# THE CARLITZ-LENSTRA-WAN CONJECTURE ON EXPECTIONAL POLYNOMIALS: AN ELEMENTARY VERSION

STEPHEN D. COHEN AND MICHAEL D. FRIED

Abstract. We give a proof, following an argument of H.W. Lenstra, of the conjecture of L. Carlitz (1966) as generalized by D. Wan (1993).

This says, there are no exceptional polynomials of degree $n$ over $\mathbb{F}_q$ if $(n, q-1) > 1$. Fried, Guralnick and Saxl proved a much stronger result, showing that primitive exceptional polynomials have monodromy groups with degrees either a power of the characteristic (and the monodromy group is affine), or they are cyclic, dihedral (from Tchebychev polynomials) or when the characteristic is $p = 2$ or 3 the monodromy group is $\mathrm{PSL}_2(p^a)$ with $a$ odd. In the original paper we didn't realize the community wouldn't recognize that the elementary Lenstra-Wan statement follows from [FGS93] – which was written before that statement was formulated. From [FGS93] – generalizing results from the proof of the Schur conjecture – a brief argument concludes the Wan conjecture by giving a strong characterization of the values of $q$ for which an indecomposable polynomial of degree $n$ (not a power of $p$) can be exceptional over $\mathbb{F}_q$. By contrast, the Lenstra-Wan statement captures little of the content of [FGS93].

## 1. Introduction

Exceptional polynomials over finite fields have a special place in coding theory and cryptography. In particular, the Carlitz conjecture (recently generalized by Wan) gives important information on the degrees of exceptional polynomials over a given finite field. See [**1**], [**2**] and [**3**] for a survey of exceptional polynomials, the known classes and a history of the work on the Carlitz conjecture. A proof of the Carlitz conjecture in [**3**] used the classification of finite simple groups. This was to deduce results on the primitive groups arising in a Galois theoretic translation of the problem. Excluding cyclic and Chebychev polynomials, and $p = 2$ and 3, this proved all exceptional indecomposable polynomials over $\mathbb{F}_q$ have degrees a power of the characteristic. Excluding $p = 2$ and 3, this is a proof of Wan's conjecture. The simple proof of Wan's conjecture in this note removes all group theory.

Let $k = \mathbb{F}_q$ be the finite field of order $q$, a power of its characteristic $p$. A separable polynomial $f[X]$ in $k[X]$ is one for which $f \neq f_1^p$. We assume all polynomials are separable. Then, $f$ of degree greater than 1 is *exceptional* over $k$ if it permutes (as a function) infinitely many finite extensions of $k$. We use an equivalent definition in this note: the two-variable polynomial $(f(X) - f(Y))/(X - Y)$ has no absolutely irreducible factors in $k[X, Y]$. That is, any irreducible factor in $k[X, Y]$ factors further in $k'[X, Y]$ for some finite extension $k' = \mathbb{F}_{q^s}, s > 1$. In 1966, L. Carlitz made a conjecture equivalent to this: there is no exceptional polynomial of even degree over $\mathbb{F}_q$, $q$ odd. In 1993, D. Wan stated a stronger conjecture [**4**]). H.W. Lenstra recently proved this.

**Theorem 1.1** (H.W. Lenstra)**.** *Suppose $(n, q-1) > 1$. Then there is no exceptional polyomial of degree $n$ over $\mathbb{F}_q$.*

If $p \nmid n$, the proof is easy. The full result, however, seemed hard. All approaches use a criterion for exceptionality involving the Galois group $G$ of $f(X) - z$ ($z$ an indeterminate) over $k(z)$. Here regard $G$ as a transitive permutation group on its roots. A simple reduction to the case in which $f$ is functionally indecomposable allows us to assume $G$ is primitive. An analysis along such lines led to the proof of the Carlitz conjecture in [**3**]. Actually, [**3**] shows $G$ must be an affine group unless $p = 2$ or 3. This note does not replicate the last result, which opened the possibility for a complete classification of exceptional polynomials.

Lenstra's proof of Wan's conjecture made a more detailed use of the ramification groups at infinity of the polynomial $f(X)-z$ over $k(z)$ than did [**3**]. Neither primitive group theory, nor the classification of finite simple groups appear in this proof. Lenstra's argument inspired us to reconstruct a proof using general exceptional covers [**2**]. This led to the more elementary account given here. We are grateful to Lenstra for communicating his argument to us. He may incorporate a proof, illuminating the underlying concepts, in a further article of his own.

## 2. A Galois-theoretic criterion

Let $f$ be an exceptional polynomial of degree $n(>1)$ over $k = \mathbb{F}_q$. We may suppose $f$ is monic and, replacing $f(X)$ by $f(X) - f(0)$, that $f(0) = 0$. It is convenient to work with the rational function $f(1/X) \in k(X)$ and its reciprocal $1/f(1/X) = X^n/g(X)$. Here $g(X)$ is the *polynomial* $X^n f(1/X)$. Note: $\deg g \leq n-1$ (since $f(0) = 0$) and $g(0) = 1$ (since $f$ is monic). Obviously, $f(1/X)$ is an "exceptional function" over $k$ in that

$$\phi(X,Y) = \frac{X^n g(Y) - Y^n g(X)}{X - Y} \in k[X,Y]$$

has no absolutely irreducible factors over $k$. Let $k' = \mathbb{F}_{q^s}$ ($s > 1$) be the minimal extension of $k$ such that every irreducible factor of $\phi$ in $k[X,Y]$ splits into more than one factor in $k'[X,Y]$. The parameter $[k' : k] = s$ is important for the sequel.

Let $z$ be an indeterminate. Next, let $F(X) = X^n - zg(X)$: $F$ is a monic irreducible polynomial of degree $n$ in $X$ with coefficients in $k[z]$. A key step considers $F$ to be a polynomial in $X$ over $k\{z\}$, the field of formal power series (Laurent series) in $z$ over $k$. Then $F$ is an Eisenstein polynomial with respect to the unique valuations of $k\{z\}$ and $k'\{z\}$. Hence, $F(X)$ is an irreducible polynomial of degree $n$ over $k\{z\}$ and over $k'\{z\}$. Moreover, if $Y$ is a root of $F$ in a splitting field $L$ over $k\{z\}$, then $k\{z\}(Y)$ is simply the formal power series field $k\{Y\}$. Similarly, $k'\{z\}(Y) = k'\{Y\}$, a subfield of $L$ (since $k' \subseteq L$ from the definition of $k'$).

Now define $G(= \mathrm{Gal}(L/k\{z\})$ to be the Galois group of $F$ over $k\{z\}$. Regard it as a (transitive) permutation group on its roots. Let $G^*$ to be the subset of $G$ comprising those automorphisms whose restrictions to $k'$ generate $\mathrm{Gal}(k'/k)$, a cyclic group of order $s$. Then $G^*$ has cardinality $(\phi(s)/s)|G|$. Standard arguments in [1, Theorem 4.2], [3, "Exceptionality Lemma"] yield the following implication of exceptionality.

**Lemma 2.1.** *Every member of $G^*$ (as above) fixes precisely one root of $F$.*

*Proof.* Let $\phi(s)$ be the number of cosets of $\mathbb{Z}/s$ relatively prime to s. Any irreducible factor $\phi_1(X,Y)$ of $\phi(X,Y)$in $k[X,Y]$, as a polynomial in $X$ with coefficients in $k[Y]$, splits into several conjugate factors over $k'[Y]$. Thus, although $\phi_1$ may factor further over $k\{Y\}$, each of these factors must decompose further into conjugate factors over $k'\{Y\}$. Therefore, any $\tau \in G^* \cap \mathrm{Gal}(L/k\{Y\})$, (with $Y$ a root of $F$) fixes no factor of $\phi$ over $k'\{Y\}$. In particular, $\tau$ fixes no root of $F$ other than $Y$. That is, every member of $G^*$ that fixes a root of $F$ fixes no other root. We draw a conclusion on the union of the $n$ sets of cardinality $(\phi(s)/sn)|G|$ obtained by intersecting $G^*$ with the one-point stabilizers of $G$. This is a *disjoint* union of cardinality $(\phi(s)/s)|G| = |G^*|$. Therefore $G^*$ is this union and the proof is complete.

## 3. Proof of theorem

Besides the assumption of Section 2, now suppose $(n, q-1) > 1$ and $r$ is a prime divisor of $(n, q-1)$. Write $n = rm$.

Regard $g(Y) = 1 + c_1 Y + \cdots + c_{n-1} Y^{n-1}$ $(c_1, \ldots, c_{n-1} \in k)$ as a member of $k\{Y\}$. There is a (unique) formal power series $h(Y) = 1 + b_1 Y + b_2 Y^2 + \ldots \in k\{Y\}$ with $h^r(Y) = 1/g(Y)$. Thus $b_1 = -c_1/r, b_2 = (a/r^2) - (c_2/r)$, etc., where $a = (r+1)/2$. (Interpret $a$ as a member of $\mathbb{F}_2$ when $p = 2$ and $r$ is odd.)

With $Y$ again a root of $F$ (in $L$), put $Z = Y^m h(Y) \in k\{Y\}$. Then $Z^r = z$ and, $k\{z\}(Z) = k\{Z\}$ is an extension of $k\{z\}$ of degree $r$. Moreover, since $r$ divides $q-1$, $k$ contains all $r$th roots of unity. So $k\{Z\}/k\{z\}$ is a cyclic Galois extension of degree $r$ contained in $k\{Y\}$. Similarly, $k'\{Z\}/k'\{z\}$ is a cyclic extension of degree $r$ contained in $k'\{Y\}$. It follows that $F(X)$ splits over $k\{Z\}$ or $k'\{Z\}$ as a product of $r$ irreducible polynomials $P_1(X), \ldots, P_r(X)$ of degree $m$ in $X$. For $i = 1, \ldots, r$, let $S_i$ denote the set of roots (in $L$) of $P_i$.

Let $\tau \in \mathrm{Gal}(L/k'\{z\})$ have its restriction to $k'\{Z\}$ generate $\mathrm{Gal}(k'\{Z\}/k'\{z\})$. Then, $\tau$ cyclically permutes the sets $S_1, \ldots, S_r$, but it acts trivially on $k'$. Further, let restriction of $\sigma \in \mathrm{Gal}(L/k\{Z\})$ to $k'$ be a generator of $\mathrm{Gal}(k'/k)$: $\sigma \in G^*$. Then $\sigma$ fixes the coefficients of each of $P_1, \ldots, P_r$. Thus, it fixes each set $S_1, \ldots, S_r$. Finally, set $\rho = \sigma\tau \in G$. Then $\rho \in G^*$ since $\sigma \in G^*$ and $\tau$ acts trivially on $k'$. On the other hand, $\rho$ permutes $S_1, \ldots, S_r$ cyclically since $\tau$ does and $\sigma$ fixes each of these sets. This implies $\tau$ is a member of $G^*$ that fixes no root of $F$, in contradiction to the Lemma.

## References

[CM95] S.D. Cohen and R.W. Matthews, Exceptional polynomials over finite fields, *Finite Fields and Their Applications*, to appear.

[Fr94] M. Fried, Global construction of general exceptional covers, *Contemp. Math.* **168** (1994), 69–100.

[FGS93] M.D. Fried, R. Guralnick and J. Saxl, Schur covers and Carlitz's conjecture, *Israel J. Math.* **82** (1993), 157–225.

[W93] D. Wan, A generalization of the Carlitz conjecture, *Finite Fields, Coding Theory and Advances in Communications and Computing, Lecture Notes in Pure and Applied Math.*, Dekker, **141** (1993), 431–432.

Dept. of Mathematics, University of Glasgow,, *Glasgow G12 8QW, Scotland*
*E-mail address*: sdc@maths.gla.ac.uk

Dept. of Mathematics, University of California,, *Irvine, California 92717, USA*
*E-mail address*: mfried@math.uci.edu