PERMUTATION GROUPS GENERATED BY BINOMIALS

MICHAEL E. ZIEVE

ABSTRACT. Let $G(q)$ be the group of permutations of $\mathbb{F}_q^*$ generated by those permutations which can be represented as $c \mapsto ac^m + bc^n$ with $a, b \in \mathbb{F}_q^*$ and $0 < m < n < q$. We show that there are infinitely many q for which $G(q)$ is the group of all permutations of $\mathbb{F}_q^*$. This resolves a conjecture of Vasilyev and Rybalkin.

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field of cardinality q. We will be interested in the group of permutations of $\mathbb{F}_q$ induced by certain special permutations, especially by permutations of the form $c \mapsto f(c)$ where $f(x) \in \mathbb{F}_q[x]$ is a polynomial having a particularly simple form. One result along these lines is due to Carlitz [3] (see also [17]), who showed that if $q > 2$ then the symmetric group S_q is generated by the permutations of $\mathbb{F}_q$ induced by x^{q-2} and by degree-one polynomials in $\mathbb{F}_q[x]$. Recently Vasilyev and Rybalkin [15] investigated the group of permutations of $\mathbb{F}_q$ generated by those permutations which are induced by binomials. In order to obtain a problem which is not solved by Carlitz's result, they required that the binomials be "honest" binomials, in the sense that they are not monomials in disguise. One way to disguise a monomial is to add to it some multiple of $x^q - x$, since this does not affect the function it induces on $\mathbb{F}_q$. Another way to disguise a monomial is to add a constant to it, which does not affect whether or not the function induces a permutation of $\mathbb{F}_q$. In light of these two operations, Vasilyev and Rybalkin restrict to binomials of the form $ax^m + bx^n$ with $a, b \in \mathbb{F}_q^*$ and $0 < m < n < q$. Note that any such binomial fixes 0, so if it induces a permutation of $\mathbb{F}_q$ then it also induces a permutation of $\mathbb{F}_q^*$. We write $G(q)$ for the subgroup of S_{q-1} generated by all such binomial permutations:

The author thanks Cheryl Praeger and Pablo Spiga for helpful correspondence about group theory, and especially for pointing him to [12]. The author also thanks Igor Shparlinski and Kannan Soundararajan for discussions about Remark 6.2, and the NSF for support under grant DMS-1162181.

Definition 1.1. Let $G(q)$ be the group of permutations of $\mathbb{F}_q^*$ generated by the permutations of $\mathbb{F}_q^*$ which can be represented as $ax^m + bx^n$ with $a, b \in \mathbb{F}_q^*$ and $0 < m < n < q$.

Vasilyev and Rybalkin conjectured [15, Conj. 2] that there are infinitely many prime powers q for which $G(q)$ equals the group S_{q-1} of all permutations of $\mathbb{F}_q^*$. We remark that such prime powers q seem to be rare: for instance, Vasilyev and Rybalkin checked that there are precisely 18 such q with $q < 5000$. Our main result asserts that there do indeed exist infinitely many such q:

Theorem 1.2. *There are infinitely many primes p for which $G(p^2)$ equals S_{p^2-1}. In fact,*

$$\liminf_{N\to\infty} \frac{\#\{\text{primes } p \le N : G(p^2) = S_{p^2-1}\}}{\#\{\text{primes } p \le N\}} \ge \frac{1}{96}.$$

We did not attempt to optimize the bound 1/96 in this result. This bound can be improved by using further arguments of a similar nature to the arguments in our proof. However, it is not clear to us whether this bound can be improved to 1.

Our proof of Theorem 1.2 relies on the classification of primitive subgroups of S_n which contain an n-cycle; here a subgroup H of S_n is *primitive* if the only partitions of $\{1, 2, \ldots, n\}$ which are preserved by H are the trivial partitions $\{\{1, 2, \ldots, n\}\}$ and $\{\{1\}, \{2\}, \ldots, \{n\}\}$. This classification is a consequence of the classification of finite simple groups. An unusual feature of our situation is that it is easy to construct a $(p^2 - 1)$-cycle in $G(p^2)$, while the difficult part of our proof is showing that $G(p^2)$ is primitive. Fortunately, not many partitions of $\{1, 2, \ldots, p^2 - 1\}$ are preserved by the $(p^2 - 1)$-cycle, and we show that any such partition besides the two trivial ones will not be preserved by some member of one of three known families of permutation binomials on $\mathbb{F}_{p^2}$, at least if p is a sufficiently large prime which is congruent to either 5 or 11 mod 24.

We do not know whether there are infinitely many primes p for which $G(p)$ equals S_{p-1}. In fact we do not even have a guess what the answer should be. As we will explain, existing conjectures about permutation binomials "almost" imply that there are only finitely many such p, but only if we change a certain constant in those conjectures in a way that makes them false. It would be interesting to analyze this question further.

Related permutation groups have been considered in the literature, for instance see [13]. Most notably, Wan and Lidl [16] determined the group $W(q, d)$ of permutations of $\mathbb{F}_q$ generated by all permutations

induced by polynomials of the form $x^r h(x^d)$ where d is a fixed divisor of $q-1$, and $r \in \mathbb{Z}$ and $h \in \mathbb{F}_q[x]$ are allowed to vary. The Wan–Lidl group lies "behind the scenes" for the work of the present paper, since if d denotes the greatest common divisor of all the integers $\gcd(n-m, q-1)$ where there is a permutation of $\mathbb{F}_q$ induced by a binomial having terms of degrees m and n (with $0 < m < n < q$), then $G(q)$ is contained in $W(q,d)$. Thus, in order that $G(q)$ should equal S_{q-1}, it is necessary (but not always sufficient) that $d = 1$.

This paper is organized as follows. In the next section we review the group-theoretic results we will use. In section 3 we present the permutation binomials which will be used in our proof. We prove Theorem 1.2 in section 5, after showing that $G(p^2)$ is primitive for certain classes of primes p in section 4. In section 6 we discuss whether there are infinitely many primes p for which $G(p)$ equals S_{p-1}. We conclude in section 7 by mentioning some questions for further study.

2. Primitive subgroups of S_n containing an n-cycle

In this section we recall the group-theoretic result needed in our proof.

Definition 2.1. If G is a subgroup of S_n, then a partition $\mathcal{P}$ of $\{1, 2, \ldots, n\}$ is called *G-invariant* if, for every part S in $\mathcal{P}$ and every $g \in G$, the set $g(S)$ is also a part in $\mathcal{P}$.

Definition 2.2. A subgroup G of S_n is called *primitive* if the only G-invariant partitions of $\{1, 2, \ldots, n\}$ are the trivial coarse partition $\{\{1, 2, \ldots, n\}\}$ and the trivial fine partition $\{\{1\}, \{2\}, \ldots, \{n\}\}$.

We will use the following result (whose proof relies on the classification of finite simple groups):

Theorem 2.3. *A primitive subgroups G of S_n contains an n-cycle if and only if one of the following holds:*

1. *$G = S_n$ for some $n \geq 1$ or $G = A_n$ for some odd $n \geq 3$*
2. *$C_p \leq G \leq \mathrm{AGL}_1(p)$ where $n = p$ is prime*
3. *$\mathrm{PGL}_d(\ell) \leq G \leq \mathrm{P\Gamma L}_d(\ell)$ where ℓ is a prime power, $d \geq 2$, and $n = (\ell^d - 1)/(\ell - 1)$*
4. *$G = \mathrm{PSL}_2(11)$ or M_{11}, where in both cases $n = 11$*
5. *$G = M_{23}$ where $n = 23$.*

In fact we will only need the following numerical consequence of Theorem 2.3:

Corollary 2.4. *If n is even and $n \neq (\ell^d - 1)/(\ell - 1)$ for all integers $d \geq 2$ and prime powers ℓ, then the only primitive subgroup of S_n which contains an n-cycle is S_n itself.*

Proofs of Theorem 2.3, assuming certain previous results, are given in [7, Thm. 3] and [11]. The proof in [7] relies on [6, Thm. 4.1], for which the only proof in the literature is given in [11]. The proof of Theorem 2.3 given in [11] relies on the correctness of the list in [2, p. 8] of the simple groups which occur as minimal normal subgroups of a doubly transitive group, although the proof in [2] does not address the sporadic groups except by saying they "can be handled by *ad hoc* arguments". A detailed treatment of the sporadic groups is given in [12] (see especially Table 5.1), which verifies the claim in [2], and combined with [11] yields a proof of Theorem 2.3. We remark that, besides the classification of finite simple groups, the main work in this proof is carried out in [4, 5, 8].

3. Some permutation binomials

In this section we exhibit the classes of permutation binomials which will be used in this paper. The first class of permutation binomials appeared in early work of Betti [1, p. 74] and Mathieu [10, p. 275].

Proposition 3.1. *If r is a prime power and $a \in \mathbb{F}_{r^k}^*$ is an element such that $a^{(r^k-1)/(r-1)} \neq 1$, then $f(x) := x^r - ax$ permutes $\mathbb{F}_{r^k}$.*

Proof. The function $c \mapsto f(c)$ induces a homomorphism from the additive group of $\mathbb{F}_{r^k}$ to itself, so it is bijective if and only if its kernel is trivial. The kernel is trivial if and only if a is not an $(r-1)$-th power in $\mathbb{F}_{r^k}^*$, or equivalently $a^{(r^k-1)/(r-1)} \neq 1$. □

The second class of permutation binomials we will need arose in my work with Tucker [14]. Since that paper has not been published, I include the proof of the needed result for the reader's convenience. I gave a slightly different proof in the recent paper [22].

Proposition 3.2. *If r is a prime power with $r \equiv 2 \pmod 3$, and $a \in \mathbb{F}_{r^2}^*$ is such that a^{r-1} has order $6/\gcd(r,2)$ in $\mathbb{F}_{r^2}^*$, then $f(x) := x^{r+2} + ax$ permutes $\mathbb{F}_{r^2}$.*

Proof. If $c \in \mathbb{F}_{r^2}^*$ satisfies $c^{r+1} = 1$, then $f(cx) = c \cdot f(x)$. Thus, $f(\mathbb{F}_{r^2})$ consists of the set of $(r+1)$-th roots of the elements of $f(\mathbb{F}_{r^2})^{r+1}$. The Proposition asserts that $f(\mathbb{F}_{r^2})^{r+1}$ equals $\mathbb{F}_{r^2}^{r+1}$, or in other words equals $\mathbb{F}_r$. For $c \in \mathbb{F}_{r^2}$ we compute

$$f(c)^{r+1} = (c^{r+2} + ac)^{r+1} = c^{r+1}(c^{r+1} + a)^{r+1}.$$

Writing $b := c^{r+1}$, so that $b \in \mathbb{F}_r$, we have

$$\begin{aligned} f(c)^{r+1} &= b(b+a)^{r+1} \\ &= b(b+a)^r(b+a) \\ &= b(b+a^r)(b+a) \\ &= b^3 + b^2(a+a^r) + ba^{r+1}. \end{aligned}$$

Since $3 \nmid r$, it follows that

$$f(c)^{r+1} = \Big(b + \frac{a+a^r}{3}\Big)^3 - \Big(\frac{a+a^r}{3}\Big)^3 + b \cdot \Big(a^{r+1} - \frac{(a+a^r)^2}{3}\Big).$$

Next we compute

$$a^{r+1} - \frac{(a+a^r)^2}{3} = -\frac{1}{3}(a^2 - a^{r+1} + a^{2r}) = -\frac{a^2}{3}(1 - a^{r-1} + a^{2r-2}),$$

which equals 0 because a^{r-1} is a primitive $6/\gcd(r,2)$-th root of unity and hence is a root of the $6/\gcd(r,2)$-th cyclotomic polynomial. Thus, for $c \in \mathbb{F}_{r^2}$ we have

$$f(c)^{r+1} = \Big(c^{r+1} + \frac{a+a^r}{3}\Big)^3 - \Big(\frac{a+a^r}{3}\Big)^3.$$

Since $r \equiv 2 \pmod 3$, we know that x^3 permutes $\mathbb{F}_r$ (because it induces a homomorphism from $\mathbb{F}_r^*$ to itself with trivial kernel). It follows that $g(x) := (x+d)^3 - d^3$ permutes $\mathbb{F}_r$, where $d := (a+a^r)/3$. Finally, since $\mathbb{F}_{r^2}^{r+1} = \mathbb{F}_r$, we see that c^{r+1} takes on all values in $\mathbb{F}_r$ when c varies over $\mathbb{F}_{r^2}$, so that $f(c)^{r+1} = g(c^{r+1})$ also takes on all values in $\mathbb{F}_r$, whence $f(\mathbb{F}_{r^2})^{r+1} = \mathbb{F}_r$, as desired. □

Many variants of the above permutation polynomials can be obtained using related ideas; see [14, 18, 19, 20, 21, 22] for details.

The next result comes from my joint work with Masuda, and is a part of [9, Thm. 1.5]:

Proposition 3.3. *Let $q \geq 4$ be a prime power, and let $0 < m < n$ be integers such that $\gcd(m, n, q-1) = 1$. Let T denote the number of values $a \in \mathbb{F}_q$ for which $ax^m + x^n$ permutes $\mathbb{F}_q$, and write $s := (q-1)/\gcd(n-m, q-1)$. Then*

$$\frac{T}{(s-1)!} \geq \frac{q - 2\sqrt{q} + 1}{s^{s-1}} - (s-3)\sqrt{q} - 2.$$

We will use the following consequence of this result.

Corollary 3.4. *For any positive integer s and any prime power q with $q \equiv 1 \pmod s$, let N denote the number of values $a \in \mathbb{F}_q^*$ for which*

$x(a+x^{(q-1)/s})$ permutes $\mathbb{F}_q$. If $s=2$ and $q\geq 7$ then $N>0$. If $s=8$ and $q\geq 109951213112009$ then $N\geq 3$.

Proof. If $s=2$ then Proposition 3.3 gives $T\geq (q-2\sqrt{q}+1)/2+\sqrt{q}-2=(q-3)/2$, so that if $q>5$ then $N\geq T-1>0$. If $s=8$ then Proposition 3.3 gives $T/7!\geq (\sqrt{q}-1)^2/8^7-5\sqrt{q}-2$, and one can check that this implies $T>3$ (and hence $N\geq 3$) when $q\geq 109951213112009$. □

Remark 3.5. The value 109951213112009 in this result can be improved by various methods, but we do not see how to improve it to a reasonably small value.

4. Primitivity of $G(q)$

In this section we show that the group $G(q)$ is a primitive subgroup of S_{q-1} for all q satisfying certain properties. We first show that if $G(q)$ is nontrivial then it contains a $(q-1)$-cycle.

Lemma 4.1. *Let q be a prime power for which there exist $a,b\in\mathbb{F}_q^*$ and $0<m<n<q$ such that $f(x):=ax^m+bx^n$ permutes $\mathbb{F}_q$. Then, for any generator w of $\mathbb{F}_q^*$, the group $G(q)$ contains the permutation of $\mathbb{F}_q^*$ induced by wx, which is a $(q-1)$-cycle.*

Proof. Let σ and ρ be the elements of $G(q)$ induced by $f(x)$ and $wf(x)$, respectively. Then $\rho\sigma^{-1}$ is induced by wx, which is a $(q-1)$-cycle. □

Corollary 4.2. *Let $q>5$ be a prime power which cannot be written as 2^p with p prime. Then, for any generator w of $\mathbb{F}_q^*$, the group $G(q)$ contains the map induced by wx, which is a $(q-1)$-cycle.*

Proof. In light of Lemma 4.1, it suffices to show that there is a permutation binomial over $\mathbb{F}_q$ in which both terms have degrees between 1 and $q-1$. If $q=r^e$ with $e>1$ and $r>2$, this follows from Proposition 3.1. If q is odd and $q>5$ then it follows from Corollary 3.4 with $s=2$. □

Remark 4.3. We note that $G(q)$ is the trivial group if $q=2^p$ where 2^p-1 is prime. For, in this case any $0<m<n<q$ will satisfy $\gcd(n-m,q-1)=1$, so that every element of $\mathbb{F}_q^*$ has a unique $(n-m)$-th root in $\mathbb{F}_q^*$. For any $a,b\in\mathbb{F}_q^*$ it follows that ax^m+bx^n does not permute $\mathbb{F}_q$, since it takes value 0 when x is either 0 or the $(n-m)$-th root of $-a/b$ in $\mathbb{F}_q^*$. Thus, if there are infinitely many Mersenne primes then there are infinitely many prime powers q for which $G(q)=1$.

Remark 4.4. We know very little about $G(q)$ when $q = 2^p$ where p is prime but $2^p - 1$ is composite. Proposition 3.1 implies that $G(q)$ is nontrivial if $q-1$ has a nontrivial divisor which is very small compared to $q-1$ (for instance, such a divisor must be smaller than a constant times $\log q$). But we know nothing about $G(q)$ when $q-1$ has no such divisor: it is conceivable that $G(q)$ is always trivial in this case, and it is also conceivable that $G(q)$ always equals S_{q-1} in this case.

In case $G(q)$ contains a $(q-1)$-cycle, there are only a few possibilities for a $G(q)$-invariant partition of $\mathbb{F}_q^*$:

Corollary 4.5. *Let $q > 5$ be a prime power which is either odd or a power of 4. Then every partition of $\mathbb{F}_q^*$ which is preserved by $G(q)$ must consist of all the cosets of a subgroup of $\mathbb{F}_q^*$.*

Proof. Let $\mathcal{P}$ be a partition of $\mathbb{F}_q^*$ which is preserved by $G(q)$, and let S be the part in $\mathcal{P}$ which contains 1. For any $u \in \mathbb{F}_q^*$, Corollary 4.2 implies that ux is in $G(q)$, so that $\mathcal{P}$ is preserved by ux, whence uS is a part of $\mathcal{P}$. In particular, if $v \in S$ then vS is a part of $\mathcal{P}$ which contains v, so $vS \cap S$ is nonempty, whence $vS = S$. Thus S is a nonempty subset of $\mathbb{F}_q^*$ which is closed under multiplication, so it is a subgroup. Finally, $\mathcal{P}$ consists of the sets uS with $u \in \mathbb{F}_q^*$, namely the cosets of S in $\mathbb{F}_q^*$. □

In what follows, if d is a divisor of $q-1$ then we write μ_d for the group of d-th roots of unity in $\mathbb{F}_q^*$. The next result is the key tool we will use to show in certain cases that $G(q)$ does not preserve any of the nontrivial partitions of $\mathbb{F}_q^*$ described in Corollary 4.5.

Proposition 4.6. *Let q be a prime power, and let d and k be positive divisors of $q-1$ such that $d \nmid k$. Then there are at most d elements $a \in \mathbb{F}_q^*$ for which $x^{k+1} + ax$ maps all elements of μ_d into the same coset of $\mathbb{F}_q^*$ mod μ_d.*

Proof. Fix an element $c \in \mu_d \setminus \mu_k$. Pick $a \in \mathbb{F}_q^*$ for which $f(x) := x^{k+1} + ax$ maps μ_d into a coset of $\mathbb{F}_q^*/\mu_d$. Since 1 and c are in μ_d, there exists $b \in \mu_d$ for which $f(c) = b \cdot f(1)$. Thus

$$c^{k+1} + ac = f(c) = b \cdot f(1) = b \cdot \big(1 + a\big),$$

so that

$$(c-b)a = b - c^{k+1}.$$

It follows that $c \neq b$, since otherwise the left side would be zero so also the right side would be zero, whence $c = b = c^{k+1}$ so $c^k = 1$,

contradicting our hypothesis that $c \notin \mu_k$. Thus we obtain

$$a = \frac{b - c^{k+1}}{c - b},$$

so in particular the value of a is uniquely determined by the value of b (since c is fixed). Since $b \in \mu_d$, this means there are at most d choices for a. □

Theorem 4.7. *Let $r \geq 10485731$ be a prime power with $r \equiv 2 \pmod 3$ and $r \equiv \pm 3 \pmod 8$, and let $q = r^2$. Then the group $G(q)$ is a primitive subgroup of S_{q-1}.*

Proof. By Corollary 4.5, it suffices to prove that if d is a proper divisor of $q-1$ such that $G(q)$ preserves the set of cosets of $\mathbb{F}_q^*$ mod μ_d, then $d = 1$. Let d be such a divisor of $q-1$. By Proposition 3.1, there are $q - 1 - (r+1)$ elements $a \in \mathbb{F}_q^*$ for which $x^r - ax$ permutes $\mathbb{F}_q$. Since each such polynomial $x^r - ax$ defines a function from $\mathbb{F}_q^*/\mu_d$ into itself, by Proposition 4.6 with $k = r-1$ we conclude that either d divides $r-1$ or $d \geq q - 1 - (r+1)$. But $q - 1 - (r+1) > (q-1)/2 \geq d$, so in fact $d \mid (r-1)$.

Next, Proposition 3.2 implies that there are $2(r-1)$ elements $a \in \mathbb{F}_q^*$ for which $x^{r+2} + ax$ permutes $\mathbb{F}_q$. By Proposition 4.6 with $k = r+1$, we conclude that d divides $r+1$, so $d \mid \gcd(r-1, r+1) = 2$.

Finally, by Corollary 3.4, there are at least three elements $a \in \mathbb{F}_q^*$ for which $x(x^{(q-1)/8} + a)$ permutes $\mathbb{F}_q$. Our hypothesis $r \equiv \pm 3 \pmod 8$ implies that $r-1$ and $r+1$ are congruent to 2 and 4 mod 8 (in some order), so that $r^2 - 1 \equiv 8 \pmod{16}$. By Proposition 4.6 with $k = (q-1)/8$, we conclude that d divides $(q-1)/8$; since $(q-1)/8$ is odd and $d \mid 2$, it follows that $d = 1$. As noted above, by Corollary 4.5 this implies that $G(q)$ is primitive. □

5. Proof of the main result

We now prove Theorem 1.2. Let r be a prime power, and write $q = r^2$. By Corollary 4.2 and Theorem 4.7, if r is sufficiently large and $r \equiv 2 \pmod 3$ and $r \equiv \pm 3 \pmod 8$, then $G(q)$ is a primitive subgroup of S_{q-1} which contains a $(q-1)$-cycle. In light of Corollary 2.4, it follows that $G(q) = S_{q-1}$ if $q-1$ cannot be written as $(\ell^d - 1)/(\ell - 1)$ with $d \geq 2$ and ℓ a prime power. Let us add the requirements that $r \equiv \pm 3 \pmod 7$ and $r \equiv \pm 6 \pmod{17}$. Then $r^2 - 2$ is divisible by both 7 and 17, and hence is not a prime power; thus $r^2 - 1 \neq (\ell^2 - 1)/(\ell - 1)$ for any prime power ℓ. Since $r^2 - 1$ is even, if $r^2 - 1 = (\ell^d - 1)/(\ell - 1)$ then $\ell^d = 1 + (r^2 - 1)(\ell - 1)$ is odd and thus ℓ is odd, whence $r^2 - 1 =$

$\ell^{d-1} + \ell^{d-2} + \cdots + 1 \equiv d \pmod 2$ implies that d is even. Since $d > 2$, we must have $d \geq 4$.

The Prime Number Theorem for arithmetic progressions implies that, as $N \to \infty$ the number of primes $r \leq \sqrt{N}$ such that

- $r \equiv 2 \pmod 3$
- $r \equiv \pm 3 \pmod 8$
- $r \equiv \pm 3 \pmod 7$
- $r \equiv \pm 6 \pmod{17}$

is asymptotic to

$$\frac{2^3}{\phi(3 \cdot 8 \cdot 7 \cdot 17)} \frac{\sqrt{N}}{\log(\sqrt{N})} = \frac{1}{48} \frac{\sqrt{N}}{\log(N)}.$$

For any fixed $d \geq 4$, the number

$$\#\Big\{\text{prime powers } \ell : \frac{\ell^d - 1}{\ell - 1} \leq N\Big\}$$

is at most the number of prime powers ℓ such that $\ell^{d-1} \leq N$. In particular, there only exist any such ℓ if $d \leq 1 + \log_2(N)$. Summing over all d, we find that

$$\#\Big\{(\ell, d) : \ell \text{ is a prime power, } d \geq 4, \text{ and } \frac{\ell^d - 1}{\ell - 1} \leq N\Big\}$$

is at most

$$\sum_{d=4}^{1+\lfloor \log_2(N) \rfloor} \sum_{\substack{\ell \text{ is a prime power} \\ \ell^{d-1} \leq N}} 1 \leq \sum_{d=4}^{1+\lfloor \log_2(N) \rfloor} \sum_{\substack{\ell \text{ is a prime power} \\ \ell^{3} \leq N}} 1 \leq \log_2(N) \cdot N^{1/3}.$$

Since the ratio

$$\frac{\log_2(N) \cdot N^{1/3}}{\sqrt{N}/(48 \log(N))}$$

approaches zero as $N \to \infty$, it follows that the number of primes $r \leq \sqrt{N}$ such that

- $r \equiv 2 \pmod 3$
- $r \equiv \pm 3 \pmod 8$
- $r \equiv \pm 3 \pmod 7$
- $r \equiv \pm 6 \pmod{17}$
- $r^2 - 1$ cannot be written as $(\ell^d - 1)/(\ell - 1)$ with $d \geq 2$ and ℓ a prime power

is asymptotic to $\sqrt{N}/(48\log(N))$. By Corollary 4.2 and Theorem 4.7, for any such r the group $G(r^2)$ is primitive and contains an (r^2-1)-cycle, and hence (by Corollary 2.4) equals the symmetric group on $\mathbb{F}_{r^2}^*$. This proves Theorem 1.2.

6. Prime fields

In this section we discuss whether there are infinitely many primes p for which $G(p)$ equals S_{p-1}. We will focus on the question whether there are infinitely many primes p for which $G(p)$ is primitive. According to the heuristic in [9, Section 4], for all sufficiently large primes p we expect that every permutation binomial ax^m+bx^n over $\mathbb{F}_p$ (with $a,b\in\mathbb{F}_p^*$ and $0<m<n<p$) will satisfy $\gcd(n-m,p-1)>p/(2\log p)$. In [9] we noted that we had verified this conclusion for all primes $p<10^5$; an independent verification for $p<15000$ is announced in [15]. We now show that the factor '2' in this bound plays a crucial role in connection with $G(p)$, in the sense that if this factor could be improved to a constant less than 1 then there would only be finitely many primes p for which $G(p)$ is primitive.

Proposition 6.1. *Fix a real number $c>1$. For any prime power q which is sufficiently large compared to c, if $G(q)$ is primitive then there exist $a,b\in\mathbb{F}_q^*$ and $0<m<n<q$ such that ax^m+bx^n induces a permutation of $\mathbb{F}_q$ and $\gcd(n-m,q-1)<c(q-1)/\log q$.*

Proof. Let q be a prime power such that $G(q)$ is primitive but all permutation binomials ax^m+bx^n over $\mathbb{F}_q$ have $\gcd(n-m,q-1)\geq c(q-1)/\log q$. Primitivity implies in particular that there is no divisor k of $q-1$ such that $1<k<q-1$ and $G(q)$ induces a permutation on $\mathbb{F}_q^*/\mu_k$, where μ_k denotes the group of k-th roots of unity in $\mathbb{F}_q^*$. It follows that the gcd of all the numbers $\gcd(n-m,q-1)$ for which ax^m+bx^n permutes $\mathbb{F}_q$ (with $a,b\in\mathbb{F}_q^*$ and $0<m<n<q$) must be 1. Writing $\gcd(n-m,q-1)=(q-1)/d$ where $d\mid(q-1)$, it follows that

$$1=\gcd(\{(q-1)/d:\ d\mid(q-1)\text{ and }d\leq(\log q)/c\}),$$

or equivalently

$$q-1=\operatorname{lcm}(\{d:\ d\mid(q-1)\text{ and }d\leq(\log q)/c\}),$$

which can be rewritten as

$$q-1=\operatorname{lcm}(\{d:\ d\mid(q-1),\ \ d\text{ is a prime power, and }d\leq(\log q)/c\}),$$

or equivalently

$$q-1 \quad \leq \prod_{\substack{d \mid (q-1) \\ d \leq (\log q)/c \\ d=p^k \text{ with } p \text{ prime and } k \geq 1}} p.$$

Removing the condition $d \mid (q-1)$ can only increase the right side; if we remove this condition and then take logs of both sides, we obtain

$$\log(q-1) \quad \leq \sum_{\substack{d \leq (\log q)/c \\ d=p^k \text{ with } p \text{ prime and } k \geq 1}} \log p.$$

By the Prime Number Theorem, the right side is asymptotic to $(\log q)/c$ as $q \to \infty$, so for sufficiently large q the right side is smaller than the left side. This contradiction completes the proof. □

Remark 6.2. Correspondence with Igor Shparlinski and Kannan Soundararajan yielded a heuristic argument suggesting a converse to the above result. Namely, suppose there exists a number $c < 1$ such that, if q is sufficiently large q and $0 < m < n < q$ satisfy $\gcd(m, n, q-1) = 1$ and $\gcd(n-m, q-1) > cq/\log q$, then there exist $a, b \in \mathbb{F}_q^*$ such that $ax^m + bx^n$ permutes $\mathbb{F}_q$. We do not know whether such a number c should exist, but a result in this direction (with c replaced by $2 \log\log q$) is proved in [9, Thm. 3.1]. Our heuristic suggests that, if such a number $c < 1$ exists, then there should be infinitely many primes q for which $G(q)$ is primitive.

7. Concluding remarks

We have shown that $G(q)$ equals S_{q-1} for many q's which are squares of primes: in fact, for a density-1 subset of those q's which are squares of the primes in certain arithmetic progressions. We do not know whether $G(q)$ equals S_{q-1} for a density-1 subset of the q's which are squares of primes. We also do not know how often $G(q)$ equals S_{q-1} for other types of prime powers q. In particular, does this happen for infinitely many primes q? We suspect that it happens whenever q is a sufficiently large power of 4.

When $G(q)$ does not equal S_{q-1}, it would be interesting to investigate what the group $G(q)$ turns out to be. Let $r(q)$ be the greatest common divisor of all numbers of the form $\gcd(n-m, q-1)$ where $0 < m < n < q$ and there exist $a, b \in \mathbb{F}_q^*$ such that $ax^m + bx^n$ permutes $\mathbb{F}_q$. Proposition 4.6, and even moreso its proof, suggests that usually $r(q)$ will be the largest proper divisor d of $q-1$ for which $G(q)$ permutes the cosets of $\mathbb{F}_q^*$ mod μ_d. When this happens, one might guess that $G(q)$ usually equals the full group of permutations of $\mathbb{F}_q$ induced by polynomials of

the form $x^i h(x^{r(q)})$ with $i > 0$. The latter group was determined by Wan and Lidl [16]: it is the semidirect product of $(\mathbb{Z}/r(q)\mathbb{Z})^*$ by the wreath product $(\mathbb{Z}/r(q)\mathbb{Z}) \wr S_{(q-1)/r(q)}$. It seems that one can at least show that $G(q)$ contains a copy of $S_{(q-1)/r(q)}$ under some hypotheses, since the action of $G(q)$ on $\mathbb{F}_q^*/\mu_{r(q)}$ induces a map $G(q) \to S_{(q-1)/r(q)}$ whose image is primitive and contains a $(q-1)/r(q)$-cycle. It would be interesting to investigate this further.

References

[1] E. Betti, Sulla risoluzione delle Equazioni algebriche, *Ann. Sci. Mat. Fis.* **3** (1852), 49–115. 4

[2] P. J. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981), 1–22. 4

[3] L. Carlitz, Permutations in a finite field, *Proc. Amer. Math. Soc.* **4** (1953), 538. 1

[4] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups*. (Clarendon Press, Oxford, 1985). 4

[5] C. W. Curtis, W. M. Kantor and G. M. Seitz, The 2-transitive permutation representations of the finite Chevalley groups, *Trans. Amer. Math. Soc.* **218** (1976), 1–59. 4

[6] W. Feit, Some consequences of the classification of finite simple groups. In *The Santa Cruz conference on finite groups*, Proc. Sympos. Pure Math. 37 (American Mathematical Society, 1980), pp. 175–181. 4

[7] G. A. Jones, Cyclic regular subgroups of primitive permutation groups, *J. Group Theory* **5** (2002), 403–407. 4

[8] M. W. Liebeck, C. E. Praeger and J. Saxl, The maximal factorizations of the finite simple groups and their automorphism groups, *Memoirs Amer. Math. Soc.* **432** (1990). 4

[9] A. M. Masuda and M. E. Zieve, Permutation binomials over finite fields, *Trans. Amer. Math. Soc.* **361** (2009), 4169–4180. 5, 10, 11

[10] É. Mathieu, Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables, *J. Math. Pures Appl. (2)* **6** (1861), 241–323. 4

[11] J. P. McSorley, Cyclic permutations in doubly-transitive groups, *Comm. Algebra* **25** (1997), 33–35. 4

[12] C. E. Praeger and L. H. Soicher, *Low rank representations and graphs for sporadic groups*. (Cambridge University Press, 1997). 1, 4

[13] R. M. Stafford, Groups of permutation polynomials over finite fields, *Finite Fields Appl.* **4** (1998), 450–452. 2

[14] T. J. Tucker and M. E. Zieve, Permutation polynomials, curves without points, and Latin squares, preprint, 2000. 4, 5

[15] N. N. Vasilyev and M. A. Rybalkin, Permutation binomials and their groups, *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)* **387** (2011), 83–101; translated in *J. Math. Sci. (N. Y.)* **179** (2011), 679–689. 1, 2, 10

[16] D. Wan and R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, *Monatsh. Math.* **112** (1991), 149–163. 2, 12

[17] M. E. Zieve, On a theorem of Carlitz, *J. Group Theory*, to appear. arXiv:0810.2834. 1

[18] M. E. Zieve, Some families of permutation polynomials over finite fields, *Internat. J. Number Theory* **4** (2008), 851–857. 5

[19] M. E. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$, *Proc. Amer. Math. Soc.* **137** (2009), 2209–2216. 5

[20] M. E. Zieve, Classes of permutation polynomials based on cyclotomy and an additive analogue, in *Additive Number Theory*, Springer (2010), 355–359. 5

[21] M. E. Zieve, Permutation polynomials on $\mathbb{F}_q$ induced from Rédei function bijections on subgroups of $\mathbb{F}_q^*$, arXiv:1310.0776. 5

[22] M. E. Zieve, Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal latin squares, arXiv:1312.1325. 4, 5

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109–1043, USA

Mathematical Sciences Center, Tsinghua University, Beijing 100084, China

E-mail address: zieve@umich.edu

URL: www.math.lsa.umich.edu/∼zieve/