined.

We state this result as follows:

Theorem 3.2. *Let f be an exceptional indecomposable polynomial of degree n over k with $n \neq p^a$. Then one of the following occurs:*

(1) *n is prime and the geometric monodromy group of f is cyclic or dihedral, f is a cyclic polynomial or a Dickson polynomial;*
(2) *$p = 2$ or 3, $n = p^a(p^a - 1)/2$ for $1 < a$ with a odd, the geometric monodromy group is $PSL(2, p^a)$. Moreover, f is geometrically equivalent to a CM-polynomial, an LZ-polynomial or a GRZ-polynomial.*

Applying this result gives a complete classification of indecomposable exceptional polynomials of degree not a power of the characteristic. If $p \geq 5$, the only such polynomials are of prime degree n

and essentially x^n with k not containing an nth root of 1 or Dickson polynomials of degree n with an nth root of 1 not quadratic over k.

This leaves the case $n = p^a$. An easy source of examples comes from the cases where the Galois closure of the cover has genus zero.

The only family of examples known where this is not the case are some polynomials constructed in [20] – this was done for odd characteristic but there is an analogous family in characteristic 2.

We conjecture that aside from possibly a short list of exceptions that we now know all exceptional polynomials.

4. Davenport Pairs

Let $X_i, i = 1, 2$ and Y be smooth projective curves defined over a finite field $k = \mathbb{F}_q$. Let $f_i : X \to Y$ be separable covers of degree n_i also defined over k. We assume that the f_i are geometric covers – i.e. they still have degree n_i over the algebraic closure of k.

Following [5], we define

Definition 4.1. *We say that the pair (f_1, f_2) is a Davenport pair if $f_1(X(q^e)) = f_2(X(q^e))$ for infinitely many e. We say that (f_1, f_2) is a strong Davenport pair if $f_1(X(q^e)) = f_2(X(q^e))$ for all e.*

We let Z be any curve containing the Galois closure of the compositum of $k(X_i), i = 1, 2$ over $k(Y)$. We keep the notation of the earlier sections. Let $k(Z_i)$ denote the Galois closure of $k(X_i)/k(Y)$ and let k_i' be the algebraic closure of k in $k(Z_i)$. Let $m = |A : G|$ and note that A/G is cyclic. If $G \le B \le A$, let B_0 be the subset of B consisting of elements b such that bG generates B/G. If J is a subgroup of A, let $c(J) = \bigcup_{g \in A} J^g$ – so $c(J)$ is just the union of the conjugacy classes of A that intersect J. Equivalently, $c(J)$ is the collection of elements in A that have a fixed point on A/J.

Let H_i be the subgroup of A corresponding to $k(X_i)$. Let Ω_i be the A-set consisting of the left cosets of H_i in A. As we have noted, the fact that the covers are geometric is equivalent to the fact that G is transitive on Ω_i.

Note that if the f_i are a Davenport pair, there are infinitely many e such that $f_1(X(q^e)) = f_2(X(q^e))$ with $(e, m) = s$ fixed. By replacing k by its unique extension of degree s, we can then assume that $s = 1$. It follows that over all these extensions, the arithmetic monodromy group is unchanged (the passage to the degree s extension replaces A by its unique subgroup $B \ge G$ of index s).

Let $y \in Y(q^e)$ (where we now assume that $(e,m) = 1$) be a rational point. Let D be its decomposition group and I its inertia group (i.e. the decomposition group and inertia group of some point of z over y). Since y is rational, it follows that $A = GD$, D/I is cyclic and $I \leq G$.

We can now characterize Davenport pairs by various conditions. We consider a slightly weaker condition. See also [15] and [16].

Theorem 4.2. *Let $f_i : X_i \to Y$, $i = 1,2$ be separable covers of degree n_i defined over $\mathbb{F}_q$. The following are equivalent:*

(1) $f_1(X(q^e)) \subseteq f_2(X(q^e)$ *for infinitely many e;*
(2) $|f_1(X(q^e) \setminus f_2(X(q^e)| < c$ *for some constant c for infinitely many e (indeed, c can be replaced by $cq^{e/2-\epsilon}$ for any $\epsilon > 0$);*
(3) $B_0 \cap c(H_2) \subseteq B_0 \cap c(H_1)$ *for some subgroup B with $G \leq B \leq A$;*
(4) *There is a positive integer s such that $f_1(X(q^e)) \subseteq f_2(X(q^e))$ for all e with $(e,m) = s$.*

Proof. Clearly, the last condition implies the first and the first implies the second. Assume the second condition. Choose s so that there are infinitely many e satisfying the condition with $(e,m) = s$. Let $G \leq B \leq A$ with $|A : B| = s$. If $(e,m) = s$, then B is the Galois group of the Galois closure of the compositum $\mathbb{F}_{q^e}(X_i), i = 1,2$ over $\mathbb{F}_{q^e}(Y)$. We claim that $B_0 \cap c(H_2) \subseteq B_0 \cap c(H_1)$. If not, there exists a cyclic subgroup D of B with $B = DG$ such that D has no fixed points on A/H_2 but does on A/H_1. By Chebotarev density (see [16]), this implies that for e sufficiently large with $(e,m) = s$, there are $O(q^e)$ rational points on Y with decomposition group D and inertia group 1. By Lemma 2.2, this implies that for such points $y \in Y$, $y \in f_1(X_1(q^e))$ but are not in $f_2(X_2(q^e))$.

Finally, assume that $B_0 \cap c(H_1) \subseteq B_0 \cap c(H_2)$ for some subgroup B with $G \leq B \leq A$. Let $s = |A : B|$ and consider the fields $\mathbb{F}_{q^e}$ with $(e,m) = s$. Then B is the full monodromy group over such fields. Passing to this extension field allows us to assume that $A = B$. Let $y \in Y(q^e)$ with decomposition group D and inertia group I. By Lemma 2.2, it suffices to show that (D,I) has a common orbit on A/H_2 if it does on A/H_1. Then $A = DG$ (because y is an F_{q^e} point). Assume that D and I have a common orbit on A/H_1 containing ω_1. Let dI generate D/I. Thus, dG generates A/G (as $I \leq D \cap G$). It follows that $d\omega_1 = g\omega_1$ for some $g \in I$, whence dg^{-1} fixes ω_1. By hypothesis, this implies that dg^{-1} fixes some $\omega_2 \in A/H_2$. Thus,

$D\omega_2 = I\omega_2$ and so D and I have a common orbit on A/H_2 as required. $\square$

We immediately obtain the following two corollaries:

Corollary 4.3. *The following are equivalent:*

(1) *f_1 and f_2 are a Davenport pair;*
(2) *$B_0 \cap c(H_1) = B_0 \cap c(H_2)$ for some subgroup B with the property $G \leq B \leq A$;*
(3) *The images of f_i on $X_i'(q^e)$ agree for infinitely many e (or for a sufficiently large e).*
(4) *The images of f_i on $X_i(q^e)$ agree for infinitely many e (or for a sufficiently large e).*

Since strong Davenport pairs are just Davenport pairs for over every extension, we have the following result characterizing strong Davenport pairs.

Corollary 4.4. *The following are equivalent:*

(1) *f_1 and f_2 are a strong Davenport pair;*
(2) *$B_0 \cap c(H_1) = B_0 \cap c(H_2)$ for every subgroup B with the property $G \leq B \leq A$;*
(3) *The images of f_i on $X_i'(q^e)$ agree for all e.*
(4) *The images of f_i on $X_i(q^e)$ agree for all e.*

5. Kronecker Equivalent Permutation Actions

We first state a well known easy result – see [21].

Lemma 5.1. *Let G be a normal subgroup of a finite group A with A/G cyclic. Let A act on a finite set Ω. The number of common A, G orbits on Ω is the average number of fixed points of an element in the coset aG where aG generates A/G.*

Let A be a finite group with a normal subgroup G such that A/G is cyclic. Suppose that $\Omega_i, i = 1, 2$ are A-sets with G transitive on each Ω_i.

Let H_i be a point stabilizer on Ω_i. Let $J_i = c(H_i)$ (so J_i is just the union of the conjugates of H_i – since $A = GH_i$, J_i is the union of the G-conjugates of H_i).

Let A_0 be a fixed coset of G in A. By passing to the subgroup generated by this coset, we may and do assume that A_0 generates A/G.

We say that Ω_1 and Ω_2 are Kronecker equivalent if $A_0 \cap J_1 = A_0 \cap J_2$ and write $\Omega_1 =_K \Omega_2$. A particularly interesting case is when $A = G$ – then the condition is just that H_1 and H_2 intersect precisely the same conjugacy classes of G. Note that Ω_1 is exceptional is precisely equivalent to $A_0 \subseteq J_1$.

We say that $\Omega_1 \leq_K \Omega_2$ if $A_0 \cap J_1 \subset A_0 \cap J_2$.

If Γ is an A-set and W is a normal subgroup of A, we let Γ/A denote the set of W-orbits on Γ.

Lemma 5.2. *If $\Omega_1 \leq_K \Omega_2$ and N is a normal subgroup of A contained in G, then $\Omega_1/N \leq_K \Omega_2/N$ (for the pair $A/N, GN/N$).*

Proof. This follows from the trivial fact that if Γ is any A-set and $x \in A$, then x has a fixed point on Γ/N if and only if xn has a fixed point on Γ for some $n \in N$. Thus, x has a fixed point on Ω_1/N implies that xn has a fixed point on Ω_1 for some $n \in N$, whence also on Ω_2 and so x has a fixed point on Ω_2/N. □

In particular, we apply this to the case that N is the subgroup of G acting trivially on Ω_i. So we may often reduce to the case that G acts faithfully on one of the sets. The reason we assumed that $N \leq G$ in the previous result was that there is no guarantee that $xN \subseteq A_0$ unless $N \leq G$. However, we can still say something (note the Kronecker condition is not used in this next result):

Lemma 5.3. *Assume that A is faithful on $\Omega_1 \cup \Omega_2$, A/G is cyclic and that G acts faithfully on both Ω_j with $j = 1$ and 2. Assume moreover that A is primitive on Ω_1. Let J_i be the kernel of the action of A on Ω_i.*

1. *Either $J_2 = 1$ or $|\Omega_1| = |\Omega_2|$ is a prime n and $A = G \times J_2$ with G and J_2 each of order n.*
2. *If A is primitive and faithful on Ω_2, then A is faithful on Ω_1.*

Proof. Since G is faithful, $J_i \cap G = 1$ and J_i is cyclic. Note that $[A, J_i] \leq G \cap J_i = 1$ (since $G \leq [A, A]$). Thus, J_i is central in A.

Since A is primitive on Ω_1, either J_2 acts trivially on Ω_1 (and so $J_2 = 1$) or J_2 is transitive on Ω_1. In the latter case, the action of A on Ω_1 is primitive and has a normal cyclic subgroup whence Ω_1 has prime order r and the image of A on Ω_1 is contained in the normalizer of a Sylow r-subgroup of the corresponding symmetric group.

Since A centralizes J_2, it follows that the image of A acting on Ω_1 is cyclic of order r. Since G is transitive on both sets, both Ω_1 and Ω_2 have cardinality r. As G centralizes J_1, and they both act faithfully on Ω_2, J_1 is also an r-group, whence A is. Since A acts faithfully on $\Omega_1 \cup \Omega_2$, $A = G \times J_2$ with $G \cong J_2$ cyclic of order r.

Now assume that $J_2 = 1$. If A is primitive on Ω_2 and $J_1 \neq 1$, then applying the first part of the result shows that $A = G \times J_1$ with each G cyclic of prime order. It follows that A is not faithful on Ω_1, a contradiction. So $J_2 = 1$ implies that $J_1 = 1$ as required. □

Lemma 5.4. *Suppose that $D \leq A$ with $A = GD$ and $I \leq G \cap D$ with I normal in D. Assume that D/I is cyclic. If I is transitive on Ω_2 and Ω_1' is a common D, I-orbit of Ω_1, then $\Omega_1' \leq_K \Omega_2$ for D, I. In particular, if I is transitive on each Ω_i and the Ω_i are Kronecker equivalent for (A, G), then Ω_1, Ω_2 are Kronecker equivalent for (D, I).*

Proof. Let $x \in D \cap A_0$. If x has a fixed point on Ω_1', then x has a fixed point on Ω_2. □

6. Arithmetically Equivalent Covers

In this section, we consider a stronger condition that Kronecker equivalence. Let $f_i : X_i \to Y$ be covers over a field k of degree n_i. Let L be the Galois closure of the compositum of $k(X_1)k(X_2)/k(Y)$. Let A be the arithmetic Galois group of $L/k(Y)$ and G the geometric Galois group. Let H_i be the Galois group of $L/l(X_i)$. Thus, $|A : H_i| = n_i$. If k' is a finite extension of k and $y \in Y(k')$, let $N_i(y, k') = |\{x \in X_i(k') | f_i(x) = y_i\}|$. Strong Davenport pairs are characterized by $N_1(y) = 0$ if and only if $N_2(y) = 0$. We consider the condition that in fact these numbers are equal.

Proposition 6.1. *Assume that k is procyclic. Consider the following conditions:*

(i) $N_1(y, k') = N_2(y, k')$ *for all* $y \in Y(k')$ *for all extensions* k'/k*;*
(ii) $N_1(y, k') = N_2(y, k')$ *for all unramified (in both extensions)* $y \in Y(k')$ *for all extensions* k'/k*;*
(iii) *The permutation characters* $1_{H_i}^A$ *are equal.*

Then the third condition implies the first which implies the second. If k is algebraic over a finite field, then all three conditions are equivalent.

Proof. Clearly the first condition implies the second for any k.

Assume the third condition. By Lemma 2.2, $N_i(y, k')$ is the number of common D_y, I_y orbits on A/H_i. By Lemma 5.1, this is the average number of fixed points of an element in the coset aI_y where D_y/I_y is generated by aI_y. Our hypothesis implies that every element in A has the same number of fixed points on A/H_1 and A/H_2, whence the first condition holds.

Assume the second condition with k algebraic over a finite field. By Lemma 2.2, this implies that every decomposition group over an unramified point has the same number of fixed points on A/H_1 and A/H_2. By Chebotarev density, every cyclic subgroup of A is the decomposition group of some unramified point over some extension k'/k. Thus, the third condition holds. The proof is complete. □

We say two such covers are a very strong Davenport pair. This condition has been studied extensively. It comes up in considering number fields with the same zeta functions and for similar reasons in constructing isospectral manifolds that are not isometric. See [17]. The following corollary is immediate from the previous proposition (from the fact that the permutation characters coincide).

Corollary 6.2. *Suppose that $f_i : X_i \to Y$ are a very strong Davenport pair over the finite field k. Let n_i be the degree of f_i.*

(1) $n_1 = n_2$;
(2) *the arithmetic and geometric monodromy groups of the f_i coincide;*
(3) *the set of $y \in Y$ that are totally ramified under f_1 is the same as the set of $y \in Y$ that are totally ramified under f_2;*
(4) *X_1 and X_2 have the same genus; and*
(5) *If f_1 is a polynomial, then f_2 is equivalent to a polynomial.*

Proof. These results all follow from the fact that $1_{H_1}^A = 1_{H_2}^A$. This implies that the degrees of the permutation characters are the same ($n_1 = n_2$). It also implies that any normal subgroup of A contained in H_1 is also contained in H_2 (and vice versa), whence the second condition. Since totally ramified points are those with a single point over them, this clearly follows from the definition.

For the genus condition, we note (see [19]) that the genus of X_i is $1/2 \dim V^{H_i}$, where V is the Tate module (or the module of r-torsion points on the Jacobian of $Z - Z$ the curve corresponding to the Galois closure – for any sufficiently large prime r). By Frobenius reciprocity, this is the same for H_1 and H_2.

Now suppose that f_1 is a polynomial. Thus, $X_1 = Y = \mathbb{P}^1$ and $f_1^{-1}(\infty) = \{\infty\}$. So also $X_2 = \mathbb{P}^1$ and $\infty \in Y$ is totally ramified. Composing with an automorphism of X_2, we may assume that $f_2(\infty) = \infty$ and then f_2 is also a polynomial. □

We now consider an example. In some sense, this is the generic example. Let $G = \mathrm{GL}(d, q) = \mathrm{GL}(V)$. Let P_j denote that stabilizer of a subspace of dimension j. It is well known that P_j and P_{d-j} induce the same permutation character (because the transpose map preserves conjugacy classes and takes P_j to a conjugate of P_{d-j}). In fact, this holds more generally for any parabolic subgroup and its opposite (not necessarily maximal parabolics).

We can modify this slightly by considering the action on vectors and linear functionals. Indeed more generally, we can take H_1 to be any subgroup of G and H_2 its image under the transpose map (or the inverse-transpose automorphism of G). Then H_1 and H_2 induce the same permutation character.

A particularly interesting case is to take H_1 to be the stabilizer of a nonzero vector $v \in V$. Then H_2 is the stabilizer of a nonzero element $v^* \in V^*$, where V^* is the dual space of V. Since H_1 and H_2 induce the same permutation character in $\mathrm{GL}(V)$, if G acts on a curve Z, the covers $Z/H_1 \to Z/G$ and $Z/H_2 \to Z/G$ are a very strong Davenport pair. In particular, if the first cover is a polynomial cover, the second cover is as well. Examples of such polynomials have been constructed by Abhyankar, Elkies and Bluher. See also Fried [14].

Let us also observe that the same remarks hold for any subgroup A of $\mathrm{GL}(V)$ that is transitive on nonzero vectors (and so also on the nonzero elements of the dual space) – for any element of A has the same number of fixed points in both permutation representations. In particular, this applies to $\mathrm{SL}(V)$ and the group of semilinear transfomations (embed this group in the group of linear transformations of bigger dimension over the prime field).

7. Generalization of Carlitz-Wan

Suppose that $f_i : X_i \to Y$ are a Davenport pair over $\mathbb{F}_q$. We have seen that the set of e such that the images of rational points over $\mathbb{F}_{q^e}$ depends only on the arithmetic monodromy group over $\mathbb{F}_{q^e}$. Thus, there will be a collection $s_1, \dots, s_d$ so that the images on rational points are the same over $\mathbb{F}_{q^e}$ whenever $\gcd(e, |A : G|) = s_j$ for some j. After passing to an extension of degree s_j, we see that the values on rational points will be identical for all extensions of degree relatively prime to $|B : G|$, where B/G is the subgroup of index s_j in A/G.

If n is a positive integer and π is a set of primes, then we may write $n = n_\pi n'$ where n' is divisible by no primes in π. This defines n_π.

Theorem 7.1. *Assume that $f_i : X_i \to Y$ are covers of curves of degree n_i defined over $k = \mathbb{F}_q$ and $y_0 \in Y(q)$ is totally ramified for f_2. Assume moreover that $y_0 \in f_1(X(q^e)) \subseteq f_2(X(q^e))$ for all e with $\gcd(e, s) = t$. Let π be the set of primes dividing $q^t - 1$. Let n_1' be the local degree of some rational point of X_1 over y_0. Then $(n_1')_\pi$ is a multiple of $(n_2)_\pi$.*

Proof. We may replace q by q^t, so assume that $t = 1$. We pick notation as above and let $k'(Z)$ be the Galois closure of $k(X_1)k(X_2)/k(Y)$ with Galois group A. Let H_i be the subgroup of A fixing $\mathbb{F}_q(X_i)$ and $\Omega_i = A/H_i$. Then G is transitive on each Ω_i. We have seen that our hypothesis on the images of the f_i are rational points is precisely that $\Omega_1 \leq_K \Omega_2$.

Let D be the decomposition group and I the inertia group of some point in the Galois closure over y_0. Since y_0 is in the image of f_1, there exists some common D, I orbit $\Omega_1' \subseteq \Omega_1$. Since $I \leq D \cap G$ and $A = GD$, it follows that $\Omega_1' \leq_K \Omega_2$ for (D, I).

So $n_1' = |\Omega_1'|$ and we may assume that $(A, G) = (D, I)$. In particular, we have a Galois extension with a totally ramified point.

Since D is the Galois group of the corresponding extension of local fields, we can complete the fields and consider extensions of local fields. We change notation and consider $\Omega_1' = \Omega_1$.

Let P the Sylow p-subgroup of I. Then P is characteristic in I which is normal in D and so P is normal in D. By Lemma 5.2, it follows that $\Omega_1/P \leq_K \Omega_2/P$ for $(D/P, (D \cap G)/P)$. The covers (corresponding to the subgroups $(H_i \cap D)P$) still have the desired property and we have only modified the degrees by a factor of a power of p. So we may assume that I is cyclic of order prime to p. Indeed, precisely the same argument shows that we may assume that any prime dividing the order of I also divides $q - 1$.

Since we are in the situation where $\mathbb{F}_q$ contains all rth roots of unity for any $r|n_i$, it follows that the geometric extensions of degree n_i are in fact Galois (there is a unique such extension – this is easily seen by reducing to the case a prime degree extension). Thus, we have now reduced to the case $D = I$ and $H_1 \leq H_2$, whence n_2 divides n_1 as desired (of course, we have modified these from the original n_i but only by factors relatively prime to $q-1$). $\square$

Note that the hypothesis in the previous theorem (and in the corollaries) can be weakened – for example, we only need the condition for infinitely many e rather than all e (or any sufficiently large e suffices).

We now state some corollaries of the previous result. The first one was obtained in the case that the f_i are polynomials in [5]. The proof is similar. Moreover, both proofs are minor variations of the proofs given for the Carlitz-Wan conjecture – see [7] and [20].

Corollary 7.2. *Assume that $f_i : X_i \to Y$ are covers of curves of degree n_i defined over $k = \mathbb{F}_q$ and $y_0 \in Y(q)$ is totally ramified in each cover. Let A be the Galois group of the Galois closure of the compositum of $k(X_1)k(X_2)/k(Y)$. Let G be the geometric Galois group and set $s = |A : G|$. Assume moreover that $f_1(X(q^e)) = f_2(X(q^e))$ for infinitely many e with $\gcd(e, s) = t$. Let π be the set of primes dividing $q^t - 1$. Then $(n_1)_\pi = (n_2)_\pi$. In particular, $\gcd(n_1, q^t - 1) = \gcd(n_2, q^t - 1)$.*

In particular, if $f_1 : X_1 \to Y$ is exceptional over $\mathbb{F}_q$ with a totally ramified rational point, then $\gcd(f_1, f_2)$ is a Davenport pair with f_2 the identity on $X_2 = Y$. Thus, $\gcd(n_1, q-1) = 1$. This is the Carlitz-Wan conjecture (under the additional condition that f_1 is a polynomial). This is essentially in [15]. See also [7] and [20].

Corollary 7.3. *If $f : X \to Y$ is an exceptional cover of degree n over $\mathbb{F}_q$ and there exists a totally ramified rational point, then $\gcd(n, q-1) = 1$.*

In particular, the previous result applies to exceptional polynomials. Of course, this result for exceptional polynomials is quite minor compared to the classification of all exceptional polynomials whose degree is not a power of the characteristic.

If (f_1, f_2) are a strong Davenport pair, then the previous results apply to every extension of the base field, whence $\gcd(n_1, q^s - 1) = \gcd(n_2, q^s - 1)$ for all $s \geq 1$. This yields (see also [5]):

Corollary 7.4. *If $f_i : X_i \to Y$, $i = 1, 2$ are a strong Davenport pair over $\mathbb{F}_q$ of degree n_i, then $n_1' = n_2'$ where m' is the p'-part of m.*

8. Davenport pairs with f_1 indecomposable

In this section, we generalize some results in [5] about Davenport pairs of polynomials of degree prime to the characteristic. We consider the case where one of the covers is indecomposable with a totally ramified rational point. We first consider the case where both are indecomposable with a totally ramified rational point.

Theorem 8.1. *Let k be a finite field of characteristic p. Suppose that $f_i : X_i \to Y$ are inequivalent indecomposable covers over the finite field k of degree n_i and $\mathcal{V}_{f_2}(k') = \mathcal{V}_{f_1}(k')$ for infinitely many extensions k'/k. Assume also that there exists $y \in Y(k)$ that is totally ramified for each f_i. Let A_i and G_i denote the arithmetic and geometric monodromy groups of f_i. Let A denote the monodromy group of the composite extension.*

(a) *$n = n_1 = n_2$ is a prime, $A_i = G_i \cong \mathbb{Z}/n$ and $A = G \times \mathbb{Z}/n$; or*

(b) *$A = A_1 = A_2$ and $G = G_1 = G_2$.*

Moreover if (b) *holds, then*

(c) *$n_1 = 5$, $n_2 = 10$ and $G_1 = G_2 = A_5$; or*

(d) *$n_1 = 25$, $n_2 = 100$ and $G_1 = G_2 = A_5 \wr S_2$; or*

(e) *$n = p^a$ and f_i is of affine type; or*

(f) *$n_1 = n_2$ and (f_1, f_2) is a strong Davenport pair.*

Proof. Assume that f_1 is not exceptional (and so neither is f_2). Let Ω_1 and Ω_2 denote the A-sets of degree n_i corresponding to the extensions. As we have seen $\Omega_1 = \Omega_1/K_1$ is Kronecker equivalent to Ω_2/K_1. Since A acts primitively on Ω_2, it follows that K_1 is either trivial on Ω_2 or transitive. In the latter case, this would imply that the action on Ω_1 is exceptional, a contradiction. So K_1 is trivial on each Ω_i and so is trivial (as A is the Galois closure of the compositum field). Similarly, $K_2 = 1$.

Suppose that A does not act faithfully on Ω_1. Then we apply Lemma 5.3 and conclude that $A = G \times J$ with G and J cyclic of order prime order n as allowed in the conclusion.

So A is faithful and primitive on each Ω_i. It follows that the Galois closure of each cover are the same. So $A_1 = A_2 = A$ and $G_1 = G_2 = G$.

We now apply the main results of [23] which give a classification of all such groups. If A has a normal nontrivial p-subgroup N, then $n = p^a = |N|$ in any primitive action and the theorem holds. In all other cases, A has a unique minimal normal subgroup N that is the direct product of $t \geq 1$ copies of a nonabelian simple group L. If $t > 2$, it follows from [23] that $n = p^a$ and the permutation characters agree. If $t \leq 2$, again the possibilities are given in [23] and a straightforward inspection yields that $n_1 = n_2$ and the permutation characters on the Ω_i agree. $\square$

In the affine case above, we do not know if there are really examples with polynomials which are Davenport pairs but which are not strong Davenport pairs. There are examples (see below) if we do not insist that X_i has genus zero.

Except for the affine examples, one can give a list of all the possible (group theoretic) examples in the previous theorem. The main family is when the socle of A is $PSL(d,q)$ with $d \geq 3$ and $n_1 = n_2 = (q^d - 1)/(q-1)$. The two actions are on 1-spaces and hyperplanes. Abhyankar (see [1], [2], [3], [4]) has shown that these do correspond to polynomials (at least if $p|q$ and in certain small examples) and so give rise to a nontrivial pair of strong Davenport polynomials (see [5], [14]). We expect these group theoretic examples to lead to very few examples of polynomials in other characteristics.

L	L_ω	n	p
$L_5(2)$	P_2	155	31
$U_4(3)$	$L_3(4)$	162	3
$L_2(11)$	A_5	11	**
$L_2(19)$	A_5	57	19
$L_2(23)$	S_4	253	23
$L_2(29)$	A_5	209	29
$L_2(59)$	A_5	1711	59
M_{23}	$M_{21}.2, 2^4A_6$	253	23

There are a few sporadic examples that can be read off from the results in [23]. The above is a complete list of the group theory possibilities (excluding the ones mentioned above) satisfying the conditions of the previous theorem under the added condition that the socle of A is a nonabelian simple group. There also infinitely many examples when the socle of A is not simple – all but finitely many such examples have degree a power of p. In all but the second example, $A = G = L$. In the second example, it follows that $|A : L| = 2$ or 4. For the families given above, there is only one possibility for the characteristic except for the case $G = L_2(11)$. Indeed, in that case, we know that there examples in any characteristic greater than 11 and very likely in smaller characteristics as well.

If we consider the case where only say f_1 is indecomposable, then one must work a bit harder but there is a similar result. We will address this in future work. We can prove a result with no assumption on the existence of a totally ramified point.

Theorem 8.2. *Let k be a finite field of characteristic p. Suppose that $f_i : X_i \to Y$ are covers over the finite field k of degree n_i and form a Davenport pair. Assume that f_1 is indecomposable and is not exceptional. Then $f_2 = g \circ h$ where $g : Y' \to Y$ is indecomposable, (f_1, g) is a Davenport pair and setting A_0 to be the Galois group of the Galois closure of $k(Y')k(X_1)/k(Y)$, either*

(a) *g has prime degree $r = n_1$, a prime and $A_0 \cong \mathbb{Z}/r \times \mathbb{Z}/r$; or*
(b) *A_0 is the Galois closure of $k(X_1)/k(Y)$ and of $k(Y')/k(Y)$ (i.e. f_1 and g have the same arithmetic and geometric monodromy groups).*

Proof. We use the standard notation. In particular, A is the Galois closure of $k(X_1)k(X_2)/k(Y)$. Let K_i be the kernel of G on Ω_i. Then Ω_1 and Ω_2/K_1 are still Kronecker equivalent, whence we may assume that $K_1 = 1$, i.e. G acts faithfully on Ω_2. If $K_2 \neq 1$, then K_2 acts nontrivially on Ω_1 and so Ω_1/K_2 is trivial and in particular exceptional. By Lemma 5.2, Ω_1/K_2 and Ω_2 are Kronecker equivalent. Since Ω_2 is not exceptional by hypothesis, $K_2 = 1$ as well.

We can now apply Lemma 5.3 to conclude that (a) or (b) holds. □

9. GENERIC COVERS

In this section, we consider strong Davenport pairs (f_1, f_2) from X_i to Y over k where f_1 is generic of degree n – i.e. the geometric monodromy group of f_1 is S_n (and therefore also the arithmetic monodromy group). The following theorem follows fairly easily from a group theoretic result in [17].

Theorem 9.1. *Let k be a finite field. Let $f_i : X_i \to Y$ be covers defined over k. Assume that f_1 has degree n and the geometric monodromy group of f_1 is S_n. If (f_1, f_2) is a strong Davenport pair, then f_1 and f_2 are equivalent over k. In particular, f_1 has degree n and is indecomposable with monodromy group S_n.*

Proof. We can replace k by an extension and assume that $A = G$. The condition is now that H_1 and H_2 intersect precisely the same conjugacy classes of G. Now apply [17] to conclude that H_1 and H_2 are conjugate. $\square$

If we only assume that we have a Davenport pair, one cannot hope to prove such a theorem. We can always compose with exceptional covers to obtain Davenport pairs. However, we can prove:

Theorem 9.2. *Let k be a finite field. Let $f_i : X_i \to Y$ be covers defined over k. Assume that f_1 has degree $n > 2$ and the geometric monodromy group of f_1 is S_n. If (f_1, f_2) is a Davenport pair, then we can write $f_2 = g \circ h$ (over k) with f_1 and g equivalent over k. In particular, g has degree n and is indecomposable with monodromy group S_n.*

Proof. Let A be the Galois group of the Galois closure of $k(X_1)k(X_2)$ over $k(Y)$. Let G denote the geometric Galois group. Let H_i denote the subgroups corresponding to $k(X_i)$. Let Ω_i denote the corresponding A-sets.

So $[A : H_1] = n$ and $A/K \cong S_n$ where K is the largest normal subgroup of A contained in H_1. Let $J = K \cap G$. Since Ω_1 and Ω_2/J are still Kronecker equivalent, there is no harm in assuming that $J = 1$ (this amounts to writing f_2 as a composition of covers with the outside term forming a Davenport pair with f_1). Thus, G is faithful on Ω_1 and so $G = S_n$. By Lemma 5.3, as $n > 2$, A is faithful on each Ω_i, whence $A = G = S_n$.

It follows that Ω_1 and Ω_2 are Kronecker equivalent for G. By [17] Ω_1 and Ω_2 are isomorphic G-sets. The result follows. $\square$

The previous result is not true for $n = 2$ – consider the polynomials X^2 and bX^2 with b a nonsquare. If $n = 1$, there is no content to the theorem. A modification of the proof if we replace S_n by A_n yields a similar result (but we need to assume that n is not 3 or 5).

We ask:

Question 9.3. *If (f, g) are a Davenport pair with f generic of degree $n > 2$, is $g = g_1 \circ g_2$ where g_1 is equivalent to f and g_2 exceptional?*

10. SOME EXAMPLES

Recall we saw that strong Davenport pairs with a common totally ramified rational point have degrees that are the same up to a power of the characteristic. We give some examples to show that one cannot weaken the hypotheses much.

We first recall that one can construct infinitely many pairs of (very) strong Davenport pairs – see §6.

Our next examples shows that there exist a pair (f, g) with f a polynomial and g a rational function that form a strong Davenport pair and violate the theorem on degrees.

Let k be a finite field of cardinality $q = p^a$ with $p = 5$ or $q^2 \equiv 1 \bmod 5$. Then $G = A_5$ embeds in $PSL(2, k)$.

Let $Z = \mathbb{P}^1_{k'}$. Then G acts on Z. Let $H_1 = A_4$ and $H_2 = S_3$. Consider the covers $f_i : X_i := Z/H_i \to Z/A_5$. Then f_1 is a polynomial cover of degree 5 and f_2 is a rational function of degree 10.

It is straightforward to check the following (using the group theoretic interpretation given above):

Proposition 10.1. *Let k be a finite field of cardinality $q = p^a$ with $p = 5$ or $q \equiv -1 \bmod 5$. There exists a polynomial f_1 of degree 5 and a rational function f_2 of degree 10 over k such that:*

(1) *f_1 and f_2 are a strong Davenport pair and are each indecomposable; and*
(2) *$(p-1, 5) = 1$ and $(p-1, 10) = 2$;*

We show that even for polynomials, it is not the case that strong Davenport pairs must consist of polynomials of the same degree (but this is true if the degree is prime to p – see [5] or §4).

Let G be a Borel subgroup of $PGL(2, k)$. Let H_i be any two nontrivial subgroups of G of order a power of p. Then G acts on $Z = \mathbb{P}^1_k$. The covers $f_i : X_i := Z/H_i \to Z/G$ are polynomials and are a strong Davenport pair (because H_1 and H_2 intersect precisely the same conjugacy classes in G) and need not have the same degree (as long as $q \neq p$). Thus,

Proposition 10.2. *There exist a pair of polynomials of distinct degrees which are a strong Davenport pair.*

The next example shows that there are indecomposable Davenport pairs which are neither exceptional covers or strong Davenport pairs. Moreover, each cover has a totally ramified point. We are not sure if this can happen for polynomial covers.

We give an example in characteristic $p \geq 5$. Let $A = VS_p$ (semidirect) where V is the heart of the n-dimensional permutation module for S_p over $\mathbb{F}_p$. Let $H_1 = S_n$ and set $n = |V| = p^{p-2}$. By [25], there exists a cover $f_1 : X_1 \to Y$ of degree n over some extension k of $\mathbb{F}_p$ of degree with arithmetic monodromy group A, geometric monodromy $G = VA_n$ with a totally ramified rational point. Let Z denote the curve corresponding to the Galois closure. So $X_1 = Z/H_1$. Then $H^1(S_p, V) \neq 0$. So we can choose $H_2 \leq A$ with $A = VH_2$ and H_2 not conjugate to H_1. Let f_2 be the corresponding cover from $X_1 = Z/H_2 \to Y$. If $g \in A \setminus G$, then g has a fixed point on A/H_1 if and only if it does so on A/H_2 (because any such g will have order prime to p). It follows that f_1 and f_2 are Davenport pairs and indeed will have the same image on rational points over any odd degree extension of k. On the other hand, over any even degree extension, the arithmetic monodromy group will be G. There are elements of order p in G which have fixed points on G/H_1 but not on G/H_2 (and vice versa). Thus, f_1 and f_2 have incomparable images on rational points over any even degree extension. Since A_n acts irreducibly on V, f_1 and f_2 are geometrically indecomposable.

Proposition 10.3. *There exist a Davenport pair of indecomposable covers each with a totally ramified rational point which are not a strong Davenport pair.*

11. Derangements and Cardinality of the Image

We fix some notation for the remainder of this section. Let $f : X \to Y$ be a branched degree n covering of curves over the finite field k of cardinality q. Let A and G denote the arithmetic and geometric monodromy groups and Ω the corresponding G-set of cardinality n. Set $e = |A : G|$ and for each divisor m of e, let A_m be the (unique) subgroup of A containing G with $|A : A_m| = m$. Let Z denote the curve corresponding to the Galois closure and let k' be the field of constants of Z (so $|k' : k| = e$).

We saw in §2 that $y \in \mathcal{V}_f(k)$ if and only if D, I have a common orbit on Ω, where D, I are the decomposition and inertia groups of some point in the Galois closure over y. In particular, if we ignore branch points, then $I = 1$ and D is a cyclic group. Since we are only considering $y \in Y(k)$, it follows that $A = GD$. Thus, D is generated by some element $a \in A$ with $A/G = \langle aG \rangle$ and we see that there is a rational point over y in X if and only if a has a fixed point on Ω.

The Chebotarev density theorem (see [16], [27], [26]) basically says that for k sufficiently large, the possible decomposition groups are uniformly distributed over the coset aG.

This analysis applies equally well to any finite extension field K of k – the only difference being that the arithmetic monodromy group over K is A_m where $m = \gcd(e, |K:k|)$.

Set $\rho(m)$ to be the proportion of the elements in the coset aG which have no fixed points on Ω (elements with no fixed points are called derangements).

An immediate corollary to the Chebotarev density result is the following:

Theorem 11.1. $|\mathcal{V}_f(K)| = (1 - \rho(m))|K| + O(|K|^{1/2})$, *where* $m = \gcd(|K:k|, e)$.

The constants in the error term depend on f, X, Y although one can be more precise. See [26] for more on this. One main result of [27] is:

Theorem 11.2. *Assume that f is not bijective on rational points. Then* $|\mathcal{V}_f(K)| \leq (1 - 1/n))|K| + O(|K|^{1/2})$.

This is proved as a consequence of the elementary group theoretic result that either every element in the coset aG has a unique fixed point or $\rho(m) \geq 1/n$. There are examples (even for polynomials) where this bound cannot be improved – see [9]. However, with extra hypotheses, these bounds can be greatly improved. One such result was obtained in [27]:

Theorem 11.3. *Assume that f has a totally ramified point and has degree prime to the characteristic of k. If f is not bijective on rational points, then* $|\mathcal{V}_f(K)| \leq (5/6)|K| + O(|K|^{1/2})$.

We hope to extend this result to indecomposable polynomials when n is not a power of p. Even for indecomposable polynomials of degree a power of p, one can improve the result – it is easy to classify the possibilities where the $(1 - 1/n)$ occurs. We expect to classify the cases where the main term is greater than $(1 - n^{-1/2})$ and also to show that aside from covers of degree a power of p, for any indecomposable cover, the main term is at most $1 - 1/\log(n)$. This is ongoing joint with work with Fulman.

The Chebotarev density theorem also holds for finite separable maps between higher dimensional normal varieties and the previous results can be stated in a similar manner – see [27] for some such statements.

REFERENCES

1. S. Abhyankar, Nice equations for nice groups, Israel J. Math. 88 (1994), 1–23.
2. S. Abhyankar, Symplectic groups and permutation polynomials, Part I, preprint.
3. S. Abhyankar, Shreeram S., Orthogonal groups and permutation polynomials, preprint.
4. S. Abhyankar and N. Inglis, Galois groups of some vectorial polynomials, Trans. Amer. Math. Soc. 353 (2001), 2941–2869.
5. W. Aiken, M. Fried, and L. Holt, Davenport pairs over finite fields, Pacific J. Math., to appear.
6. S. D. Cohen, Permutation Polynomials in Shum, Kar-Ping et al, ed., Algebras and combinatorics, Papers from the international congress, ICAC'97, Hong Kong, August 1997, Singapore, Springer, 133–146 (1999).
7. S. D. Cohen and M. D. Fried, Lenstra's proof of the Carlitz-Wan conjecture on exceptional polynomials: an elementary version, Finite Fields Appl. 1 (1995), 372–375.
8. S. D. Cohen and R. W. Matthews, A class of exceptional polynomials, Trans. Amer. Math. Soc. 345 (1994), 897–909.
9. T. W. Cusick and P. Müller, Wan's bound for value sets of polynomials. Finite fields and applications (Glasgow, 1995), 69–72, London Math. Soc. Lecture Note Ser., 233, Cambridge Univ. Press, Cambridge, 1996.
10. N. Elkies, Linearized algebra and finite groups of Lie type I. Linear and symplectic groups, Applications of curves over finite fields (Seattle, WA, 1997), 77–107, Contemp. Math. 245 (1999).
11. W. Feit, On symmetric balanced incomplete block designs with doubly transitive automorphism groups. J. Combinatorial Th. Ser. A 14 (1973), 221–247.
12. M. D. Fried, Galois groups and complex multiplication, Trans. Amer. Math. Soc. 235 (1978), 141-162.
13. M. D. Fried, On a theorem of MacCluer, Acta Arith. XXV (1974), 122-127.
14. M. D. Fried, Variables separated polynomials, the genus 0 problem and moduli spaces, Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), 169–228, de Gruyter, Berlin, 1999.
15. M. D. Fried, R. Guralnick, and J. Saxl, Schur covers and Carlitz's conjecture. Israel J. Math. 82 (1993), 157–225.
16. M. D. Fried and M. Jarden, Field arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 11, Springer-Verlag, Berlin, 1986.
17. R. Guralnick, Zeroes of permutation characters with applications to prime splitting and Brauer groups, J. Algebra 131 (1990), 294–302.
18. R. Guralnick, Some applications of subgroup structure to probabilistic generation and covers of curves, Algebraic groups and their representations (Cambridge, 1997), 301–320, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 517, Kluwer Acad. Publ., Dordrecht, 1998.
19. R. Guralnick, Monodromy groups of coverings of curves, to appear.
20. R. Guralnick and P. Müller, Exceptional polynomials of affine type. J. Algebra 194 (1997), no. 2, 429–454.

21. R. Guralnick, P. Müller, and J. Saxl, The rational function analogue of a question of Schur and exceptionality of permutation representations, Memoirs Amer. Math. Soc., to appear.
22. R. Guralnick, J. Rosenberg and M. Zieve, A new class of exceptional polynomials in characteristic 2, preprint.
23. R. Guralnick and J. Saxl, Monodromy groups of polynomials, Groups of Lie type and their geometries (Como, 1993), 125–150, London Math. Soc. Lecture Note Ser., 207, Cambridge Univ. Press, Cambridge, 1995.
24. R. Guralnick and J. Saxl, Exceptional polynomials over arbitrary fields, to appear.
25. R. Guralnick and K. Stevenson, Prescribing ramification, in Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), 387–406, Proc. Sympos. Pure Math., 70, Amer. Math. Soc., Providence, RI, 2002.
26. R. Guralnick, T. Tucker and M. Zieve, Exceptional covers and bijections on rational points, preprint.
27. R. Guralnick and D. Wan, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, Israel J. Math. 101 (1997), 255–287.
28. R. Guralnick and M. Zieve, Polynomials with monodromy $PSL(2,q)$, preprint.
29. H. Lenstra, D. Moulton and M. Zieve, Exceptional covers, in preparation.
30. H. Lenstra and M. Zieve, A family of exceptional polynomials in characteristic three, Finite fields and applications (Glasgow, 1995), 209–218, London Math. Soc. Lecture Note Ser., 233, Cambridge Univ. Press, Cambridge, 1996.
31. P. Müller, New examples of exceptional polynomials. Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993), 245–249, Contemp. Math., 168, Amer. Math. Soc., Providence, RI, 1994.
32. P. Müller, Primitive monodromy groups of polynomials, Recent developments in the inverse Galois problem (Seattle, WA, 1993), 385–401, Contemp. Math., 186, Amer. Math. Soc., Providence, RI, 1995.
33. P. Müller, Kronecker conjugacy of polynomials, Trans. Amer. Math. Soc. 350 (1998), 1823–1850.
34. P. Müller, Kronecker conjugacy of polynomials. Trans. Amer. Math. Soc. 350 (1998), 1823–1850.
35. J.-P. Serre, Local Fields, Translated from the French by Marvin Jay Greenberg. Grad. Texts Math. 67. Springer-Verlag, New York-Berlin, 1979.
36. B. L. van der Waerden, Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen, Math. Ann. 111 (1935), 731–733.

Robert M. Guralnick,
Department of Mathematics,
University of Southern California,
Los Angeles, CA 90089-1113, USA
guralnic@math.usc.edu

Received on 6 January 2002.