**Bounds For Fixed Point Free Elements In A Transitive Group and Applications to Curves over Finite Fields**


Robert Guralnick†
Department of Mathematics
University of Southern California
Los Angeles,CA 90089
guralnic@mtha.usc.edu

Daqing Wan†
Department of Mathematics
Pennsylvania State University
University Park, PA 16802
wan@math.psu.edu



We investigate $V_f$, the cardinality of the value set of a polynomial $f$ of degree $n$ over a finite field of cardinality $q$. It has been shown that if $f$ is not bijective, then $V_f \leq q-(q-1)/n$. Polynomials do exist which essentially achieve that bound. We do prove that if the degree of $f$ is prime to the characteristic and $f$ is not bijective, then asymptotically $V_f \leq (5/6)q$. We consider related problems for curves and higher dimensional varieties. This problem is related to the number of fixed point free elements in finite groups, and we prove some results in that setting as well.


## 1. Introduction

We begin with an arithmetic question which motivated our interest in the group theoretic problem of estimating the number of fixed point free elements in a transitive group.

Let $\mathbf{F}_q$ be a finite field of $q$ elements with characteristic $p$ and let $f(T)$ be a polynomial of degree $n$ $(n>1)$ in $\mathbf{F}_q[T]$ which is not a polynomial in $T^p$. The arithmetic question raised by Chowla [Ch] is to estimate the number $V_f$ of distinct values taken by $f(T)$ as $T$ runs over $\mathbf{F}_q$. Birch and Swinnerton-Dyer [BS] showed that if the Galois group of $f(T)-t=0$ over $\bar{\mathbf{F}}_q(t)$ is the symmetric group $S_n$, then

$$V_f = (\sum_{k=1}^{n} \frac{(-1)^{k-1}}{k!})q + O(\sqrt{q}), \tag{1.0}$$

where the constant in the error term depends only on $n$. The above formula was conjectured by Chowla and others.

In this paper, we are interested in upper bounds for $V_f$. It is clear that $V_f \leq q$ with equality holding if and only if $f(T)$ is a permutation polynomial over $\mathbf{F}_q$. If $V_f < q$, then


† both authors partially supported by the NSF

we have the following elementary upper bound for $V_f$ as conjectured in [Mu] and proved in [Wa]:

$$V_f \leq q - (q-1)/n, \tag{1.1}$$

Simple proofs of (1.1) have been given by Turnwald [Tu] and Lenstra (personal communication). We would like to know if the bound in (1.1) is reasonably good asymptotically when $q$ is large compared to $n$. This would depend on the polynomial $f(T)$ in consideration.

It is well known that there is an asymptotic formula for $V_f$ in terms of certain Galois groups (cf. [Co]). More precisely, let $G$ be the Galois group of $f(T) - t = 0$ over $\mathbf{F}_q(t)$ and let $N$ be the Galois group of $f(T) - t = 0$ over $\bar{\mathbf{F}}_q(t)$, where $\bar{\mathbf{F}}_q$ is an algebraic closure of $\mathbf{F}_q$. Both groups act transitively on the $n$ roots of $f(T) - t = 0$. The geometric monodromy group $N$ is a normal subgroup of the arithmetic monodromy group $G$. The quotient $G/N$ is a cyclic group (possibly trivial). Let $xN$ be the coset which is the Frobenius generator of the cyclic group $G/N$. The Cebotarev density theorem for function fields yields the following asymptotic formula:

$$V_f = (1 - \frac{|S_0|}{|N|})q + O(\sqrt{q}), \tag{1.2}$$

where $S_0$ is the set of group elements in the coset $xN$ which fix no roots of $f(T) - t = 0$. Note that the constant in the above error term depends only on $n$, not on $q$. Thus, to understand the asymptotic behavior of $V_f$, it suffices to understand the quotient

$$s_0 = \frac{|S_0|}{|N|}.$$

It is clear that $s_0 \geq 0$ with equality holding if and only if $f(T)$ is an exceptional polynomial over $\mathbf{F}_q$ (see [FGS] for a classification of the possible monodromy groups for exceptional polynomials). Lenstra recently observed that if $s_0 > 0$, then $s_0 \geq 1/n$ with equality holding if and only if $G = N$ is a Frobenius group of order $n(n-1)$ with $n$ a prime power. Our purpose here is to find the next possible value for $s_0$ assuming $s_0 > 1/n$. We have

**Theorem 1.1.** *Let $f(T)$ be a polynomial over $\mathbf{F}_q$ of degree $n > 6$ which is not a polynomial in $T^p$. If $s_0 > 1/n$, then $s_0 \geq 2/n$ with equality holding if and only if $G = N$ is a Frobenius group of order $n(n-1)/2$ with $n$ a prime power. In particular, $V_f \leq (1 - 2/n)q + O_n(\sqrt{q})$ unless $f$ is exceptional or $G = N$ is a Frobenius group of order $n(n-1)$.*

As it will be seen in the next section, our proof of the Theorem above is significantly harder than the proof of the bound $s_0 \geq 1/n$ for $s_0 \neq 0$. In fact, in addition to some non-trivial elementary arguments, we also have to use the classification of finite simple groups. We do not know an elementary proof of Theorem 1.1. It was suggested by Lenstra that if the polynomial $f(T)$ is tame (i.e. all ramifications of the corresponding cover of $\mathbb{P}^1$ to $\mathbb{P}^1$ are tame), then it should be possible to have an absolute lower bound $s_0 > c$ for some absolute positive constant $c$. We show that this is indeed the case. Indeed, we only need to assume that there is tame ramification at $\infty$ (or equivalently the degree is prime to the characteristic).

**Theorem 1.2.** *Let $f(T)$ be a polynomial over $\mathbf{F}_q$ of degree $n > 1$ with $n$ not divisible by the characteristic of $\mathbf{F}_q$. Then we have $s_0 > 1/6$ whenever $s_0 > 0$. In particular, either $f$ is bijective or $V_f \leq (5/6)q + O_n(\sqrt{q})$.*

No attempt is made here to optimize the constant $1/6$. If $n$ is not a multiple of $p$, there will be polynomials whose monodromy groups are $S_n$ or the dihedral group of order $2n$. This shows that $1/6$ cannot be improved to any better than $1/e$ (symmetric groups) or more easily $1/2$ (dihedral groups) even for $f$ indecomposable and $n$ large. If we assume that all ramification is tame, then we show that $s_0 > 0$ implies that $s_0 \geq 16/63$ and that the bound is best possible (see Corollary 4.8).

If we drop the assumption that $n$ is prime to $p$, then the result is false. The Frobenius group of order $p^a(p^a - 1)$ can be identified with the group of upper triangular matrices in $PGL_2(p^a)$ and so acts on $\mathbb{P}^1$. Moreover, it fixes $\infty$. Thus, there is a polynomial $f$ of degree $p^a$ whose geometric monodromy group is Frobenius of order $p^a(p^a - 1)$. It can be written down explicitly – it satisfies $f(x^{p^a-1}) = (x^{p^a} - x)^{p^a-1}$ and thus $f(x) = x(x-1)^{p^a-1}$. If $p^a - 1$ divides $q - 1$, then the arithmetic monodromy group is equal to the geometric monodromy group. Thus, $s_0 = 1/p^a = 1/n$.

In terms of the value set, one can compute directly that $V_f = qd/(d+1)$, where $d = (p^a - 1, q - 1)$ (this has been considered by Müller, Flynn and Cusick ). In particular, the elementary bound in (1.1) is attained for this polynomial $f(x)$ of degree $n = p^a$ if $\mathbf{F}_q$ contains $\mathbf{F}_{p^a}$ as a subfield.

Again, our proof of Theorem 1.2 depends on the classification of finite simple groups. In terms of our motivating question on value sets, this shows that if the degree $n$ is not divisible by $p$ and if $V_f < q$, then

$$V_f \leq \frac{5}{6}q + O(\sqrt{q}). \tag{1.3}$$

This is a vast improvement of (1.1) if $q$ is large compared to $n$ and $n$ is not divisible by $p$.

Some of the above results can be generalized to coverings of non-singular curves and even to coverings of higher dimensional varieties. See sections 3-5. The higher dimensional value set problem was first considered by Serre [S2] in connection with Hilbert's irreducibility theorem and the inverse Galois problem. Let $f : Y \longrightarrow Z$ be a finite morphism of degree $n$ between two absolutely irreducible $m$-dimensional ($m > 0$) quasi-projective varieties defined over $\mathbf{F}_q$. Let $V_f$ be the cardinality of the value set $f(Y(\mathbf{F}_q))$. Assume that $f$ is not exceptional over $\mathbf{F}_q$, i.e., the fiber product $Y \times_Z Y$ with its diagonal removed contains some absolutely irreducible component of dimension $m$ defined over $F$. Then, we have the bound

$$V_f \leq (1 - \frac{1}{n})q^m + O(q^{m-1/2}). \tag{1.4}$$

The weaker estimate

$$V_f \leq (1 - \frac{1}{n!})q^m + O(q^{m-1/2}). \tag{1.5}$$

was given in [S2, Theorem 3.6.2]. The higher dimensional bound in (1.4) holds because there is a similar Cebotarev density theorem for higher dimensional varieties, see Fried

[Fr2, section 4]. More higher dimensional results are given in section 5, as well as a direct geometric proof avoiding the Cebotarev density theorem.

In the special case that $G = N$, the above group theoretic question about $s_0$ also arises naturally in other context. Let $G$ be a transitive permutation group acting on a set $X$ of $n$ letters with $n > 2$. Let $S_0$ be the set of elements of $G$ which fix no letters of $X$. A classical simple result of Jordan [Jo] says that $|S_0| > 0$. Motivated by number theoretic and algorithmic applications such as the number field sieve [BLP, Section 9], Lenstra (1990) asked the question of finding a good lower bound for the quotient

$$s_0(G) = \frac{|S_0|}{|G|},$$

see the paper by Boston et al [Bo]. Soon afterwards, Cameron and Cohen [CC] showed that $s_0(G) \geq 1/n$ with equality holding if and only if $G$ is a Frobenius group of order $n(n-1)$, where $n$ is a prime power. A simpler proof of the Cameron-Cohen result is given in [Bo] where the value $s_0(G)$ is calculated for several classes of groups. A natural open problem as posed in [Bo, p. 3274] is to find the next possible bound if $s_0 > 1/n$ and classify the optimal groups. This problem is solved here.

**Theorem 1.3.** *Let $G$ be a transitive permutation group of degree $n$. One of the following holds:*
(a) *$G$ is a Frobenius group of order $n(n-1)$ with $n$ a prime power and $s_0(G) = 1/n$;*
(b) *$G$ is a Frobenius group of order $n(n-1)/2$ with $n$ an odd prime power and $s_0(G) = 2/n$;*
(c) *$G = S_4(n = 4, s_0 = 3/8), S_5(n = 5, s_0 = 11/30)$, $A_5(n = 5, 6, s_0 = 2/n)$, $Z/2(n = 2, s_0 = 1/2)$ or $Z/3Z(n = 3, s_0 = 2/3)$; or*
(d) *$s_0(G) > 2/n$.*

**Acknowledgment**. The second author would like to thank H. W. Lenstra, Jr for valuable discussions on the above problem about $s_0$. We would also like to thank Peter Müller and Michael Zieve for comments on an earlier version of the paper and Michael Fried for discussions on the Cebatorev density theorem.

## 2. The Case $G = N$

In this section, we prove the group theoretic Theorem 1.3. Let $G$ be a transitive permutation group acting on a set $X$ of $n$ letters. To prove the theorem, we first derive some elementary bounds which relate the number $s_0$ to the minimal degree $\mu$ of the group $G$. Recall that $\mu$ is the minimal number of elements moved by a non-identity element of $G$. A detailed investigation of the minimal degree is given in Liebeck-Saxl [LS].

We digress slightly for a brief discussion of Frobenius groups. See [Pa] for more details. $G$ is said to be regular on $X$ if no nontrivial element fixes a point. $G$ is called a Frobenius group on $X$ if $G$ is not regular on $X$ but no nontrivial element fixes more than 1 point. If $G$ is Frobenius, it follows by character theory that $G$ contains a normal subgroup $A$ acting regularly (and in particular transitively) on $X$. Thus, $|A| = n$ and we can identify $X$ with $A$. If $G$ is regular or Frobenius, it follows that $|G| = nd$ where $d|(n-1)$. Thus, $s_0 = (n-1)/dn$.

We consider 2 special cases. If $d = n-1$, it follows that any two nonidentity elements of $A$ are conjugate in $G$, whence $A$ is an elementary abelian $p$-group for some prime $p$ (and so $n$ is a power of $p$). If $d = (n-1)/2$, there are two conjugacy classes (in $G$) of nonidentity elements in $A$ each of size $d$. It is an easy exercise to prove that this again implies that $A$ is an elementary abelian $p$-group for some prime $p$ (necessarily odd) and $n$ is a power of $p$.

More generally, it follows by a result of Thompson that for any Frobenius group the normal subgroup $A$ is nilpotent.

For $0 \le i \le n$, let $S_i$ be the set of elements of $G$ which fix exactly $i$ letters of $X$. Define $s_i = s_i(G) = |S_i|/|G|$. It follows from the definition that $s_n = 1/|G|$ and $s_{n-1} = \cdots = s_{n-\mu+1} = 0$, where $\mu$ is the minimal degree of $G$. We want to estimate $s_0$. Trivially, we have the relation

$$s_0 + s_1 + s_2 + \cdots + s_n = 1. \tag{2.1}$$

To derive more relations among the numbers $s_i$, we define $X_j$ $(1 \le j \le n)$ to be the $j$-fold Cartesian product with all diagonals removed. Namely, the set $X_j$ consists of all $j$-tuples from $X$ with all coordinates distinct. Let $r_j$ be the number of orbits of $X_j$ under the coordinate-wise action of $G$. Since $G$ is transitive, we have $r_1 = 1$. We may apply Burnside's formula (or use elementary character theory) to the action of $G$ on $X_j$ and deduce the following relations:

$$\sum_{i=j}^{n} \binom{i}{j} s_i = \frac{r_j}{j!}, \ 1 \le j \le n. \tag{2.2}$$

To estimate $s_0$, we try to eliminate some of the numbers $s_i$ from the above relations. Subtract (2.1) from the first equation of (2.2), one sees that

$$s_0 = \frac{r_1}{1!} - (1 - s_0) = \sum_{i=2}^{n} \binom{i-1}{1} s_i. \tag{2.3}$$

Multiply equation (2.3) by $n/2$ and subtract the second equation of (2.2), one checks that

$$\frac{ns_0}{2} - \frac{r_2}{2} = \sum_{i=2}^{n-\mu} \frac{(n-i)(i-1)}{2} s_i \ge 0. \tag{2.4}$$

This immediately gives the previously known bound $s_0 \ge r_2/n$ $(\ge 1/n)$ with equality holding if and only if all $s_i = 0$ for $2 \le i < n$, namely, $G$ is a Frobenius group of order $n(n-1)$ or $\mathbb{Z}/2$ (for $n = 2$).

To obtain finer bounds, we need to make use of $r_3$. Multiply the second equation of (2.2) by $(n-2)/3$ and subtract the third equation of (2.2), we deduce that

$$\frac{(n-2)r_2 - r_3}{3!} = \sum_{i=2}^{n-\mu} \frac{(n-i)i(i-1)}{3!} s_i \ge 0. \tag{2.5}$$

Now, we eliminate $s_{n-\mu}$ from (2.4) and (2.5). Multiply (2.4) by $(n-\mu)/3$ and subtract (2.5), it follows that

$$\frac{n-\mu}{3}\left(\frac{ns_0}{2}-\frac{r_2}{2}\right)-\frac{(n-2)r_2-r_3}{3!}=\sum_{i=2}^{n-\mu-1}\frac{(n-i)(n-\mu-i)(i-1)}{3!}s_i\geq 0.$$

Solving this inequality, we derive the bound

$$s_0\geq\frac{r_2}{n}+\frac{(n-2)r_2-r_3}{n(n-\mu)}. \tag{2.6}$$

Note that the last term in (2.6) is always nonnegative in view of (2.5). It is strictly positive unless $G$ is a Frobenius group (i.e., $s_2=\cdots=s_{n-1}=0$). If $G$ is a Frobenius group, then $s_0=(n-1)/|G|$ and so $s_0>2/n$ unless $|G|=n(n-1)$ or $n(n-1)/2$. Since the one point stabilizer $G_x$ acts as fixed point free automorphisms of the regular normal subgroup $N$ of $G$, it follows easily that $n=|N|$ is a prime power.

If $n\leq 6$, Theorem 1.3 follows by inspection of the various primitive groups. To prove the theorem, we may therefore assume that $n>6$, $r_2=1$ and $1<r_3<n-2$; namely, $G$ is 2-transitive but neither 3-transitive nor sharply 2-transitive (since $n>6$). We shall assume this condition throughout the remainder of this section. Thus, the bound in (2.6) reduces to

$$s_0\geq\frac{1}{n}+\frac{n-(r_3+2)}{n(n-\mu)}. \tag{2.7}$$

We want to prove that $s_0>2/n$. Note that the number $(r_3+2)$ in (2.7) is just the number of orbits of the stabilizer of two letters acting on $X$ since $G$ is doubly transitive. By (2.7), we have

**Lemma 2.1.** *If $(r_3+2)<\mu$, then $s_0>2/n$.*

We now derive a simple bound for $r_3+2$ in terms of $\mu$. Multiply the second equation of (2.2) by $(n-\mu-2)/3$ and subtract the third equation of (2.2), one computes that

$$\frac{(n-\mu-2)-r_3}{3!}\geq-\frac{n(n-1)\mu}{3!|G|}. \tag{2.8}$$

Namely,

$$(r_3+2)\leq n-\mu+[n(n-1)\mu/|G|], \tag{2.9}$$

where $[x]$ denotes the integral part of $x$.

As a trivial application of (2.9), we have $r_3+2\leq n-\frac{\mu}{2}$ since $|G|\geq n(n-1)2$ for $G$ 2-transitive but not sharply. The equality $(r_3+2)=n-\frac{\mu}{2}$ holds only if $|G|=n(n-1)2$. This can also be proved directly: the number $(r_3+2)$ of orbits of the stabilizer of two letters is the sum of the number $(\leq n-\mu)$ of orbits of length one and the number $(\leq\mu/2)$ of orbits of length greater than one.

By (2.7) and the remark above, we have:

**Lemma 2.2.** (a) *If $\mu > 2n/3$, then $s_0 > 2/n$;*
(b) *If $\mu = 2n/3$, then $s_0 > 2/n$ unless $G_{xy}$ is a subgroup of order 2.*

**Remark**. Manning's (cf. [Wi] ) classical bound $\mu > n/3 + O(\sqrt{n})$ together with (2.9) easily gives the weaker inequality $s_0 > (\frac{5}{4} - \epsilon)/n$ if $s_0 > 1/n$. But this is a little far from the optimal $2/n$.

We still assume $G$ is 2-transitive and neither sharply 2-transitive nor 3-transitive.

We first consider the affine case. So $G$ is a 2-transitive subgroup of $A\Gamma L_d(q)$, the group of affine semilinear transformations of a $d$-dimensional space $V$ of $\mathbf{F}_q$ with $n = q^d$. Note that we can identify $V$ as a subgroup of $G$ (acting via translation) and $G = VG_0$, where $G_0$ is the stabilizer of 0. So $G_0$ is a subgroup of $\Gamma L_d(q)$, the group of semilinear transformations.

**Lemma 2.3.** (a) *If $d > 1$, then $\mu \geq (q-1)n/q$.*
(b) *If $d = 1$ and $q$ is prime, then $\mu = q - 1$.*
(c) *If $d = 1$ and $q = q_0^e$ with $e$ prime and minimal, then $\mu \geq q - q_0$.*

**Proof.** Let $1 \neq g \in G$ fixing 0 which moves the fewest points. We may assume that $g$ has prime order. If $g$ is linear, then its fixed points form a proper subspace and so $g$ moves at least $q^d - q^{d-1}$ points. Otherwise, $g$ is conjugate to a field automorphism (this follows by Lang's theorem). It follows that the number of fixed points is $q_0^d$ where $q = q_0^e$. If $d > 1$, the linear case is worst possible. If $d = 1$ and $q$ is prime, then only the linear case occurs. ∎

Combining Lemma 2.2 and Lemma 2.3 yields that $s_0 > 2/n$ unless $q \leq 3$ or $d = 1$ and $q = 4$ or 9. If $d = 1$ and $q = 4$ or 9, then the result follows easily by inspection.

Moreover, if $q = 3$, the result follows from Lemma 2.2(b) unless $\mu = 2n/3$ and $G_{0v}$ has order 2. Let $1 \neq g \in G_{0v}$. If $d = 1$ or 2, the result follows by inspection. Let $g \neq h$ be a conjugate of $g$ in $G_0$ (since $G_0$ is transitive on the nonzero vectors in $V$, such $h$ exists). Then $g$ and $h$ are trivial on some $d - 2$ dimensional space and so are both contained in $G_{0w}$ for some $w$. This contradicts the fact that $G_{0w}$ has order 2.

So we may assume that $q = 2$. If $d \leq 2$, the result follows by inspection. If $G_0$ does not contain any transvections (i.e. unipotent elements fixing a hyperplane), then $\mu \geq 3n/4$. Lemma 2.2 gives $s_0 > 2/n$. Thus, $G_0$ is a transitive subgroup on $V - \{0\}$ of $GL_d(2)$ containing transvections. It follows by McLaughlin [Mc] that $G_0 = SL_d(2)$ or $Sp_d(2)$ (with $d \geq 4$ even in the last case). In the first case, $G_0$ is 2-transitive on $V - \{0\}$ and so $G$ is 3-transitive. In the latter case, $G_{0v}$ has 3 orbits on nonzero vectors (depending upon the inner product with $v$) and so $r_3 + 2 = 4$. Since $\mu = n/2$ and $n \geq 16$, the result holds here by Lemma 2.1.

In fact, one does not need to use McLaughlin's result here. If $d \leq 3$, this is obvious. For $d > 3$, we can find three transvections which act irreducibly on a 3-dimensional space. If $d > 3$, this group is contained in $G_{0w}$ for some $w$. Then $r_3 + 2 \leq n/4$ and $\mu = n/2$. The result holds here by Lemma 2.1.

This completes the proof for the bound $s_0 > 2/n$ for $G$ in the affine case (note that this also completes the proof for the general result if $G$ is solvable).

We now assume that $G$ does not preserve an affine structure on the set. We are still assuming that $G$ is 2-transitive but not 3-transitive. It follows easily that $G$ contains a simple nonabelian normal subgroup $L$ with $L \subseteq G \subseteq \mathrm{Aut}(L)$ (cf. [Wi, Ex. 12.4]). The following table lists all such 2-transitive groups aside from the cases where $L$ is alternating or a Mathieu group (in which case $L$ is 3-transitive – note that $M_{11}$ has a multiply transitive representations of degree 11 and 12).

The table lists the simple group $L$, the permutation degree $n$, an upper bound for $n-\mu$ and an upper bound for $r_3+2$.

Unfortunately the table depends upon the classification of finite simple groups (see Kantor [Ka]):

**Table 1: 2-transitive Almost Simple Groups**

| $L$ | $n$ | $n-\mu$ | $r_3+2$ |
|---|---|---|---|
| $L_2(q), 4 < q$, $q$ not prime | $q+1$ | $q^{1/2}+1$ | 4 |
| $L_2(p), 4 < p$, $p$ prime | $p+1$ | 2 | 4 |
| $\mathrm{Sz(q), q} = 2^{2e+1} \geq 8$ | $q^2+1$ | $q^{2/3}+1$ | $q+3$ |
| ${}^2G_2(q), q = 3^{2e+1} \geq 27$ | $q^3+1$ | $q+1$ | $q^2+q+4$ |
| $U_3(q), q > 2$ and nonsquare | $q^3+1$ | $q+1$ | $3q+2$ |
| $U_3(q)$, $q$ square | $q^3+1$ | $q^{3/2}+1$ | $3q+2$ |
| $L_d(q), d \geq 3$ | $(q^d-1)/(q-1)$ | $(q^{d-1}-1)/(q-1)$ | 4 |
| $\mathrm{Sp_{2d}}(2), \mathrm{d} \geq 3$ | $2^{2d-1} \pm 2^{d-1}$ | $2^{2d-2}$ | 4 |
| $A_7$ | 15 | 7 | 4 |
| $L_2(11)$ | 11 | 3 | 4 |
| $L_2(8)$ | 28 | 4 | 16 |
| HS | 176 | 16 | 5 |
| $\mathrm{Co}_3$ | 276 | 36 | 4 |

A few comments are in order about the table. In all cases except $L = L_2(8)$, $L$ itself is 2-transitive. The information for the last five cases can be read off from [ATLAS]. If $L = L_d(q)$, the action is on the 1-spaces (or hyperplanes) of a $d$-dimensional vector space over $\mathbf{F}_q$ and all quantities are easy to compute. If $L = U_3(q)$, the action is on singular 1-spaces (singular with respect to a hermitian form) in a three dimensional space over $\mathbf{F}_{q^2}$ and the estimates are quite easy to obtain.

If $L = \mathrm{Sz}(q)$ or ${}^2G_2(q)$, these estimates follow easily from well known properties of the groups (cf. [HB, 10.3.10, 11.13.2]).

Finally, if $L = \mathrm{Sp_{2d}}(2)$, then $G = L$ and the point stabilizers are $O^{\pm}_{2d}(2)$ and the action on the nontrivial orbit is just the natural action of the orthogonal group on singular vectors. This easily gives $r_3+2 = 4$. The maximum number of fixed points for a nonidentity element is bounded by $1+k$ where $k$ is the number of singular vectors in a hyperplane.

In all cases, it follows that $r_3 + 2 < \mu$ (except $L = L_2(p) \cong A_5$ with $p = 5$ and $n = 6$ – in that case, it follows that $s_0 = 1/3 = 2/n$ if $G = L$ and $s_0 > 2/n$ for $G = PGL_2(5)$). The proof of Theorem 1.3 is complete. ■

To conclude this section, we note that for those groups $G$ with $r_2 = 1$ and $r_3 \leq 2$, an absolute positive lower bound for $s_0$ can be obtained. In fact, by an inclusion-exclusion argument, one sees that the alternating sum of equation (2.1) with the first three equations of (2.2) gives that for $n > 3$,

$$\begin{aligned} s_0 &> \sum_{i=0}^{n}(\binom{i}{0} - \binom{i}{1} + \binom{i}{2} - \binom{i}{3})s_i \\ &= 1 - \frac{r_1}{1} + \frac{r_2}{2!} - \frac{r_3}{3!} \\ &= \frac{r_2}{2} - \frac{r_3}{6}. \end{aligned} \tag{2.10}$$

This can also be checked directly from the the following inclusion-exclusion inequality

$$\binom{i}{0} - \binom{i}{1} + \binom{i}{2} - \binom{i}{3} \begin{cases} = 1, & \text{if } i = 0, \\ = 0, & \text{if } i = 1, 2, 3, \\ < 0, & \text{if } i > 3. \end{cases}$$

and the fact that $s_n = 1/|G| > 0$. In particular, we have

**Corollary 2.4.** *Let $n > 3$. If $r_3 = 1$, then $s_0 > 1/3$. If $r_2 = 1$ and $r_3 = 2$, then $s_0 > 1/6$.*

A similar inclusion-exclusion argument shows that for $n > 2$,

$$\begin{aligned} s_0 &< \sum_{i=0}^{n}(\binom{i}{0} - \binom{i}{1} + \binom{i}{2})s_i \\ &= 1 - \frac{r_1}{1} + \frac{r_2}{2!} \\ &= \frac{r_2}{2}. \end{aligned} \tag{2.11}$$

Thus, we have

**Corollary 2.5.** *Let $n > 2$. If $r_2 = 1$, then $s_0 < 1/2$.*

## 3. The General Case

In this section, we study the general case when $G$ may not be equal to $N$. Let $G$ be a group with a normal subgroup $N$ with $G/N$ cyclic. Let $x$ denote a generator for $G/N$. We generalize the notions discussed earlier. We have a complete generalization of Theorem 1.3 only for those pair $(G, N)$ which comes from a covering of connected smooth projective curves with a totally ramified $\mathbf{F}_q$-rational point. First we note the following easy result (which is essentially proved in [FGS, §13]). We give a different proof suggested by Müller.

**Lemma 3.1.** *Let $G$ act on a finite set $X$. Let $\phi$ denote the following permutation character: $\phi(g) = |X^g|$. Let $r = r(X)$ be the number of common $G, N$ orbits on $X$. Then*

$$(1/|N|) \sum_{g \in xN} \phi(g) = r.$$

**Proof.** Clearly, we may assume that $G$ is transitive on $X$. Note that $N$ is also transitive on $X$ if and only if $xg$ has a fixed point for some $g \in N$. So, $N$ is not transitive if and only if both sides of the equation are 0. So assume that $G$ and $N$ are both transitive (so $r = 1$).

Set

$$Y = \{(xg, \omega) \in xN \times X | xg(\omega) = \omega\}.$$

Let $G_\omega$ be the point stabilizer in $G$ of $\omega$ (and similarly for $N$). On one hand, $|Y| = \sum_{g \in xN} \phi(g)$. On the other hand, if $\omega \in X$ and $xg$ fixes $\omega$, then $G_\omega \cap xN = xgN_\omega$. In particular, there are $|N_\omega|$ elements in $G_\omega \cap xN$. Thus, $|Y| = |X||N_\omega| = |N|$ as desired. ■

Now assume that $G$ and $N$ are both transitive on $X$. We will denote the cardinality of $X$ by $n$. By passing to a quotient, we may always reduce to the case that $G$ is faithful on $X$. We assume that from now on.

Let $S_i$ be the set of elements in the coset $xN$ which fix exactly $i$ elements of $X$. Let $s_i = |S_i|/|N|$. Let $r_i$ be the number of common $G, N$ orbits on the $i$-fold cartesian product of $X$ with the diagonals removed (so all coordinates are distinct).

We first note that:

**Lemma 3.2.** *The following are equivalent:*
(a) $r_2 = 0$;
(b) $s_0 = 0$;
(c) *Every element in the coset $xN$ fixes a unique point;*
(d) *Every element in the coset $xN$ fixes at most one point;*
(e) *Every element in the coset $xN$ fixes at least one point.*

**Proof.** The equivalence of (c)-(e) follows from Lemma 3.1 (see also [FGS, 13.1]). Clearly (b) and (e) are equivalent. Note $G(a, b) = N(a, b)$ if and only if some element in $xN$ fixes $(a, b)$. So $r_2 \neq 0$ is equivalent to some element in $xN$ fixing at least two points. Thus, (a) is equivalent to (d). ■

The triple $(G, N, X)$ is called exceptional if it satisfies the above conditions. If $G$ is the arithmetic monodromy group of a branched covering (always separable) of connected smooth projective curves over a finite field and $N$ is the geometric monodromy group, then these triples correspond to exceptional coverings (see [FGS]).

**Lemma 3.3.** *Let $H$ be a point stabilizer of some point of $X$. Let $K$ be a subgroup of $G$ containing $H$. Let $Y$ be the coset space $G/K$ and $Z$ the coset space $K/H$.*
(a) $s_0(G, N, X) \geq s_0(G, N, Y)$;
(b) *if $(G, N, Y)$ is exceptional, then $s_0(G, N, X) = s_0(K, N \cap K, Z)$; and*
(c) *$(G, N, X)$ is exceptional if and only if $(G, N, Y)$ and $(K, N \cap K, Z)$ are exceptional.*

**Proof.** Since $N$ is transitive, it follows that $G = HN = KN$ and so $x(N \cap K)$ generates $K/(N \cap K)$. If $x$ fixes no point in $Y$, then clearly it fixes no point in $X$, whence (a).

Assume that $(G, N, Y)$ is exceptional. Let $K_y$ denote the stabilizer of a point $y \in Y$. Then $xN$ is a disjoint union of the $xN \cap K_y$, $y \in Y$ (since each element of $xN$ fixes a unique point of $Y$). The number of fixed point free elements in each intersection is independent of $y$ (since these sets are all conjugate). Thus, the number of fixed point free elements on $X$ is $|Y|S_0(K, K \cap N, Z)$ and (b) holds.

If $X$ is exceptional, then (a) implies $Y$ is. On the other hand, if $Y$ is exceptional, then (b) implies that $X$ is exceptional if and only if $Z$ is. This proves (c), which can also be easily deduced from Lemma 3.2. ∎

In [FGS], it was proved that if $(G, N, X)$ is an exceptional triple with $G$ primitive on $X$ which corresponds to an exceptional covering of connected smooth projective curves over a finite field with a rational point that is totally ramified (e.g., if $f$ is an exceptional polynomial), then $G$ was shown to be either a solvable group of prime degree or an affine group of degree a power of the characteristic or one additional infinite family in characteristic 2 or 3. Moreover, the previous lemma shows that any exceptional covering is a composition of primitive exceptional coverings (see [FGS]).

Now assume that $r_2 \geq 1$. Arguing exactly as in section 2, we obtain:

$$s_0 \geq \frac{r_2}{n} + \frac{(n-2)r_2 - r_3}{n(n-\mu)}. \tag{3.1}$$

Moreover, the last term on the right is strictly positive unless for each $(a, b)$ with $G(a, b) = N(a, b)$, $G_{a,b} = 1$. Since $G = NG_{a,b}$, this implies that $G = N$ and $G$ is a Frobenius group. This case has already been handled. Lemmas 2.1-2.2 are also valid in the present more general case.

Thus, we have shown:

**Lemma 3.4.** (a) *If $r_2 > 0$, then either $s_0 > r_2/n$ or $G = N$ is a Frobenius group (or regular group) on $X$.*

(b) *If $G = N$ is a Frobenius group (or regular group) on $X$, then $s_0 = r_2/n$.*

(c) *If $r_2 > 1$, then $s_0 \geq 2/n$ with equality holding if and only if either $G = N$ is a Frobenius group of order $n(n-1)/2$ with $n$ an odd prime power or $G = N$ is cyclic of order 3.*

(d) *If $r_2 = 1$, then $s_0 \geq 1/n$ with equality if and only if $G = N$ is a Frobenius group of order $n(n-1)$ with $n$ a prime power or $G = N$ is cyclic of order 2.*

If $G$ is a Frobenius group and $G \neq N$, then every element in $xN$ has at most one fixed point, whence exactly one and so $G$ is exceptional.

**Lemma 3.5.** *If $G$ is not primitive on $X$, then one of the following holds:*

(a) *$s_0 > 2/n$;*

(b) *$(G, N, X)$ is exceptional; or*

(c) *$n = 4$, $G$ has order 8, $N$ has order 4 and $s_0 = 2/n$.*

**Proof.** If $r_2 = 0$, then the triple is exceptional. If $r_2 > 1$, then $s_0 > 2/n$ unless $G$ is Frobenius of order $n(n-1)/2$ and so is primitive.

So we may assume that $r_2 = 1$. If $G = N$, then $G$ is 2-transitive and primitive.

First consider the case that $n = 4$. It follows that $G$ is a 2-group (otherwise $G$ is 2-transitive). If it has order 4, then $G$ acts regularly, whence $s_0 \geq 3/n$. Otherwise, $G$ is dihedral of order 8. If $G = N$, $s_0 = 5/8$. If $G \neq N$, then $N$ has order 4 and since every nonidentity element has either 0 or 2 fixed points, $s_0 = 1/2$.

Suppose $G$ is not primitive on $X$. Let $H$ be the stabilizer of a point in $X$ and let $H < K < G$. Set $Y = G/K$. If $(G, N, Y)$ is not exceptional, then $s_0(Y) \geq 1/m$ where $m = [G : K]$. Clearly, $s_0(Y) \geq s_0$ ( by Lemma 3.2). Thus, $s_0(Y) \geq 2/n$ with equality possible only if $n = 2m$ and $G$ acting on $Y$ is a Frobenius group order $m(m-1)$. If $g \in xN$ has no fixed points on $Y$, then clearly this is also true on $X$. The number of such elements is $|S_0(Y)| \geq (2/n)|N|$. If $m > 2$, then some element in $xN$ acts nontrivially on $Y$ but with fixed points. We may then assume that $x \in K$. Since $K \cap N \neq H \cap N$ (as $G = HN = KN$ and $K > H$), we may also assume that $x \notin H$. Then $x$ has a unique fixed point on $Y$. Thus, the only possible fixed points for $x$ on $X$ are $gH$ with $g \in K$. Since $x \notin H$, $x$ fixes no such point and so has none on $X$. Hence $s_0 > s_0(Y) \geq 2/n$. If $m = 2$, then $n = 4$ and (c) holds.

If $(G, N, Y)$ is exceptional, then $(K, N \cap K, Z)$ is not (where $Z = K/H$). Then each element in $xN$ fixes a unique coset of $K$, whence (Lemma 3.2) $s_0 = s_0(K, N \cap K, Z) \geq 1/m$ where $m = [K : H]$. Since degree 2 permutation representations are not exceptional, $m > 2$. Hence $s_0 \geq 3/n$. ■

One can use induction and the previous result to show that if $X = G/H$ and there is a chain of subgroups $H = H_0 < H_1 < \ldots < H_d < G$, then either $X$ is exceptional or $s_0 \geq 2^{d-1}/n$.

We would like to classify all triples with $s_0 \leq 2/n$. By the previous lemmas, it suffices to consider the primitive case.

We will not classify all possibilities, but we assume that $G$ is the arithmetic monodromy group of a branched covering of connected smooth projective curves defined over a finite field and $N$ is the geometric monodromy group. Moreover, we will further assume that there is a totally ramified $\mathbf{F}_q$-rational point (e.g., a polynomial map from $\mathbb{P}^1$ to $\mathbb{P}^1$ - so $\infty$ is the totally ramified point). Without loss of generality by Lemma 3.5, we also assume that the covering is indecomposable of degree $n$. Thus, $G$ is a primitive (faithful) permutation group of degree $n$.

As noted above, exceptional groups (corresponding to monodromy groups of exceptional covers with a totally ramified rational point) were essentially classified in [FGS] (exactly which affine groups are possible was left open). In [GS], a list of possibilities for $G$ (and the permutation action) were determined.

**Theorem 3.6.** *Let $\alpha : X \to Y$ be a separable branched covering of degree $n$ with $X, Y, \alpha$ defined over $\mathbf{F}_q$. Assume moreover that one of the branch points is totally ramified and is $\mathbf{F}_q$-rational. Let $p$ be the characteristic of $F$. Let $G$ be the arithmetic monodromy group of the covering and $N$ the geometric monodromy group. Then one of the following holds:*

(a) *$r_2 = 0$ and the covering is exceptional;*
(b) *$r_2 = 1$ , $s_0 = 1/n$ and $G = N$ is Frobenius of order $n(n-1)$ with $n$ a prime or $p^a$;*
(c) *$r_2 = 2$, $s_0 = 2/n$ and $G = N$ is Frobenius of order $n(n-1)/2$ with $n$ an odd prime or $p^a$ (with $p > 2$);*
(d) *$s_0 > 2/n$; or*
(e) *$n \leq 6$, $G = N$ and $1/n \leq s_0 \leq 2/n$ or $n = 4$, $|G/N| = 2$ and $s_0 = 2/4$.*

**Proof.** By Lemma 3.5, we may assume that the cover is indecomposable (over $\mathbf{F}_q$). By the preceding remarks, we may assume that $r_2 = 1$.

First assume that $G$ is affine and $n = r^a$ for some prime power $r$. By Lemmas 2.2 and 2.3, it follows that $s_0 > 2/n$ unless $n = 4$ or 9 or $r \leq 3$. We identify $X$ with a vector space $V$ of over the field of $r$ elements. Then $G_0$, the stabilizer of 0, is a group of semilinear transformations on $V$.

If $n = r = 4$, then $G = A_4$ or $S_4$. If $G = A_4$ and $N$ has order 4, then $G$ is exceptional. If $G = N = A_4$, then $G$ is Frobenius.

If $n = 9$, then by inspection it follows that either $G = N$ is Frobenius, $G$ is exceptional, or $s_0 \geq 1/3$.

Next assume $q = 3$, $n = 3^a > 9$ and $r_2 = 1$. It follows from Lemmas 2.2 and 2.3 that either $G$ is Frobenius, $s_0 > 2/n$ or we may assume that $x$ is a reflection and $G_{0,v}$ has order 2 for any $v \neq 0$ fixed by $x$. If $w$ is fixed by $x$, then $G(0, w) = N(0, w)$. Since $r_2 = 1$, it follows that the nonzero elements of the fixed hyperplane $W$ of $x$ is contained in a single $G_0$-orbit. Let $u$ be a vector in the $-1$ eigenspace of $x$. Since $G_{0,v} = \langle x \rangle$, the centralizer of $x$ is transitive on the nonzero elements in $W$. Moreover, since $G_0$ is irreducible on $V$ (by primitivity), it follows that $G_0 u = G_0 v$. Thus, some reflection $x'$ centralizes $u$. Since $a > 2$, $x$ and $x'$ both fix some nonzero vector $w$ in $W$. Then $G_{0,w}$ has order greater than 2. Since $v$ and $w$ are in the same $G_0$-orbit, the same is true for $G_{0,v}$, a contradiction.

Now assume $r = 2$, $n = 2^a > 4$, and $r_2 = 1$. We may assume that $x$ fixes 0. If $xN_0$ does not contain a transvection, then the minimal degree of an element in $xN$ is $(3/4)n$ and $s_0 > 2/n$ (by the argument of Lemma 2.2). So we may assume that $x$ is a transvection. Let $W$ be the fixed hyperplane of $x$. Since $N(0, w) = G(0, w)$ for any nonzero element of $W$ and $r_2 = 1$, $G(0, w) = G(0, v)$ and all nonzero vectors of $W$ are in the same $G_0$-orbit.

Let $H$ be the subgroup of $G_0$ generated by transvections. Since all nonzero vectors in $W$ are in the same $G_0$-orbit, for each $0 \neq w \in W$, there is a transvection $\tau_w$ centered on $w$. This implies that the only possible nontrivial invariant subspace is $W$. Since $H$ is normal in $G_0$, this would imply that $G_0$ would leave $W$ invariant, a contradiction. It follows by [Mc] that the only irreducible subgroups of $GL(V))$ for which a single orbit contains all nonzero vectors in a hyperplane are $SL(V)$ or $Sp(V)$. Now argue as above.

It follows by [GS] that in the affine case $n = p^a$, $n$ is prime or $n = 4$.

So we may assume that $G$ is not affine. Now using [GS], we have the following cases to consider:

(i) $F^*(G) = L$ is simple and is given [GS, 3.1];
(ii) $F^*(G) = L \times L$ with $L$ simple and $n = 4p^{2a}$, $p$ odd given in [GS, 4.2];
(iii) $F^*(G) = P\Omega_4^+(q)$, $n = q(q^2 - 1)/(2, q - 1)$ with $q \geq 4$;
(iv) $n = p^a$; or

We first note that if $G$ is 2-transitive (in particular, if $G = N$ and $r_2 = 1$), then we argue precisely as above in the 2-transitive case. If $G$ is a rank 3 permutation group (i.e. $G_a$ has three orbits), then $r_2 = 0$ or $r_2 = 2$ and we are done.

Consider (i). The following are immediate consequences of [GS, 3.1]. If $L$ is a sporadic simple group, then $r_2 > 1$ or $G$ is 2-transitive. If $L$ is an alternating group (which is not a classical group), then $G$ is either 2-transitive or rank 3. Moreover, $L$ is not an exceptional Chevalley group. Thus, the remaining case is $L$ classical.

In case B(i) of [GS, 3.1], $L$ is an even dimensional unitary group (at least 4 dimensional) or an orthogonal group (of dimension at least 3 and + type in even dimension) and the point stabilizer (in $L$) may be taken to be the stabilizer of a nonsingular 1-space (of $-$ type if $L$ is an odd dimensional orthogonal group). Note that case (iii) above also is of the same type (except that $L$ is not simple). In the unitary case, it follows that $r_2 > 1$ (the pairs of 1-spaces represented by $(u, v)$ with $(u, v)/(u, u)$ either 0 or 1 correspond to $L$-orbits which are $\mathrm{Aut}(L)$-orbits). Similarly, $r_2 > 1$ for orthogonal groups in dimension at least 4 for fields of odd characteristic and even dimensional orthogonal groups in even characteristic.

Next consider the three dimensional orthogonal groups. In this case, $L = \Omega_3(q) = L_2(q)$. We may assume that $q \geq 4$. If $q = 4$, $G$ is 2-transitive and if $q = 5$, $G$ is rank 3, so we may assume that $q > 5$. We can identify $X$ with the set of orbits of size 2 on $\mathbb{P}^1$ of the field automorphism $\sigma$ defined by $a \mapsto a^q$.

We claim that any nonidentity element fixes at most $(4/q)n$ points. It suffices to consider elements of prime order. If $g$ has odd prime order, then it fixes an orbit of size 2 of $\sigma$ only if it fixes each point. If $g \in PGL_2(q)$, then $g$ fixes at most 2 points in $\mathbb{P}^1$, whence $g$ fixes at most 1 point in $X$. Otherwise $g$ is conjugate to an element inducing a field automorphism, whence $g$ fixes at most $(q^{2/3} - q^{1/3})/2$ points on $X$ and the claim holds. If $g$ is an involution and $g \in PGL_2(q)$, then $g$ fixes at most $(2q+4)n/(q^2-q)$ points and the claim holds. Finally, if $g$ is an involution conjugate to a field automorphism, then $g$ will fix at most $(q_0 + 1)n/(q + 1)q_0$ points on $X$, where $q_0^2 = q$ (note $q$ is a square in this case). In particular, $\mu > (2/3)n$ for $q \geq 11$. It follows by Lemma 2.2 that either $G$ is exceptional or that $s_0 > 2/n$. If $q = 8$, $G = N$ and $r_2 = 3$ or $G$ is exceptional. If $q = 9$, one checks directly that $r_2 > 1$.

If $q = 7$, then either $G = N$ and $r_2 = 6$ or $|G/N| = 2$. In the latter case, we compute that $r_2 = 1$ and $s_0 = 1/3$.

It follows by [FGS] that $G$ is exceptional only if $G = \mathrm{Aut}(L)$ with $q = r^a$ for $r = 2, 3$ and $a$ odd (and $L \leq N \leq M$ where $M/L$ is the Frattini subgroup of $G/L$).

Next consider $L = \Omega_{2m+1}(2^a) = Sp_{2m}(2^a)$. Then $\mathrm{Aut}(L)$ has order $a$. It follows that $\mu > (2/3)n$ (cf. [LS]) for $a > 1$ and we can apply Lemma 2.2. If $a = 1$, then $G$ is 2-transitive.

The only remaining cases with $L$ classical are given in [GS, Table B]. We may eliminate the cases where $G = N$ - in particular, those cases where $N = \mathrm{Aut}(L)$. This leaves 4 cases to consider, $(L, L_a) = (L_4(2), GL_2(4).2), (L_5(2), P_2), (\Omega_8^+(2), A_9)$ and $(P\Omega_8^+(3), \Omega_8^+(2))$. In all cases, it is verified that $r_2 > 1$.

Next consider the case that $E = F^*(G) = L_1 \times \ldots \times L_t$ with $L_i \cong L$ a nonabelian simple group and $E_a = K_1 \times \ldots \times K_t$ with $K_i$ nontrivial. Let $\ell = [L_i : K_i]$ and $n = \ell^t$ with $t > 1$. Moreover, we assume that the $L_i$ and $K_i$ are all conjugate in $G$. Since $G/N$ is cyclic, it follows that $E \leq N$. We further assume that $K_1$ acting on $L_1/K_1$ has a nontrivial unique orbit of maximal size. If $N$ is transitive on the $L_i$, then it is easy to see that $r_2 > 1$. Thus, it follows that no element of the coset $xN$ can normalize each $L_i$.

As we observed, we may assume that no element in $xN$ normalizes each $L_i$. This implies that any element of $xN$ fixes at most $(n/\ell) \leq n/5$ points. We can apply a version of (2.7) above (with $\mu$ replaced by the minimal degree of an element in the coset $xN$) to obtain $s_0 > (2/n)$.

By [GS, 4.1 and 4.2], it now follows that $s_0 > (2/n)$ in cases (ii) and (iv) above.

■

**Remark.** There should be a version of the previous result without the assumption that we are dealing with monodromy groups of polynomials (or more generally coverings with a totally ramified rational point). If $r_2 \neq 1$, it follows from the earlier discussion. This suggests that a proof may require a classification of the possibilities with $r_2 = 1$. A proof along the lines of [FGS] might be feasible. Note that we already had to deal with one case with $r_2 = 1$ (but the group was not 2-transitive) in the proof of the previous result. We do prove a weaker version of the previous theorem in section 5.

We conclude this section with a simple lower bound on $V_f$, which is proved in the same way as Corollary 2.5.

**Proposition 3.7.** *Let $\alpha : X \to Y$ be a separable covering of degree $n$ with $X, Y, \alpha$ defined over $\mathbf{F}_q$. Assume that the fiber product $X \times_Y X$ has exactly one absolutely irreducible component defined over $\mathbf{F}_q$ other than the diagonal. Then $V_f > q/2 + O(q^{1/2})$.*

Note that $r_2 + 1$ is the number of absolutely irreducible components of the fiber product above. So the assumption in the previous proposition is equivalent to $r_2 = 1$. The asymptotic result means that we let $q \to \infty$ in such a way that the hypothesis is still satisfied (this just amounts to taking extensions relatively prime to the degree of the smallest field over which every irreducible component over an algebraic closure of $\mathbf{F}_q$ of the fiber product is defined). See [U] for a similar result.

## 4. Coverings with a totally ramified point

In this section, we show that for coverings of degree prime to the characteristic with a totally ramified point, an absolute positive lower bound for $s_0$ can be obtained. We note that Corollary 2.4 (with an identical proof) is also valid for the more general $(G, N)$ case.

**Theorem 4.1.** *Let $f : X \to Y$ be an indecomposable separable covering of degree $n$ defined over a finite field $\mathbf{F}_q$ of characteristic $p$. Assume that $f$ has a totally and tamely ramified $\mathbf{F}_q$-point (so $p$ does not divide $n$). Let $N$ be the geometric monodromy group of $f$ and $G$ its arithmetic monodromy group. Then one of the following holds:*

(a) *$G$ is a Frobenius or regular group of degree $n$ a prime and either*
   (i) *$G \neq N$ and the cover is exceptional; or*
   (ii) *$G = N$ has order $nd$ for some $d|(n-1)$ and $s_0 = (n-1)/dn$; or*

(b) *$G$ and $N$ are 3-transitive of degree $n$, $r_2 = r_3 = 1$ and $s_0 > 1/3$; or*

(c) *$G$ and $N$ are 2-transitive of degree $n$, $r_2 = 1$, $r_3 = 2$ and $s_0 > 1/6$.*

**Proof.** Since $f$ is indecomposable, it follows that $G$ is primitive. Since there is a totally ramified point (and $p$ does not divide $n$), $N$ contains an $n$-cycle. It follows (cf. [Wi]) that $G$ is 2-transitive or $n$ is a prime and $G'' = 1$. In the latter case, $G$ is a Frobenius or cyclic group of order $nd$ for some $d|(n-1)$. The fixed point free elements in $G$ are precisely the $n-1$ elements of order $n$, whence (a) holds.

So we may assume that $G$ is 2-transitive and $G'' \neq 1$. Any 2-transitive group is either almost simple or affine. The only affine group with $G'' \neq 1$ containing an $n$-cycle is $S_4$ (with $n = 4$) which is 3-transitive. If $G = S_4$, then since $N$ contains an 4-cycle and $G/N$ is cyclic, it follows that $G = N$. More generally, it follows by inspection of the 3-transitive almost simple groups that $N$ would also be 3-transitive. Corollary 2.4 yields $s_0 > 1/3$ in this case.

So finally consider the case that $G$ is almost simple and is 2-transitive but not 3-transitive containing an $n$-cycle. It follows by inspection (see Table 1) that $r_3 = 2$ in this case. Corollary 2.4 yields $s_0 > 1/6$. ■

We consider in some detail the case $G = N$ is a Frobenius group of order $nd$ with $n$ prime or cyclic of order $n$ with $n$ prime. We will show that under suitable conditions that if the genus is small, then so is $d$. The next results are quite easy if we assume that all ramification is tame.

We first review the Riemann-Hurwitz formula. See [Ha] and [S1]. Let $f : X \to Y$ be a separable branched covering of connected smooth projective curves $X$ and $Y$ of degree $n$. Let $B$ be the finite set of branch points (i.e. those points that ramify). Let $L = F(X)$ and $K = F(Y)$ be the function fields of the curves. Let $g(X)$ and $g(Y)$ denote the genus of $X$ and $Y$. If $x \in X$, define $a(x) = v(\mathcal{D}_x)$, where $\mathcal{D}_x$ is the different of the extension $L_x/K_{f(x)}$ and $v$ is the corresponding discrete valuation on $L_x$. Let $e = e(x)$ denote the degree of ramification. We note the following (cf. [Ha, p. 301] or [S1]):

(a) if there is no ramification, then $a(x) = 0$;
(b) if there is tame ramification of degree $e$, then $a(x) = e - 1$;
(c) if there is wild ramification (i.e. $p|e$), then $a(x) \geq e$.

Set $\lambda(y) = \sum_{x \in f^{-1}(y)} a(x)$. Then (cf. [Ha, p. 301])

$$2(g(X) - 1) = 2n(g(Y) - 1) + \sum_{y \in B} \lambda(y).$$

Let $G$ denote the monodromy group of the cover. Let $I_y$ denote an inertia group of a point over $y$. If there is only tame ramification over $y$, then $I_y = \langle g_y \rangle$ and $\lambda(y)$ is $\operatorname{ind}(g_y) := n - \operatorname{orb}(g_y)$, where $\operatorname{orb}(g)$ is the number of orbits of $g$ in the associated permutation representation of degree $n$.

Moreover, if all points are tamely ramified (in particular, if the order of the monodromy group is not a multiple of the characteristic), then, by a result of Grothendieck (see [Gr] or [Fu]), we may order the branch points $y_1, \ldots, y_r$ and choose $g_i$, a generator for $I_{y_i}$ such that $G = \langle g_1, \ldots, g_r \rangle$ and $g_1 \cdots g_r = 1$. In any case, if $I_y$ has orbits of size of $n_1, \ldots, n_t$, then $\lambda(y) \geq \sum n_i'$, where $n_i' = n_i$ for $p|n_i$ and $n_i' = n_i - 1$ otherwise.

Now, in particular, assume that $p \neq n$ is prime and $G$ is a Frobenius group of order $nd$ (if $d = 1$, then $G$ is cyclic) as above. Thus, every nonidentity element has at most one fixed point. So either $g$ is an $n$-cycle or a product of $(n-1)/b$ cycles each of length $b$. Thus if $w$ is a point of $Y$, one of the following holds:

(d) $w$ is totally ramified and $\lambda(w) = n - 1$;
(e) $w$ is tamely but not totally ramified and $\lambda(w) = (b-1)(n-1)/b$ where the inertia group of a point over $w$ has order $b$; or

(f) $w$ is wildly ramified and $\lambda(w) \geq n - 1$.
In particular, if $w$ is ramified, then $\lambda(w) \geq (n-1)/2$.

We will show below (Theorem 4.5) that these conditions force $d$ small compared to $g(X)$. In particular, if $g(X) = 0$, then it is quite easy to see (and follows from Proposition 4.4) that $d \leq 2$ (see also [Fr1]). Indeed, the proof shows that the Galois closure also has genus zero. We state this result separately.

**Lemma 4.2.** *Let $f$ be a polynomial of prime degree $n$ with $n \neq p$. If the geometric monodromy group $N$ of $f$ is a Frobenius group, then $N$ is either cyclic or dihedral. Moreover, the Galois closure of the cover $f : \mathbb{P}^1 \to \mathbb{P}^1$ has genus zero and one of the following holds:*
(a) *$N$ is cyclic and there are 2 branch points;*
(b) *$N$ is dihedral, $p \neq 2$ and there are 3 branch points; or*
(c) *$N$ is dihedral, $p = 2$ and there are 2 branch points exactly one of which is wildly ramified.*

**Corollary 4.3.** *Assume that $f : \mathbb{P}^1 \to \mathbb{P}^1$ is a polynomial over $\mathbf{F}_q$ of degree $n$ with $n$ prime to the characteristic $p$. If $s_0 > 0$, then $s_0 > 1/6$.*

**Proof.** Since $(p, n) = 1$, the cover defined by $f$ is automatically separable. Without loss of generality, we may assume that $f$ is indecomposable over $\mathbf{F}_q$. By Theorem 4.1, it suffices to assume that $G = N$ is Frobenius or regular and $n$ is prime. By Lemma 4.2, this implies that $|G| = n$ or $2n$. Then $s_0 = (n-1)/nd \geq (n-1)/2n > 1/6$. ∎

In order to obtain an analog of Corollary 4.3 for curves of higher genus, we need to consider coverings with Frobenius monodromy group with a totally and tamely ramified point.

We separate out the case of two branch points since the argument is entirely different.

**Lemma 4.4.** *Let $X$ be a curve of genus $g$ over an algebraically closed field $F$ of characteristic $p \geq 0$. Suppose $f : X \to \mathbb{P}^1$ is a separable indecomposable branched covering of prime degree $n \neq p$ with at most two branch points. Let $g$ denote the genus of $X$. Assume that there is a branch point that is totally ramified and that the monodromy group is Frobenius of order $nd$ (so $d|(n-1)$). Then $d \leq 2g + 2$ (if $p \neq 2$, $d \leq g + 2$).*

**Proof.** Let $C$ be the normal subgroup of $G$ of order $n$. Let $B$ denote a subgroup of order $d$. Let $W$ denote the curve corresponding to the Galois closure of the covering. Let $V$ denote the curve corresponding to the fixed field of $C$. Thus, $V/\mathbb{P}^1$ is a cyclic cover of degree $d$. We assume that $B$ corresponds to $X$ in the Galois correspondence.

Of course, there are no unramified coverings of $\mathbb{P}^1$, so that there must be at least one branch point. If there is a single branch point, then $p > 0$ and $G$ is generated by its Sylow $p$-subgroups. Since $y$ is totally ramified, this implies that $n = p$, whence $G$ has order $p$ and $d = 1$.

So we assume that there are precisely two branch points and $d > 1$ (since there is nothing to prove if $d = 1$).

If both branch points are tamely ramified, then $G = \langle s, t \rangle$ where $s$ and $t$ generate inertia groups over the branch points and $st = 1$. Thus, $G$ is cyclic and $d = 1$.

Assume $y$ is totally ramified. Then the inertia group of a point over $y$ is cyclic of order $n$, whence $\lambda(y) = n - 1$. Thus, $y$ is tamely ramified and is not a branch point in the cover $V/\mathbb{P}^1$. It follows that $V/\mathbb{P}^1$ is a cyclic cover of degree $d$ and has single branch point $z$, whence $d = p^a$ for some $a$. Moreover, the inertia group of a point in $W$ over $y$ is $C$ and the inertia group of a point in $W$ over $z$ is conjugate to $B$. Let $w$ denote the unique point of $W$ with inertia group $B$ ($w$ lies over $z$ and since $B$ is its own normalizer, there is only one point in $W$ with inertia group $B$).

Let $v \in V$ and $x \in X$ be the points under $w$ (and so over $z$). If we complete at $w$, then $F(W)_w = F(V)_v$ and $F(X)_x = F(\mathbb{P}^1)_z$. We identify $B$ with the monodromy group of the cover $V/\mathbb{P}^1$. Thus, the higher ramification groups $B_i$ of $v$ (for $V/\mathbb{P}^1$) and $w$ (for the cover $W/X$) agree. Moreover, $V/\mathbb{P}^1$ and $W/X$ each are ramified at a single point ($z$ and $x$ respectively) and these points are totally ramified. Using the Riemann-Hurwitz formula (see also [S1, p. 64]) to compute the genus (with respect to these two Galois covers), we see that if $g(V)$ and $g(W)$ are the genus of $V$ and $W$, then

$$
\begin{aligned}
2(g(W) - 1) =& 2d(g - 1) + \sum_{i=0}^{\infty}(|B_i| - 1), \text{ and} \\
2(g(V) - 1) =& -2d + \sum_{i=0}^{\infty}(|B_i| - 1).
\end{aligned}
$$

Thus, $g(W) = g(V) + dg$. On the other hand, $W/V$ is a cyclic cover of degree $n$ with precisely $d$ branch points each tamely ramified with inertia group $C$ (the points over $y$ – since the point in $V$ over $z$ is unramified to $W$). Thus,

$$2(g(W) - 1) = 2n(g(V) - 1) + d(n - 1), \text{ and}$$

$$2dg = (2n - 2)(g(V) - 1) + d(n - 1).$$

Hence $2g \geq (d - 2)(n - 1)/d \geq d - 2$ and $d \leq 2g + 2$. More generally, if we factor $n - 1 = p^b m$ where $p$ does not divide $m$, we see that $d \leq (2/m)g + 2$. ∎

**Theorem 4.5.** *Let $f : X \to Y$ be a branched covering of prime degree $n \neq p$ which is tamely and totally ramified at some point $y \in Y$. Assume that the geometric monodromy group of $f$ is Frobenius of order $nd$. Let $g$ be the genus of $X$ and $h$ the genus of $Y$. Then one of the following occurs:*

(a) *$h > 0$ and $g > g - h > d/2$;*

(b) *$h = 0 = g$, $d \leq 2$ and the Galois closure of the cover has genus zero; or*

(c) *$d \leq 4g$.*

**Proof.** Note the inertia group of a point over $y$ acts transitively (because of the total ramification). Let $B$ denote the set of branch points. We use the observations (d)-(g) above.

If $h > 0$, then $2(g - h) > \lambda(y) = n - 1 \geq d$ and (a) holds. So assume that $h = 0$. The Riemann-Hurwitz formula in this case is:

$$2(n+g-1) = \sum_{z \in B} \lambda(z).$$

If $|B| \leq 2$, the result follows from the previous lemma (since $4g \geq 2g+2$ for $g > 0$).

So assume that $|B| \geq 3$. Note that $\lambda(w) \geq (n-1)/2$ for every $w \in B$. If some point $z$ is wildly ramified, its contribution to the Riemann-Hurwitz formula is at least $n-1$, whence $2g \geq (n-1)/2 \geq d/2$. Thus, $d \leq 4g$.

Similarly, if $|B| \geq 4$, it follows that $\sum \lambda(w) \geq 3(n-1)/2 + (n-1)$. Hence, the Riemann-Hurwitz formula yields $2g \geq (n-1)/2 \geq d/2$. and again we obtain $d \leq 4g$.

So we may assume that there are three branch points and no wild ramification. Let $y = y_1, y_2, y_3$ denote the branch points. Thus, $G = \langle g_1, g_2, g_3 \rangle$ where $g_1 g_2 g_3 = 1$ with $g_i$ a generator of an inertia group over $y_i$. Since $g_1$ has order $n$, it generates the normal subgroup $C$ of $G$. Thus, $G/C$ is generated by the image of $g_2$ and $g_3$ maps to its inverse. Hence $g_2$ and $g_3$ each have order $d$. Thus $\lambda(y_1) = n-1$ and $\lambda(y_2) = \lambda(y_3) = (d-1)(n-1)/d$. It follows that $2g = 2(d-1)(n-1)/d - (n-1) = (n-1)(d-2)/d \geq d-2$. Thus, $d \leq 2g+2$.

In particular, if $g = 0$, it follows that $d \leq 2$. Another application of the Riemann-Hurwitz formula shows that the Galois closure has genus 0.

■

**Corollary 4.6.** *Let $f : X \to Y$ be a branched covering of degree $n > 1$ with $n$ prime to $p$ which is totally ramified at some $\mathbf{F}_q$-rational point $y$. Let $g$ denote the genus of $X$. If $s_0 > 0$, then $s_0 > 1/6$ for $g \leq 1$ and $s_0 \geq 3/14g$ for $g > 1$.*

**Proof.** Since $s_0 \geq 1/n$, we may assume that $n \geq 7$. Without loss of generality, we may assume that $f$ is indecomposable. By Theorem 4.1, we may further assume that $G = N$ is a Frobenius group of order $nd$ or cyclic group of $n$ (i.e. $d = 1$) with $n$ prime and so $s_0 = (n-1)/dn$. If $g = 0$, then $d \leq 2$ by Theorem 4.5, whence the result. If $g \geq 1$, again by Theorem 4.5, $d \leq 4g$. Then $s_0 \geq (n-1)/4gn \geq 3/14g$. If $g = 1$, this is larger than $1/6$. ■

**Remarks.** We do not know if the bound in the previous result is best possible. It is straightforward to see that if $p$ does not divide $n(n-1)$ with $n > 2$ prime, then we may realize the Frobenius group of order $n(n-1)$ and degree $n$ as a group of automorphisms of a curve of genus $g = (n-3)/2$, whence $s_0 = 1/n$ is approximately $1/2g$.

As we have seen, if we do not assume that $n$ is prime to the characteristic, then the result is false. There should be some version of the previous result where for example the bound depends only the power of $p$ dividing $n$. An analysis of the possible monodromy groups for polynomials will be required (see [GS]).

We can improve Corollary 4.3 slightly if we assume that all ramification is tame (not just ramification over $\infty$). This essentially follows from the Feit-Müller classification of monodromy groups of indecomposable polynomials in characteristic zero and Grothendieck's theorem (that a tamely ramified cover has a branch cycle description as in the characteristic zero case).

**Theorem 4.7.** *Let $f : \mathbb{P}^1 \to \mathbb{P}^1$ be an indecomposable polynomial of degree $n$ defined over a finite field $\mathbf{F}_q$ of characteristic $p$. Assume that all ramification is tame (in particular, $p$ does not divide $n$). Let $N$ be the geometric monodromy group of $f$ and $G$ its arithmetic monodromy group. Then one of the following holds:*
(a) *$n \leq 23$ and $N$ is triply transitive;*
(b) *$n$ is prime, $G = N$ is cyclic of order $n$ and $s_0 = (n-1)/n$;*
(c) *$n$ is prime, $G = N$ is dihedral of order $2n$ and $s_0 = (n-1)/2n$;*
(d) *$n$ is prime, $N$ is cyclic of order $n$ or dihedral of order $2n$, $N \neq G$ and $f$ is exceptional;*
(e) *$G = N$ and*
 (i) *$n = 11$ and $G = L_2(11)$;*
 (ii) *$n = 13$ and $G = PGL_3(3)$;*
 (iii) *$n = 15$ and $G = A_8$;*
 (iv) *$n = 21$ and $G = P\Gamma L_3(4)$;*
 (v) *$n = 31$ and $G = L_5(2)$;or*
(f) *$A_n \subseteq N \subseteq G \subseteq S_n$.*

**Proof.** By Grothendieck [Gr], we have that $N$ will occur as the monodromy group of an indecomposable polynomial cover over $\mathbb{C}$. All such possibilities have been classified in [Mü] (see also [Fe]). ■

**Corollary 4.8.** *Let $f : X \to Y$ be a polynomial covering of degree $n$ defined over a finite field $\mathbf{F}_q$ of characteristic $p$. Assume that all ramification is tame (in particular, $p$ does not divide $n$). Then either $s_0 = 0$ or $s_0 \geq 16/63$.*

**Proof.** As usual, we may assume that $f$ is indecomposable. We apply the previous result. If $N$ is 3-transitive, then $s_0 \geq 1/3$. The bound clearly holds for $N$ cyclic or dihedral. So we are left only to verify the bound in (e) above. This is an easy calculation using [ATLAS]. ■

Note that $16/63$ occurs when $n = 21$ and $G = N = P\Gamma L_3(4)$. Thus, the bound is best possible in the previous result.

## 5. Higher dimensional varieties

In this section, we briefly discuss some generalizations of the previous curve results to higher dimensional varieties in the setting of [Se2, Theorem 3.6.2].

Let $Y$ and $Z$ be two $m$-dimensional absolutely irreducible (quasi-projective) varieties defined over $\mathbf{F}_q$. Let $f : Y \longrightarrow Z$ be a generically surjective and separable morphism of degree $n$ defined over $\mathbf{F}_q$, where $n$ is a positive integer. The map $f$ is actually a finite map if we remove suitable co-dimension 1 subvarieties from $Y$ and $Z$. Let $D$ be the (quasi-projective) variety defined by the fiber product $Y \times_Z Y$ with its diagonal removed. The variety $D$ over $\mathbf{F}_q$ is also at most $m$-dimensional if $f$ is finite. The set $D(\mathbf{F}_q)$ consists of the pairs $(P_1, P_2)$ of $\mathbf{F}_q$-rational points in $Y(\mathbf{F}_q)$ such that $P_1 \neq P_2$ and $f(P_1) = f(P_2)$. Let $V_f$ be the cardinality of the value set $f(Y(\mathbf{F}_q))$.

**Theorem 5.1.** *If $f$ is a finite map, then we have the inequality*

$$V_f \leq |Y(\mathbf{F}_q)| - \frac{|D(\mathbf{F}_q)|}{n}. \tag{5.1}$$

**Proof.** Since $f$ is a finite map of degree $n$, for each point $P \in Z$, the inverse image $f^{-1}(P)$ has cardinality at most $n$. For $0 \leq i \leq n$, let $s_i$ be the number of $\mathbf{F}_q$-rational points $P \in Z(\mathbf{F}_q)$ such that $f^{-1}(P) \cap Y(\mathbf{F}_q)$ has cardinality $i$. By this definition, one then checks directly that

$$(2-1)s_2 + (3-1)s_3 + \cdots + (n-1)s_n = |Y(\mathbf{F}_q)| - V_f. \tag{5.2}$$

and

$$2(2-1)s_2 + 3(3-1)s_3 + \cdots + n(n-1)s_n = |D(\mathbf{F}_q)|. \tag{5.3}$$

Multiply equation (5.2) by $n$ and subtract (5.3), we deduce that

$$n\big(|Y(\mathbf{F}_q)| - V_f\big) - |D(\mathbf{F}_q)| = \sum_{j=2}^{n-1}(n-j)(j-1)s_j \geq 0. \tag{5.4}$$

This immediately gives (5.1). The proof is complete. ■

**Definition 5.2.** *A finite and separable morphism $f : Y \longrightarrow Z$ is called exceptional over $\mathbf{F}_q$ if the variety $D$ as above has no absolutely irreducible components of (top) dimension $m$ defined over $\mathbf{F}_q$. A generically surjective and separable morphism $f : Y \longrightarrow Z$ as above is called exceptional if its restriction to some dense open set is a finite and exceptional map.*

**Theorem 5.3.** *Let $f : Y \longrightarrow Z$ be a generically surjective and separable morphism of degree $n$, where $Y$ and $Z$ are absolutely irreducible $m$-dimensional $\mathbf{F}_q$-varieties.*
(i). *If $f$ is not exceptional over $\mathbf{F}_q$, then*

$$V_f \leq (1 - \frac{1}{n})q^m + O(q^{m-1/2}). \tag{5.5}$$

(ii). *If $f$ is exceptional over $\mathbf{F}_q$, then*

$$|D(\mathbf{F}_q)| = O(q^{m-1}), \quad V_f = q^m + O(q^{m-1/2}). \tag{5.6}$$

**Proof.** Since any variety of dimension $m-1$ over $\mathbf{F}_q$ has at most $O(q^{m-1})$ rational points over $\mathbf{F}_q$, by restricting to suitable dense open subsets of $Y$ and $Z$, we may assume that $f$ is a finite map. Thus, we may assume that the variety $D$ has dimension at most $m$.

In case (i), the non-exceptionality of $f$ shows that the variety $D$ has at least one absolutely irreducible component of dimension $m$ defined over $\mathbf{F}_q$. The Lang-Weil estimate (a special case of Lemma 5.5 below) shows that

$$|Y(\mathbf{F}_q)| = q^m + O(q^{m-1/2}), \quad |D(\mathbf{F}_q)| \geq q^m + O(q^{m-1/2}).$$

Combining with (5.1), we deduce (5.5).

In case (ii), the exceptionality of $f$ shows that the variety $D$ has no absolutely irreducible components of top dimension $m$ defined over $\mathbf{F}_q$. Thus, each $\mathbf{F}_q$-rational point on $D$ (except those on some co-dimension 1 subvariety of $D$) is contained in an intersection of two distinct geometric components of $D$. Such an intersection has dimension at most $m-1$. Thus, the set $D(\mathbf{F}_q)$ of all $\mathbf{F}_q$-rational points on $D$ is contained in the set of $\mathbf{F}_q$-rational points of some variety of dimension at most $m-1$. The Lang-Weil estimate shows that

$$|D(\mathbf{F}_q)| = O(q^{m-1}).$$

This is the first equation of (5.6). Combining with equation (5.3) , one deduces that $s_i = O(q^{m-1})$ for all $2 \leq i \leq n$. By (5.4), we then conclude that

$$V_f = |Y(\mathbf{F}_q)| + O(q^{m-1}) = q^m + O(q^{m-1/2}). \tag{5.7}$$

**Remarks**. If $f$ is exceptional over $\mathbf{F}_q$, the crude estimate $|D(\mathbf{F}_q)| = O(q^{m-1})$ in (5.6) can be greatly improved in some cases. For example, if $Y$ and $Z$ are absolutely irreducible non-singular projective curves over $\mathbf{F}_q$ and $f : Y \longrightarrow Z$ is exceptional over $\mathbf{F}_q$ (automatically finite in this case), it is shown in [Le] (already in [FGS] if $Z = \mathbb{P}^1$) that $|D(\mathbf{F}_q)| = 0$. More general, it is shown in [Le] that $|D(\mathbf{F}_q)| = 0$ for exceptional $f$ if one assumes some natural conditions such as that the map $f$ is finite and that the varieties $Y$ and $Z$ are normal. See also [Fr3] for earlier results of this nature.

Similarly, the second estimate in (5.6) can also be improved in some cases. For instance, using Lenstra's result as above and Deligne's theorem on Riemann hypothesis, one derives immediately that

$$V_f = \frac{q^{m+1}-1}{q-1} + O(q^{m/2}),$$

if $f$ is an exceptional finite map, $Y$ is a smooth projective complete intersection and $Z$ is normal.

A similar inclusion-exclusion argument as in (2.11) and the Lang-Weil estimate shows that Proposition 3.7 carries over to higher dimensional case. We state this generalization here.

**Proposition 5.4.** *Let $f : Y \longrightarrow Z$ be a generically surjective and separable map between two absolutely irreducible varieties over $\mathbf{F}_q$. Assume that the variety $D$ has exactly one absolutely irreducible component of dimension $m$, then*

$$V_f > \frac{1}{2}q^m + O(q^{m-1/2}).$$

To extend other curve results stated in the introduction, we shall need to use group theory. This can be done exactly as the curve case because of the following asymptotic formula, which is an immediate consequence of the higher dimensional Cebotarev density theorem [Fr2].

**Lemma 5.5.** *Let $f : Y \longrightarrow Z$ be a generically surjective and separable morphism between absolutely irreducible $m$-dimensional varieties $Y$ and $Z$ defined over $\mathbf{F}_q$. Let $G$ (resp. $N$) be the arithmetic (resp. geometric) monodromy group of the map $f$. Let $xN$ be the coset which is the Frobenius generator of the cyclic group $G/N$. Then, we have the formula for the value set cardinality $V_f = |f(Y(\mathbf{F}_q))|$:*

$$V_f = (1 - s_0)q^m + O(q^{m-1/2}),$$

*where $s_0 = |S_0|/|N|$ and $S_0$ is the set of fixed point free elements in $xN$ as before.*

In the special case $Y = Z$ and $f$ is the identity map (thus $s_0 = 0$), the above lemma reduces to the well known Lang-Weil estimate. By Theorem 1.3, we obtain

**Corollary 5.6.** *Let $f : Y \longrightarrow Z$ be a generically surjective and separable map of degree $n$ between two $m$-dimensional absolutely irreducible varieties over $\mathbf{F}_q$. Assume that the covering is not exceptional and that the Galois closure of the covering is regular ($G = N$). Assume further that the monodromy group is not a Frobenius group of order $n(n-1)$. Then for $n > 6$, we have*

$$V_f \leq (1 - \frac{2}{n})q^m + O(q^{m-1/2}),$$

*with equality holding (asymptotically) if and only if $G = N$ is a Frobenius group of order $n(n-1)/2$.*

Clearly, stronger results such as Theorem 1.2 can also be extended to some higher dimensional cases for regular coverings with suitable total and tame ramification assumptions. We can prove a slightly weaker version of Theorem 1.1 that applies to higher dimensional varieties and to curves without assuming the existence of a totally ramified point. We are certain that $5/4$ can be replaced by 2 in the next result.

**Corollary 5.7.** *Let $f : Y \longrightarrow Z$ be a generically surjective and separable map of degree $n$ between two $m$-dimensional absolutely irreducible varieties over $\mathbf{F}_q$. Assume that the covering is not exceptional and that the monodromy group is not Frobenius of order $n(n-1)$. Then for $n > 6$,*

$$V_f \leq (1 - \frac{5}{4n})q^m + O(q^{m-1/2}).$$

**Proof.** We argue as in the proof of Theorem 3.6. We may assume that $f$ is indecomposable as a cover. Let $G$ and $N$ be the corresponding monodromy groups acting transitively on the corresponding set $X$. By Lemma 5.5, it suffices to prove that $s_0 \geq 5/4n$.

By [LS], it follows that $\mu > n/3$ unless $E := F^*(G) = L_1 \times \ldots \times L_t$, where each $L_i \cong A_\ell$, the alternating group of degree $\ell$ (with $\ell \geq 5$). Moreover, we may assume that in the latter case that the stabilizer in $E$ of a point is the product of stabilizers of $k$-sets for some $k$ with $1 \leq k < \ell/2$.

If $\mu > n/3$, then arguing as in section 2, we deduce that $s_0 \geq 5/4n$ (use the analog of 2.9).

Consider the remaining situation. If $N$ not transitive on the set of $L_i$ (by conjugation), then any element of $xN$ (where $xN$ generates $G/N$) will not normalize each $L_i$. It follows that any element of $xN$ fixes at most $n/5$ points, and we can argue as in the previous paragraph (because we only need to know the minimal degree for elements in the coset $xN$).

If $N$ is transitive on the $L_i$, then it is straightforward to compute that $r_2 \geq 2$ unless $t = 1 = k$. Then, $N$ is 3-transitive and $s_0 \geq 1/6$.

## References


[ATLAS] An Atlas of Finite Groups, J. Conway, R. Curtis, S. Norton, R. Parker and R. Wilson, Oxford U. Press, Oxford, 1985.

[BS] B.J. Birch and H.P.F. Swinnerton-Dyer, Note on a problem of Chowla, Acta Arith., V(1959), 417-423.

[Bo] N. Boston, W. Dabrowski, T. Foguel, P.J. Gies, J. Leavitt, D.T. Ose, and D.A. Jackson, The proportion of fixed-point-free elements of a transitive permutation group, Comm. in Algebra, 21(9), 3259-3275(1993).

[BLP] J.P. Buhler, H. W. Lenstra, Jr. and C. Pomerance, Factoring integers with the number field sieve, in "The Development of The Number Field Sieve", Lecture Notes in Math., 1554.

[CC] P. J. Cameron and A. M. Cohen, On the number of fixed point free elements in a permutation group, Annals of Discrete Math. 106/107 (1992), 135-138.

[Ch] S. Chowla, The Riemann zeta and allied functions, Bull. Amer. Math. Soc., 58(1952), 287-303.

[Co] S.D. Cohen: The distribution of polynomials over finite fields, Acta Arith. 17 (1970), 255-271.

[Fe] W. Feit, On symmetric balanced incomplete block designs with doubly transitive automorphism groups, J. Comb. Theory Ser. A 14 (1973), 221-247.

[Fr1] M. Fried, On a conjecture of Schur, Mich. Math. J. 17 (1970), 41-55.

[Fr2] M. Fried, On Hilbert's irreduciblity theorem, J. Number Theory, 6(1974), 211-232.

[Fr3] M. Fried, On a theorem of MacCluer, Acta Arith. 25 (1973/74), 121-126.

[FGS] M. Fried, R. Guralnick and J. Saxl, Schur covers and Carlitz's conjecture, Israel J. Math. 82 (1993), 157-225.

[Fu] W. Fulton, Hurwitz schemes and irreducibility of moduli of algebraic curves, Annals of Math. 90 (1969), 542-575.

[Gr] A. Grothendieck, Revêtement étales et groupe fondamental (SGA1), Lecture Notes in Math. # 224, Springer-Verlag, New York-Heidelberg, Berlin, 1971.

[GS] R. Guralnick and J. Saxl, Monodromy groups of polynomials, in Groups of Lie Type and their Geometries, W. Kantor and L. Di Martino, eds, Cambridge University Press, Cambridge, 1995, 125-150.

[Ha] R. Hartshorne, Algebraic Geometry, Springer-Verlag, New York-Heidelberg-Berlin, 1977.

[HB] B. Huppert and N. Blackburn, Finite Groups III, Springer-Verlag, New York-Heidelberg-Berlin, 1982.

[Jo] C. Jordan, Recherches sur les substitutions, J. Liouville, 17(1872), 351-367 (Oeuvres, I, no.52).

[Ka] W. Kantor, Homogeneous designs and geometric lattices, J. Combinatorial Theory, Series A 38 (1985), 66-74.
[Le] H.W. Lenstra Jr., personal communication.
[LS] M. Liebeck and J. Saxl, Minimal degrees of primitive permutation groups with an application to monodromy groups of Riemann surfaces, Proc. London Math. Soc. 63 (1991), 266-314.
[Mc] J. McLaughlin, Some subgroups of $SL_n(F_2)$ generated by transvections, Illinois J. Math. 13 (1969), 108-115.
[Mu] G.L. Mullen, Permutation polynomials over finite fields, in "Finite Fields, Coding Theory and Advances in Communications and Computing", edited by G.L. Mullen and P.J.S. Shiue, Marcel Dekker, 1993, 131-151.
[Mü] 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.
[Pa] D. Passman, Permutation Groups, W. A. Benjamin, Inc., New York, Amsterdam, 1968.
[S1] J-P. Serre, Local Fields, GTM 67, Springer-Verlag, 1979.
[S2] J-P. Serre, Topics in Galois Theory, Jones and Bartlett Publishers, 1992.
[Tu] G. Turnwald, A new criterion for permutation polynomials, Finite Fields Appl. 1 (1995), 64-82.
[U] S. Uchiyama, Sur le nombre des valeurs distinctes d'un polynôme a coefficients dans un corps fini, Proc. Japan Academy 30 (1954), 930-933.
[Wa] D. Wan, A $p$-adic lifting lemma and its application to permutation polynomials, in "Finite Fields, Coding Theory and Advances in Communications and Computing", edited by G.L. Mullen and P.J.S. Shiue, Marcel Dekker, 1993, 209-216.
[Wi] H. Wielandt, Finite Permutation Groups, Academic Press, New York, 1964.