PERMUTATION BINOMIALS OVER FINITE FIELDS

ARIANE M. MASUDA AND MICHAEL E. ZIEVE

ABSTRACT. We prove that if $x^m + ax^n$ permutes the prime field $\mathbb{F}_p$, where $m > n > 0$ and $a \in \mathbb{F}_p^*$, then $\gcd(m-n, p-1) > \sqrt{p} - 1$. Conversely, we prove that if $q \geq 4$ and $m > n > 0$ are fixed and satisfy $\gcd(m-n, q-1) > 2q(\log\log q)/\log q$, then there exist permutation binomials over $\mathbb{F}_q$ of the form $x^m + ax^n$ if and only if $\gcd(m, n, q-1) = 1$.

1. INTRODUCTION

A polynomial over a finite field is called a *permutation polynomial* if it permutes the elements of the field. These polynomials first arose in work of Betti [1] and Hermite [10] as a way to represent permutations. A general theory was developed by Hermite [10] and Dickson [6], with many subsequent developments by Carlitz and others. The simplest class of nonconstant polynomials are the monomials x^m with $m > 0$, and one easily checks that x^m permutes $\mathbb{F}_q$ if and only if m is coprime to $q-1$. However, already for binomials the situation becomes much more mysterious. Some examples occurred in Hermite's work [10], and Mathieu [17] showed that $x^{p^i} - ax$ permutes $\mathbb{F}_q$ whenever a is not a (p^i-1)-th power in $\mathbb{F}_q$; here p denotes the characteristic of $\mathbb{F}_q$.

A general nonexistence result was proved by Niederreiter and Robinson [20] and improved by Turnwald [28]:

Theorem 1.1. *If $f(x) := x^m + ax^n$ permutes $\mathbb{F}_q$, where $m > n > 0$ and $a \in \mathbb{F}_q^*$, then either $q \leq (m-2)^4 + 4m - 4$ or $m = np^i$.*

This result implies that, when $q > m^4$, the only permutation binomials over $\mathbb{F}_q$ are the compositions of Mathieu's examples with permutation monomials. The key ingredient in the proof of Theorem 1.1 is Weil's lower bound [33] for the number of $\mathbb{F}_q$-rational points on the curve $(f(x) - f(y))/(x-y)$.

We do not know whether Theorem 1.1 can be improved in general. However, for prime fields it was improved by Wan [30] and Turnwald [28]; by using ingredients from both of their proofs, one can show the following result, which improves both of their results:

Theorem 1.2. *If $f(x) := x^m + ax^n$ permutes the prime field $\mathbb{F}_p$, where $m > n > 0$ and $a \in \mathbb{F}_p^*$, then $p - 1 \leq (m-1) \cdot \max(n, \gcd(m-n, p-1))$.*

The proofs of Wan and Turnwald rely on a trick due to Hermite [10], which can be viewed as a character sum argument: they find an integer ℓ with $0 < \ell < p-1$

Date: December 23, 2008.

2000 *Mathematics Subject Classification.* 11T06.

Key words and phrases. Permutation polynomial, finite field, Weil bound.

The authors thank Jeff VanderKam and Daqing Wan for valuable conversations, and Igor Shparlinski for suggesting the use of the Brun–Titchmarsh theorem in section 4.

such that $f(x)^\ell \bmod (x^p - x)$ has degree $p-1$. This implies that $\sum_{\alpha\in\mathbb{F}_p} f(\alpha)^\ell \neq 0$, so f does not permute $\mathbb{F}_p$. We will prove the following stronger result by exhibiting two integers ℓ, of which at least one must have the above property:

Theorem 1.3. *If $f(x) := x^m + ax^n$ permutes the prime field $\mathbb{F}_p$, where $m > n > 0$ and $a \in \mathbb{F}_p^*$, then $\gcd(m-n, p-1) \geq \sqrt{p-(3/4)} - (1/2) > \sqrt{p} - 1$.*

Writing $g := \gcd(m-n, p-1)$, the conclusion of this result can be restated as $p - 1 \leq (g+1)\cdot g$, whereas the conclusion of Theorem 1.2 says that $p-1 \leq (m-1)\cdot\max(n,g)$. Thus, Theorem 1.3 implies Theorem 1.2 whenever $g+1 \leq m-1$, which always holds except in the special case that $n = 1$ and $(m-1) \mid (p-1)$. We emphasize that Theorem 1.3 is qualitatively different from all previous results, since it gives a bound on p which depends only on $\gcd(m-n, p-1)$, and not on the degree of f.

Both Theorem 1.2 and Theorem 1.3 yield improvements to Weil's lower bound for the number of rational points on the curve $(f(x)-f(y))/(x-y)$ appearing in the proof of Theorem 1.1. On a related note, for any polynomial f over $\mathbb{F}_p$ of degree in a certain range, Voloch [29] has improved Weil's upper bound for this same curve. In a different direction, for hyperelliptic curves over $\mathbb{F}_p$ one can improve both the upper and lower Weil bound when the genus is on the order of $\sqrt{p}$, by using Stepanov's method [12, 18, 24, 19, 26, 8, 34]. All of these improvements are specific to prime fields. It would be interesting to understand what are the types of curves for which one has such improvements to Weil's bounds.

Theorem 1.3 is not true for nonprime fields; one counterexample is $x^{10} + 3x$ over $\mathbb{F}_{343}$, and we have found several infinite families of counterexamples, which we will describe in a forthcoming paper.

Returning to prime fields, we suspect that Theorem 1.3 can be improved. We checked via computer that, for $p < 10^5$, the hypotheses of Theorem 1.3 imply that $\gcd(m-n, p-1) > p/(2\log p)$. It seems likely that this improved result remains true for larger p, but we do not know a proof. The best we can do is give a heuristic to the effect that 'at random' there would not be any permutation binomials $x^m + ax^n$ over $\mathbb{F}_q$ with $\gcd(m-n, q-1) < q/(2\log q)$. Of course, our examples over nonprime fields show that this heuristic is not always correct, but those examples exhibit nonrandom features dependent on the subfield structure of $\mathbb{F}_q$, which is in line with our 'at random' notion.

Conversely, following earlier investigations of Hermite [10] and Brioschi [2, 3], Carlitz [4] studied permutation binomials of the form $x^n(x^{(q-1)/2} + a)$. He showed that there are permutation binomials of this shape (with $n = 1$ and $a \in \mathbb{F}_q^*$) whenever $q \geq 7$. He proved a similar result for the form $x(x^{(q-1)/3} + a)$, and more generally in a paper with Wells [5] he proved

Theorem 1.4. *If $d > 0$ and $q \equiv 1 \pmod{d}$, where q is sufficiently large compared to d, then for each $n > 0$ with $\gcd(n, q-1) = 1$ there exists $a \in \mathbb{F}_q^*$ such that $x^n(x^{(q-1)/d} + a)$ permutes $\mathbb{F}_q$.*

The proof of this result is quite remarkable, as it uses the Weil lower bound on an auxiliary curve to prove the existence of permutation binomials. This (and a generalization in [32]) is the only known instance of the Weil bound being used to prove existence of permutation polynomials. We give a new proof of a refined version of Theorem 1.4, which allows us to estimate the number of such a's:

Theorem 1.5. *Pick integers $0 < n < m$ such that $\gcd(m, n, q-1) = 1$, and suppose $q \geq 4$. If $\gcd(m-n, q-1) > 2q(\log\log q)/\log q$, then there exists $a \in \mathbb{F}_q^*$ such that $x^m + ax^n$ permutes $\mathbb{F}_q$. Further, letting T denote the number of values $a \in \mathbb{F}_q$ for which $x^m + ax^n$ permutes $\mathbb{F}_q$, and putting $r := (q-1)/\gcd(m-n, q-1)$, we have*

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

We note that the condition $\gcd(m, n, q-1) = 1$ is clearly necessary if $x^m + ax^n$ is to permute $\mathbb{F}_q$. In some special cases, a weaker estimate for T was derived in a recent paper by Laigle-Chapuy [13], via methods quite different from ours.

We checked that, for each $q < 10^6$, and for every $m > n > 0$ satisfying $\gcd(m, n, q-1) = 1$ and $\gcd(m-n, q-1) > 2q/\log q$, there exists $a \in \mathbb{F}_q^*$ such that $x^m + ax^n$ permutes $\mathbb{F}_q$. Combined with our previously mentioned computer data, this paints a rather clear picture of permutation binomials over prime fields.

As a final remark, we note that several papers prove results about the special binomials $x^m + ax$. In general, if a binomial has a term of degree coprime to $q-1$, then one can convert it to this special form by composing with suitable permutation monomials and reducing mod $(x^q - x)$. However, there are binomials for which this is impossible. For instance, $f(x) := x^{26} + 17x^3$ permutes $\mathbb{F}_{139}$, but the degrees of both terms of f have a common factor with 138.

Throughout this paper, $\mathbb{F}_q$ is the field of order q, and p is the characteristic of $\mathbb{F}_q$. In particular, p is always prime. We prove Theorem 1.3 in the next section. Then in Section 3 we prove Theorem 1.5, and in the final section we give the heuristic argument mentioned above. In an appendix we include a proof of Theorem 1.2.

2. Nonexistence results

In this section we prove Theorem 1.3 in the following form:

Theorem 2.1. *Suppose $x^n(x^k + a)$ permutes $\mathbb{F}_p$, where $n, k > 0$ and $a \in \mathbb{F}_p^*$. Then $\gcd(k, p-1) \geq \sqrt{p - (3/4)} - (1/2) > \sqrt{p} - 1$.*

Our proof relies on Hermite's criterion [10, 6]:

Lemma 2.2. *A polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if*

1. *for each i with $0 < i < q-1$, the reduction of f^i modulo $x^q - x$ has degree less than $q-1$; and*
2. *f has precisely one root in $\mathbb{F}_q$.*

Proof of Theorem 2.1. Pick $j > 0$ such that $jk \equiv \gcd(k, p-1) \bmod (p-1)$ and $\gcd(j, p-1) = 1$; then $x^n(x^k + a)$ permutes $\mathbb{F}_p$ if and only if $x^{nj}(x^{\gcd(k,p-1)} + a)$ permutes $\mathbb{F}_p$, so we may assume that k divides $p-1$. Suppose $f := x^n(x^k + a)$ permutes $\mathbb{F}_p$, where $k \mid (p-1)$ and $k < \sqrt{p - (3/4)} - (1/2)$ (and $n, k > 0$ and $a \in \mathbb{F}_p^*$). Then $k^2 + k + 1 < p$. Let r be the least integer such that $r \geq (p-1-k)/k^2$. Then $r < (p-1-k)/k^2 + 1$, so

$$kr < (p-1)/k - 1 + k = (k-1)(1 - (p-1)/k) + p - 1 \leq p - 1.$$

Also the inequality $k^2 + k + 1 < p$ implies $(p-1-k)/k^2 > 1$, so $r > 1$.

We will apply Hermite's criterion with exponent kr. To this end, we compute

$$f^{kr} = x^{nkr}(x^k + a)^{kr} = x^{nkr} \sum_{i=0}^{kr} \binom{kr}{i} a^{kr-i} x^{ki}.$$

Write $f^{kr} = \sum_{i=0}^{kr} b_i x^{nkr+ki}$, where $b_i = \binom{kr}{i} a^{kr-i}$. Since $0 < kr < p$ and p is prime, each b_i is nonzero. Thus, the degrees of the terms of f^{kr} are

$$nkr, nkr + k, nkr + 2k, \ldots, nkr + k^2 r.$$

Since $k^2 r \geq p - 1 - k$, the degrees include members of every residue class modulo $p-1$ containing multiples of k. In particular, there is a term of degree divisible by $p-1$; but, since $0 < kr < p-1$, Hermite's criterion implies that f^{kr} cannot have a unique term of degree divisible by $p-1$, so there must be more than one such term. Thus, $nkr \equiv -E \bmod (p-1)$ for some E with $0 \leq E \leq k^2 r - (p-1)$.

Likewise, the degrees of the terms of $f^{k(r-1)}$ are

$$nk(r-1), nk(r-1) + k, nk(r-1) + 2k, \ldots, nk(r-1) + k^2(r-1).$$

Since $k^2(r-1) < p - 1 - k$, these degrees are all in distinct classes modulo $p-1$, so by Hermite's criterion none of the degrees can be divisible by $p-1$. Thus, $nk(r-1) \equiv F \bmod (p-1)$ for some F with $k \leq F \leq p - 1 - k - k^2(r-1)$.

Now we have

$$E(r-1) \equiv -nkr(r-1) \equiv -Fr \bmod (p-1),$$

so $E(r-1) + Fr$ is a multiple of $p-1$. But

$$\begin{aligned} 0 < kr &\leq E(r-1) + Fr \\ &\leq k^2 r(r-1) - (p-1)(r-1) + (p-1)r - kr - k^2(r-1)r \\ &= p - 1 - kr < p - 1, \end{aligned}$$

so $E(r-1) + Fr$ lies between consecutive multiples of $p-1$, a contradiction. □

Remark 2.3. The above proof shows that, if $\gcd(k, p-1) < \sqrt{p - (3/4)} - (1/2)$, then there exists i with $0 < i < p-1$ for which the polynomial $(x^n(x^k + a))^i$ has a unique term of degree divisible by $p-1$, contradicting our hypothesis that $x^n(x^k + a)$ permutes $\mathbb{F}_p$. As discussed in the introduction, we suspect that Theorem 2.1 can be improved substantially. However, improving our bound by more than a constant factor will require a new method: if $\gcd(k, p-1) \geq \sqrt{2p - (7/4)} - (1/2)$, then there is no $i > 0$ for which $(x^n(x^k + a))^i$ has a unique term of degree divisible by $p-1$.

We now list some consequences of Theorem 2.1.

Corollary 2.4. *If $x^n(x^k + a)$ permutes $\mathbb{F}_p$, where $n, k > 0$ and $a \in \mathbb{F}_p^*$, then $\gcd(k, p-1) > 4$.*

Proof. When $p > 19$, this is an immediate consequence of Theorem 2.1. Otherwise, the result can be verified via computer. □

In case either $(p-1)/2$ or $(p-1)/4$ is prime, Corollary 2.4 was conjectured in [15]. We proved this conjecture in our previous paper [16], where moreover we proved that the hypotheses of Corollary 2.4 imply $\gcd(k, p-1) \notin \{2, 4\}$ (without assuming primality of $(p-1)/2$ or $(p-1)/4$). Our proof in [16] did not rely on any computer calculations; instead we used repeated applications of Hermite's criterion in several different cases (depending on the class of p mod 16). By using a computer to verify small cases, we can go much further than Corollary 2.4. For instance:

Corollary 2.5. *Suppose $x^n(x^k + a)$ permutes $\mathbb{F}_p$, where $n, k > 0$ and $a \in \mathbb{F}_p^*$. If $\gcd(k, p-1) = 5$, then $p = 11$. If $\gcd(k, p-1) = 6$, then $p \in \{7, 13, 19, 31\}$. If $\gcd(k, p-1) = 7$, then $p = 29$. If $\gcd(k, p-1) = 8$, then $p = 17$. Conversely, each of these possibilities actually occurs for some n, k, a.*

There is no difficulty extending this to larger values of $\gcd(k, p-1)$.

3. Existence results

In this section we estimate the number of permutation binomials of prescribed shapes.

Theorem 3.1. *Let $n, k > 0$ be integers with $\gcd(n, k, q-1) = 1$, and suppose $q \geq 4$. If $\gcd(k, q-1) > 2q(\log\log q)/\log q$, then there exists $a \in \mathbb{F}_q^*$ such that $x^n(x^k + a)$ permutes $\mathbb{F}_q$. Further, letting T denote the number of $a \in \mathbb{F}_q$ for which $x^n(x^k + a)$ permutes $\mathbb{F}_q$, and writing $r := (q-1)/\gcd(k, q-1)$, we have*

$$\frac{r!}{r^r}\left(q + 1 - \sqrt{q}(r^{r+1} - 2r^r - r^{r-1} + 2) - (r+1)r^{r-1}\right) \leq T$$
$$\leq \frac{r!}{r^r}\left(q + 1 + \sqrt{q}(r^{r+1} - 2r^r - r^{r-1} + 2)\right).$$

Corollary 3.2. *For fixed r, as $q \to \infty$ we have $T \sim q(r!)/r^r$.*

Note that Stirling's approximation says that $r!/r^r$ is asymptotic to $\sqrt{2\pi r}/e^r$ as $r \to \infty$.

We will prove Theorem 3.1 as a consequence of several lemmas, which we suspect will be useful in future work improving the bounds in Theorem 3.1. In these lemmas, μ_r denotes the set of r^{th} roots of unity in $\mathbb{F}_q$, and $\mathrm{Sym}(\mu_r)$ denotes the set of permutations of μ_r.

Lemma 3.3. *Let $k, n > 0$ be integers with $k \mid (q-1)$ and $\gcd(n, k) = 1$, and put $r := (q-1)/k$. For $a \in \mathbb{F}_q$, the polynomial $f(x) := x^n(x^k + a)$ permutes $\mathbb{F}_q$ if and only if there exists $\pi \in \mathrm{Sym}(\mu_r)$ such that every $\zeta \in \mu_r$ satisfies $(\zeta + a)^k = \pi(\zeta)/\zeta^n$.*

Proof. For $\delta \in \mu_k$ we have $f(\delta x) = \delta^n f(x)$; since $\gcd(n, k) = 1$, it follows that the values of f on $\mathbb{F}_q$ comprise all the k^{th} roots of the values of $f(x)^k = x^{kn}(x^k + a)^k$. Thus, f permutes $\mathbb{F}_q$ if and only if $g(x) := x^n(x + a)^k$ permutes the set of k^{th} powers in $\mathbb{F}_q$, or in other words g permutes μ_r. Writing π for the map $\mu_r \to \mathbb{F}_q$ induced by g, the result follows. □

Next we restate Lemma 3.3 in terms of solutions to a system of nonlinear equations over $\mathbb{F}_q$. In this statement, $\nu : \mu_r \to \mathbb{F}_q^*$ is a fixed map with the property that $\nu(\zeta)^k = \zeta$ for every $\zeta \in \mu_r$.

Lemma 3.4. *Let k, n, r be as in Lemma 3.3. For $a \in \mathbb{F}_q$, the polynomial $f(x) := x^n(x^k + a)$ permutes $\mathbb{F}_q$ if and only if there exists $\pi \in \mathrm{Sym}(\mu_r)$ such that, for each $\zeta \in \mu_r$, there is a solution $y_\zeta \in \mathbb{F}_q^*$ to the equation $\zeta + a = y_\zeta^r \nu(\pi(\zeta)/\zeta^n)$. Moreover, for any fixed $a \in \mathbb{F}_q$, there is at most one such permutation π.*

Proof. By Lemma 3.3, f permutes $\mathbb{F}_q$ if and only if there exists $\pi \in \mathrm{Sym}(\mu_r)$ such that $(\zeta + a)^k = \pi(\zeta)/\zeta^n$ for all $\zeta \in \mu_r$. This equation shows that at most one π corresponds to a given f. For fixed π and ζ, the equation is equivalent to the existence of $y_\zeta \in \mathbb{F}_q^*$ such that $\zeta + a = y_\zeta^r \nu(\pi(\zeta)/\zeta^n)$. □

Let A be transcendental over $\mathbb{F}_q$, and for $\pi \in \mathrm{Sym}(\mu_r)$ let $F_\pi = \mathbb{F}_q(\{Y_\zeta : \zeta \in \mu_r\})$ where $Y_\zeta^r \nu(\pi(\zeta)/\zeta^n) = \zeta + A$. We will translate Lemma 3.4 into a statement about F_π, which will enable us to apply Weil's bound on the number of degree-one places of a function field over a finite field. In order to make this translation, we need to know some basic facts about F_π, which we record in the next lemma. In the

remainder of this section we use various standard facts about algebraic function fields, for which a convenient reference is [25].

Lemma 3.5. *Let k, n, r be as in Lemma 3.3. Then $\mathbb{F}_q$ is algebraically closed in F_π, and $F_\pi/\mathbb{F}_q(A)$ is Galois with group $(\mathbb{Z}/r\mathbb{Z})^r$. Moreover, the extension $F_\pi/\mathbb{F}_q(A)$ has ramification index r over $A = \infty$ and $A \in -\mu_r$, and is unramified over all other places of $\mathbb{F}_q(A)$. The genus of F_π is $(r^{r+1} - 2r^r - r^{r-1} + 2)/2$.*

Proof. Let E_ζ be the field $\mathbb{F}_q(Y_\zeta)$. Then $E_\zeta/\mathbb{F}_q(A)$ is a degree-r Kummer extension which is totally ramified over $A = \infty$ and $A = -\zeta$, and unramified over all other places. Since each extension $E_\zeta/\mathbb{F}_q(A)$ is totally ramified over a place which does not ramify in any other $E_{\zeta'}/\mathbb{F}_q(A)$, it follows that the compositum F_π of the various fields E_ζ is a degree-r^r extension of $\mathbb{F}_q(A)$ such that $\mathbb{F}_q$ is algebraically closed in F_π. Moreover, F_π is a Galois extension of $\mathbb{F}_q(A)$ with Galois group $(\mathbb{Z}/r\mathbb{Z})^r$. By Abhyankar's lemma, $F_\pi/\mathbb{F}_q(A)$ has ramification index r over $A = \infty$ and $A \in -\mu_r$, and this extension is unramified over all other places of $\mathbb{F}_q(A)$. Now the Riemann-Hurwitz formula yields the genus of F_π. □

Now we can restate Lemma 3.4 in terms of places of F_π:

Lemma 3.6. *Let k, n, r be as in Lemma 3.3. For $a \in \mathbb{F}_q$, the polynomial $f(x) := x^n(x^k + a)$ permutes $\mathbb{F}_q$ if and only if there exists $\pi \in \mathrm{Sym}(\mu_r)$ such that F_π has a degree-one place with $A = a$ and every $Y_\zeta \neq 0$. Moreover, for any fixed $a \in \mathbb{F}_q$, there is at most one such permutation π.*

Proof of Theorem 3.1. Fix k, n, r. As in the proof of Theorem 2.1, we may assume $k \mid (q-1)$. Pick a permutation $\pi \in \mathrm{Sym}(\mu_r)$ and a map $\nu : \mu_r \to \mathbb{F}_q^*$ such that $\nu(\zeta)^k = \zeta$ for every $\zeta \in \mu_r$. Let N_π denote the number of degree-one places of F_π. Then Weil's bound gives

$$|N_\pi - (q+1)| \le (r^{r+1} - 2r^r - r^{r-1} + 2)\sqrt{q}.$$

The ramified places in $F_\pi/\mathbb{F}_q(A)$ are precisely the places of F_π for which either $A = \infty$ or some $Y_\zeta \in \{0, \infty\}$. The number of such places is at most $(r+1)r^{r-1}$. All other rational places of F_π occur in $\mathrm{Gal}(\mathbb{F}_\pi/\mathbb{F}_q(A))$-orbits of size r^r, with each orbit corresponding to a unique place of $\mathbb{F}_q(A)$. Let T denote the number of values $a \in \mathbb{F}_q$ for which $x^n(x^k + a)$ permutes $\mathbb{F}_q$. By Lemma 3.6 we have

$$r! \frac{q + 1 - (r^{r+1} - 2r^r - r^{r-1} + 2)\sqrt{q} - (r+1)r^{r-1}}{r^r} \le T$$
$$\le r! \frac{q + 1 + (r^{r+1} - 2r^r - r^{r-1} + 2)\sqrt{q}}{r^r}.$$

In particular, $T > 1$ whenever $q > r^{2r+2}$ and $q > 2$. The former inequality is true whenever $q \ge 7$ and $r < (\log q)/(2 \log\log q)$, or equivalently $q \ge 7$ and

$$k > \frac{2(q-1)\log\log q}{\log q}.$$

For $q \in \{4, 5\}$ we have $2q(\log\log q)/\log q > (q-1)/2$, so it remains to show that there are permutation binomials $x^n(x^{q-1} + a)$ (with $a \neq 0$) for every n coprime to $q - 1$. By Lemma 3.3, this binomial permutes $\mathbb{F}_q$ whenever $a \in \mathbb{F}_q^* \setminus \{-1\}$. □

Remark 3.7. In this proof, we treated the various π's independently. This is inefficient, especially since distinct π's give disjoint sets of a's. If one could combine the information from distinct π's more effectively, it might be possible to remove the

$\log\log q$ factor from Theorem 3.1. We now take a first step in this direction (based on an idea in [5]), by effectively combining the information from r distinct π's. To start with, consider any of the $(r-1)!$ permutations $\pi_0 \in \mathrm{Sym}(\mu_r)$ with $\pi_0(1) = 1$. Now the '$\zeta = 1$' equation $(1+a)^k = \pi(1)$ can be used as the definition of $\pi(1)$ (so long as $a \neq -1$), and we seek solutions for each of the $(r-1)!$ permutations $\pi = (1+a)^k \cdot \pi_0$. Thus, for each such π, we pick ν as before and consider the function field defined by $Y_\zeta^r \nu(\pi_0(\zeta)/\zeta^n) = (\zeta + A)/(1 + A)$. By the same method as above, we find that

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

Here, as usual, one can obtain better bounds by applying the various improvements to the Weil bound due to Manin [14], Ihara [11], Drinfel'd-Vlăduţ [7], Serre [22, 23], Oesterlé [23], Stöhr-Voloch [26], etc.

The following variant was noted implicitly in [5] and explicitly in [32]: if q is sufficiently large compared to r and $q \equiv 1 \pmod{r}$, then there exists $a \in \mathbb{F}_q^*$ such that, for every $n, k > 0$ with $\gcd(n, q-1) = 1$ and $\gcd(k, q-1) = (q-1)/r$, the polynomial $x^n(x^k + a)$ permutes $\mathbb{F}_q$. The novel feature here is that a single a works for every n and k; one unfortunate aspect is that we need $\gcd(n, q-1) = 1$, whereas in Theorem 3.1 we required only that $\gcd(n, (q-1)/r) = 1$. The modified proof described in this remark gives a quantitative version of this result, so long as we restrict to π_0 being the identity. Let $\hat{T}$ denote the number of values $a \in \mathbb{F}_q$ such that, for every $n, k > 0$ with $\gcd(n, q-1) = 1$ and $\gcd(k, q-1) = (q-1)/r$, the polynomial $x^n(x^k + a)$ permutes $\mathbb{F}_q$. Our proof in this remark (with $\pi_0(x) = x$) shows that

$$\hat{T} \geq (q - 2\sqrt{q} + 1)/r^{r-1} - \sqrt{q}(r-3) - 2.$$

Remark 3.8. In case $r = 2$, the function field F_π occurring in the proof of Theorem 3.1 has genus zero, and hence can be parametrized. This leads to explicit expressions for the allowable values of 'a' in this case [4, 20, 31]. For larger values r, the field F_π has larger genus, so one does not expect a simple exact formula for its number of rational places. And indeed, already for $r = 3$ the data suggests there is no simple formula for the number of $a \in \mathbb{F}_q$ such that $x(x^{(q-1)/r} + a)$ permutes $\mathbb{F}_q$, or more generally for the number of permutation binomials of degree less than q for which $(q-1)/r$ is the gcd of $q-1$ with the difference between the degrees of the terms. A priori it is conceivable that there might be a nice formula for the latter number but no nice formula for the former, since the latter corresponds to the sum of the numbers of rational places on the various fields F_π; however, the data suggests there are no nice formulas when $r > 2$.

Remark 3.9. Theorem 3.1 is a refinement of a result of Carlitz and Wells [5]. Our version differs from the original one in various ways: it is effective, it gives an estimate on the number of permutation binomials of prescribed shapes, it applies when $\gcd(n, k, q-1) = 1$ rather than $\gcd(n, q-1) = 1$, and the proof is geometric (in contrast to the intricate manipulation of character sums in [5]). Still, we emphasize that the key idea of using the Weil bound to prove existence of permutation binomials is due to Carlitz [4].

4. Heuristic

In this section we give a heuristic suggesting that 'at random' there would not be any permutation binomials $x^m + ax^n$ over $\mathbb{F}_q$ (with $m > n > 0$) such that $\gcd(m-n, q-1) < q/(2\log q)$, at least for q sufficiently large.

As in the proof of Theorem 2.1, it suffices to consider $f(x) := x^n(x^k + a)$ where $k \mid (q-1)$ and n is coprime to k. By Lemma 3.3, for fixed k, we need only consider a single such value n in each class modulo $(q-1)/k$ which contains integers coprime to k. Further, since composing $f(x)$ on both sides with scalar multiples does not affect whether $f(x)$ permutes $\mathbb{F}_q$, we need only consider a's representing the distinct cosets of the k^{th} powers in $\mathbb{F}_q^*$ (for fixed k and n). Thus, for fixed k, there are fewer than q polynomials to consider. Since $\gcd(n,k) = 1$, the values of f comprise all the k^{th} roots of the values of f^k; but the latter are just 0 and the values of $x^n(x+a)^k$ on $(\mathbb{F}_q^*)^k$. Thus, f permutes $\mathbb{F}_q$ if and only if $g(x) := x^n(x+a)^k$ permutes $(\mathbb{F}_q^*)^k$. Note that $(\mathbb{F}_q^*)^k$ equals the group μ_r of r^{th} roots of unity in $\mathbb{F}_q^*$, where $r := (q-1)/k$. Here g maps μ_r into μ_r if and only if $(-a)^r \neq 1$, which we assume in what follows. Now, the probability that a random mapping $\mu_r \to \mu_r$ is bijective is $r!/r^r$. Assuming that g behaves like a random map, the expected number of permutation binomials of the form $x^n(x^k + a)$ (for fixed q, after our various equivalences on n, k, a) is at most $q(r!)/r^r$. Restricting to $k < q/(2\log q)$ and summing over all q, we get an expected number

$$E := \sum_q \sum_{\substack{r \mid (q-1) \\ r > 2\log q}} q\frac{r!}{r^r}.$$

We now show that E is finite. By reversing the order of summation, we find that $E = \sum_{r=1}^{\infty}(r!/r^r)F(r)$, where

$$F(r) := \sum_{\substack{q < e^{r/2} \\ q \equiv 1 \pmod r \\ q \text{ prime power}}} q.$$

The number of prime powers less than x which are not prime is at most

$$\sum_{n=2}^{\lfloor \log_2 x \rfloor} x^{1/n} < \sqrt{x} + \sqrt[3]{x}\log_2 x.$$

Thus, for fixed r, the number of nonprime q which contribute to $F(r)$ is at most $e^{r/4} + e^{r/6}r/(2\log 2)$. By the Brun–Titchmarsh theorem [9, Thm. 3.8], the number of prime q which contribute to $F(r)$ is at most

$$\frac{3e^{r/2}}{\phi(r)\log\frac{e^{r/2}}{r}}.$$

Since

$$\phi(r) > \frac{r}{e^\gamma \log\log r + \frac{3}{\log\log r}}$$

for $r \geq 3$ ([21, Thm. 15]), for $r \geq 3$ we have

$$\frac{F(r)}{e^r} \leq \frac{3(e^\gamma \log\log r + \frac{3}{\log\log r})}{r(\frac{r}{2} - \log r)} + \frac{1}{e^{r/4}} + \frac{r}{2e^{r/3}\log 2}.$$

Using Stirling's inequality $r! < (r/e)^r\sqrt{2\pi r}e^{1/12r}$, we get

$$E \le \sum_{r=3}^{\infty} \sqrt{2\pi r}e^{\frac{1}{12r}} \left(\frac{3e^\gamma \log\log r + \frac{9}{\log\log r}}{r(\frac{r}{2} - \log r)} + \frac{1}{e^{r/4}} + \frac{r}{2e^{r/3}\log 2} \right),$$

which is finite. By combining the above bounds on $F(r)$ with explicit calculation of the first few values of $F(r)$, we find that $E < 40$.

Since E is finite (and small), we expect that 'at random' there would be few (or no) permutation binomials $x^m + ax^n$ over $\mathbb{F}_q$ with $m > n > 0$ and $\gcd(m-n, q-1) < q/(2\log q)$.

We used a computer to verify that, for $p < 10^5$, there are no permutation binomials $x^m + ax^n$ over $\mathbb{F}_p$ with $m > n > 0$ and $\gcd(m-n, p-1) < p/(2\log p)$. Combined with the above heuristic, this leads us to conjecture that the same conclusion holds for all primes p.

On the other hand, the heuristic applies to nonprime fields as well, and for those fields we know some infinite families of counterexamples. For instance, in [27], Tom Tucker and the second author showed that $x^{p+2} + ax$ permutes $\mathbb{F}_{p^2}$ whenever $\#\langle a^{p-1}\rangle = 6$. Several additional examples can be found in [27], and we will present further examples in a forthcoming paper. However, every known counterexample over a nonprime field $\mathbb{F}_q$ has unusual properties related to the subfields of $\mathbb{F}_q$; thus, we view these examples as violating the randomness hypotheses of our heuristic, rather than the heuristic itself.

Appendix

In this appendix we prove the following result:

Theorem 1.2. *If $x^m + ax^n$ permutes the prime field $\mathbb{F}_p$, where $m > n > 0$ and $a \in \mathbb{F}_p^*$, then $p - 1 \le (m-1) \cdot \max(n, \gcd(m-n, p-1))$.*

As noted in the introduction, this result follows from Theorem 1.3 in all cases except when $n = 1$ and $(m-1) \mid (p-1)$. However, the proof we present here is quite different from the proof of Theorem 1.3, so the method might well be useful in other investigations. Theorem 1.2 may be viewed as the 'least common generalization' of a result of Wan and a result of Turnwald. Our proof uses ideas from both of their proofs. Wan's result [30, Thm. 1.3] is

Theorem. *If $x^m + ax$ permutes the prime field $\mathbb{F}_p$, where $m > 1$ and $a \in \mathbb{F}_p^*$, then $p - 1 \le (m-1) \cdot \gcd(m-1, p-1)$.*

Turnwald's result [28, Thm. 2] is

Theorem. *If $x^m + ax^n$ permutes $\mathbb{F}_p$, where $m > n > 0$ and $a \in \mathbb{F}_p^*$, then $p < m \cdot \max(n, m-n)$.*

Proof of Theorem 1.2. Suppose $f(x) := x^m + ax^n$ permutes $\mathbb{F}_p$, where $m > n > 0$ and $a \in \mathbb{F}_p^*$. If $f(x) = \hat{f}(x^e)$, then the desired inequality for f would follow from the corresponding inequality for $\hat{f}$; thus, we may assume $\gcd(m, n) = 1$. Moreover, since f permutes $\mathbb{F}_p$ we have $\gcd(m-n, p-1) > 1$ (since otherwise f has more than one root), so $n \le m-2$ and $m \ge 3$. Write $p = mk + r$ with $0 \le r < m$. Since $\gcd(n, m-n) = 1$, there are integers u, v with $nu - (m-n)v = r - 1$; we may assume $0 < u \le m - n$. Thus

$$v = (nu - r + 1)/(m-n) \le n + 1/(m-n) < n + 1,$$

so $v \le n$. Also $v > (n-m+1)/(m-n) > -1$, so $v \ge 0$.

If $v > k$, then (since $k = \lfloor p/m \rfloor$) we have $p < mv \le mn$, so the result holds. Henceforth we assume $v \le k$. Moreover, since $\gcd(m-n, p-1) \ge 2$, the result is clear when $m > p/2$; thus, we assume $m \le p/2$. Since $3 \le m$, this implies $p \ge 7$ and $m < p-3$.

We will use Hermite's criterion with exponent $k+u$. Before doing so, we show that $0 < k+u < p-1$. The first inequality is clear, since $u > 0$ and $k = \lfloor p/m \rfloor \ge 0$. Now,

$$k+u = \left\lfloor \frac{p}{m} \right\rfloor + u \le \frac{p}{m} + u \le \frac{p}{m} + m - n \le \frac{p}{m} + m - 1.$$

Since $p > m+3$ (and $m \ge 3$), we have $p > m^2/(m-1)$, so $m < p(m-1)/m$ and thus $p/m + m < p$. Hence $k+u < p-1$.

Since $0 < k+u < p-1$, we have $p \nmid \binom{k+u}{t}$ for $0 \le t \le k+u$; hence the degrees of the terms of f^{k+u} are precisely the numbers $mt + n(k+u-t)$ with $0 \le t \le k+u$. Since

$$p-1 = mk + (r-1) = mk + nu - (m-n)v = m(k-v) + n(u+v),$$

there is a term of degree $p-1$. Since f is a permutation polynomial, Hermite's criterion implies there must be another term of degree divisible by $p-1$. Thus, there exists $A \ne k-v$ with $0 \le A \le k+u$ such that $mA + n(k+u-A) \equiv 0 \bmod (p-1)$. Since increasing t will increase the value of $mt + n(k+u-t)$, and the value of this quantity for $t = A$ is larger than the corresponding value for $t = k-v$, it follows that $A > k-v$. Subtracting, we get $m(A-(k-v)) + n(k-A-v) \equiv 0 \bmod (p-1)$, so $p-1$ divides $(m-n)(A-(k-v))$. In other words, $(p-1)/\gcd(p-1, m-n)$ divides $A-(k-v)$. Since $A > k-v$, this implies

$$\frac{p-1}{\gcd(p-1, m-n)} \le A-(k-v) \le (k+u)-(k-v) = u+v.$$

Since $u \le m-n$ and $v \le n$, we have $u+v \le m$; however, equality cannot hold, since it would imply that $r-1 = nu-(m-n)v = 0$ so $r = 1$, whence $p-1 = p-r = mk$, which is a contradiction since $m > 1$ is the degree of a permutation polynomial. Thus $u+v \le m-1$, so $p-1 \le (m-1)\cdot\gcd(p-1, m-n)$. □

References

[1] E. Betti, *Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo*, Ann. Sci. Mat. Fis. **2** 1851, 5–19. (= Opere Matematiche, v. 1, 17–27)

[2] F. Brioschi, *Des substitutions de la forme* $\Theta(r) \equiv \varepsilon(r^{n-2} + ar^{(n-3)/2})$ *pour un nombre n premier de lettres*, Math. Ann. **2** 1870, 467–470. (= Opere Matematiche, v. 5, 193–197) MR1509672

[3] F. Brioschi, *Sur les fonctions de sept lettres*, C. R. Acad. Sci. Paris **95** 1882, 665–669. (= Opere Matematiche, v. 5, 31–39)

[4] L. Carlitz, *Some theorems on permutation polynomials*, Bull. Amer. Math. Soc. **68** 1962, 120–122. MR0141655 (25:5052)

[5] L. Carlitz and C. Wells, *The number of solutions of a special system of equations in a finite field*, Acta Arith. **12** 1966–1967, 77–84. MR0204417 (34:4259)

[6] L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. of Math. **11** 1896–1897, 65–120. MR1502214

[7] V. G. Drinfel'd and S. G. Vlăduţ, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17** 1983, 68–69. (= Funct. Anal. Appl. **17** 1983, 53–54) MR0695100 (85b:14028)

[8] S. El Baghdadi, *Sur un problème de L. Carlitz*, Acta Arith. **69** 1995, 39–50. MR1310841 (95m:11140)

[9] H. Halberstam and H.-E. Richert, Sieve Methods, Academic Press, London, 1974. MR0424730 (54:12689)
[10] Ch. Hermite, *Sur les fonctions de sept lettres*, C. R. Acad. Sci. Paris **57** 1863, 750–757.
[11] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo **28** 1981, 721–724. MR0656048 (84c:14016)
[12] N. M. Korobov, *An estimate of the sum of the Legendre symbols*, Dokl. Akad. Nauk SSSR **196** 1971, 764–767. (= Soviet Math. Dokl. **12** 1971, 241–245) MR0274455 (43:220)
[13] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory*, Finite Fields Appl. **13** 2007, 58–70. MR2284666 (2008c:94027)
[14] Y. I. Manin, *What is the maximum number of points on a curve over* $\mathbb{F}_2$?, J. Fac. Sci. Univ. Tokyo **28** 1981, 715–720. MR0656047 (84c:14015)
[15] A. Masuda, D. Panario, and Q. Wang, *The number of permutation binomials over* $\mathbb{F}_{4p+1}$ *where* p *and* $4p+1$ *are primes*, Electron. J. Combin. **13** 2006, R65. MR2240771 (2007c:11138)
[16] A. M. Masuda and M. E. Zieve, *Nonexistence of permutation binomials of certain shapes*, Electron. J. Combin. **14** 2007, N12. MR2320592 (2008c:11162)
[17] 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.
[18] D. A. Mit'kin, *Estimation of the sum of the Legendre symbols of polynomials of even degree*, Mat. Zametki **14** 1973, 73–81. (= Math. Notes **14** 1973, 597–602) MR0332794 (48:11120)
[19] D. A. Mit'kin, *Existence of rational points on a hyperelliptic curves over a finite prime field*, Vestnik Moskov. Univ. Ser. I Mat. Meh. **30** 1975, 86–90. (= Moscow Univ. Math. Bull. **30** 1975, 124–127) MR0401644 (53:5471)
[20] H. Niederreiter and K. H. Robinson, *Complete mappings of finite fields*, J. Austral. Math. Soc. (Series A) **33** 1982, 197–212. MR0668442 (83j:12015)
[21] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** 1962, 64–94. MR0137689 (25:1139)
[22] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. **296** 1983, 397–402. (= Œuvres [128]) MR0703906 (85b:14027)
[23] J.-P. Serre, *Rational points on curves over finite fields*, unpublished lecture notes by F. Q. Gouvêa, Harvard University, 1985.
[24] H. M. Stark, *On the Riemann hypothesis in hyperelliptic function fields*, in: Analytic Number Theory, Proc. Sympos. Pure Math. 24, 285–302, Amer. Math. Soc., Providence, 1973. MR0332793 (48:11119)
[25] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, Berlin, 1993. MR1251961 (94k:14016)
[26] K.-O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52** 1986, 1–19. MR0812443 (87b:14010)
[27] T. J. Tucker and M. E. Zieve, *Permutation polynomials, curves without points, and Latin squares*, preprint, 2000.
[28] G. Turnwald, *Permutation polynomials of binomial type*, in: Contributions to General Algebra 6, 281–286, Hölder-Pichler-Tempsky, Vienna, 1988. MR1078048 (92e:11141)
[29] J. F. Voloch, *On the number of values taken by a polynomial over a finite field*, Acta Arith. **52** 1989, 197–201. MR1005605 (90j:11138)
[30] D. Wan, *Permutation polynomials over finite fields*, Acta Math. Sinica (N.S.) **3** 1987, 1–5. MR0915843 (89b:11100)
[31] D. Wan, *Permutation binomials over finite fields*, Acta Math. Sinica (N.S.) **10** 1994, 30–35. MR1268257 (94m:11145)
[32] 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. MR1126814 (92g:11119)
[33] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Actualités Sci. Ind., no. 1041, Publ. Inst. Math. Univ. Strasbourg **7**, Hermann, Paris, 1948. MR0027151 (10:262c)
[34] U. Zannier, *Polynomials modulo p whose values are squares (elementary improvements on some consequences of Weil's bounds)*, Enseign. Math. (2) **44** 1998, 95–102. MR1643282 (99j:11072)

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, Canada K1S 5B6
Current address: Department of Mathematics and Statistics, University of Ottawa, 585 King Edward Avenue, Ottawa, Ontario, Canada K1N 6N5
E-mail address: amasuda@uottawa.ca

Center for Communications Research, 805 Bunn Drive, Princeton, New Jersey 08540
E-mail address: zieve@math.rutgers.edu
URL: www.math.rutgers.edu/∼zieve/