

A Sharp Obstruction to Uniform Low-Degree Tails over Finite Fields

Alper Ferudun*

4 October 2026

Abstract

For a prime power q and integers $m \geq n \geq 2$, let $D_q(n, m)$ be the least degree bound on a polynomial $g \in \mathbb{F}_q[X]$ for which $X^m + g(X)$ has an irreducible factor of degree n . We give the elementary sharp identity $\max_{m \geq n} D_q(n, m) = n - 1$: equality holds whenever $m \equiv -1 \pmod{q^n - 1}$. More generally, the residue $m \equiv -j$ forces $D_q(n, m) \geq n - j$ for $1 \leq j < n$. In particular, over $\mathbb{F}_2$, no tail of degree at most 6 makes $X^{254} + g(X)$ have an irreducible factor of degree 8. This disproves the unrestricted-exponent formulation of Question 7 in the AIM algorithmic number theory workshop list. It does not settle Gao's original conjecture, where the exponent is the least power of q at least n , or the separate sparse-polynomial variants.

1 The unrestricted question

Question 7 of the AIM workshop list [1, p. 27] asks for a tail $g \in \mathbb{F}_q[X]$ with $\deg g \leq 2 \log n$ such that $X^m + g(X)$ has an irreducible factor of degree n , for arbitrary integers $m \geq n$. The logarithm base is unspecified. Our obstruction is independent of that ambiguity: no sublinear bound in n can hold uniformly over all $m \geq n$ for a fixed q .

For $m \geq n \geq 2$, define $D_q(n, m)$ to be the least nonnegative integer L with the required property when $\deg g \leq L$. A degree- n irreducible always exists over $\mathbb{F}_q$. Reducing X^m modulo any such polynomial and negating the remainder shows that

$$0 \leq D_q(n, m) \leq n - 1. \quad (1)$$

In this construction $X^m + g$ is nonzero, because $m \geq n > \deg g$.

Theorem 1. *Let q be a prime power and $m \geq n \geq 2$. If $m \equiv -j \pmod{q^n - 1}$ for an integer $1 \leq j < n$, then*

$$D_q(n, m) \geq n - j.$$

In particular,

$$D_q(n, m) = n - 1 \quad \text{if } m \equiv -1 \pmod{q^n - 1}, \quad \max_{m \geq n} D_q(n, m) = n - 1.$$

Proof. Suppose a monic irreducible F of degree n divides $X^m + g(X)$, and let α be a root of F in $\mathbb{F}_{q^n}$. Since $n \geq 2$, $\alpha \neq 0$, and hence $\alpha^{q^n - 1} = 1$. The congruence for m gives

$$\alpha^{-j} + g(\alpha) = 0, \quad 1 + \alpha^j g(\alpha) = 0.$$

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: [AlperTheKing](https://github.com/AlperTheKing).

Thus F divides $1 + X^j g(X)$. This polynomial is nonzero because its constant term is 1. It follows that $j + \deg g \geq n$, proving the lower bound. The case $g = 0$ is impossible in the same equation.

For $j = 1$, combine the lower bound with (1). Finally, $m = q^n - 2$ lies in the required residue class and satisfies $m \geq n$, since $q^n \geq 2^n \geq n + 2$ for $n \geq 2$. $\square$

For completeness, the successful tails at the sharp bound have a particularly simple description.

Proposition 2. *If $m \geq n \geq 2$ and $m \equiv -1 \pmod{q^n - 1}$, the tails g of degree at most $n - 1$ which work are exactly*

$$g(X) = \frac{F(X)/F(0) - 1}{X},$$

where F runs through the monic irreducibles of degree n over $\mathbb{F}_q$. Each such g has degree $n - 1$ and corresponds to exactly one F .

Proof. The argument above shows that $F \mid 1 + Xg$. The nonzero polynomial $1 + Xg$ has degree at most n , so it equals cF for a nonzero scalar c . Comparing constant terms gives $c = 1/F(0)$ and the formula. Conversely, the formula is polynomial because its numerator vanishes at 0, and for any root α of F it gives $g(\alpha) = -\alpha^{-1} = -\alpha^m$. Thus $F \mid X^m + g$. Normalizing $1 + Xg$ to be monic recovers F , proving uniqueness. $\square$

Corollary 3. *Over $\mathbb{F}_2$, no polynomial g of degree at most 6 makes $X^{254} + g(X)$ have an irreducible factor of degree 8.*

Proof. Use $254 \equiv -1 \pmod{2^8 - 1}$ in Theorem 1. Equivalently, a putative degree-eight factor would divide $1 + Xg$, a nonzero polynomial of degree at most seven. $\square$

Here $2 \log_2 8 = 6$, so the example applies to base two, to base $q = 2$, to the natural logarithm and to base ten, even if the bound is rounded upwards. For any fixed base $b > 1$, choose n large enough that $\lceil 2 \log_b n \rceil < n - 1$ and use $m = q^n - 2$. More generally any proposed uniform bound $L(n) = o(n)$ fails for all sufficiently large n .

2 Exact finite checks

The proof does not depend on computation. The accompanying source archive nevertheless includes two exact arithmetic implementations. A bit-polynomial program enumerates the thirty monic degree-eight irreducibles over $\mathbb{F}_2$, using both the Frobenius criterion and exhaustive trial division. It tests all 128 tails of degree at most six against all thirty factors, giving 3,840 nondivisibility checks. It also computes the gcd of each $X^{254} + g$ with

$$H_8(X) = \frac{X^{256} - X}{X^{16} - X},$$

the product of the degree-eight monic irreducibles. All 128 gcds are 1. A separately implemented SymPy program repeats the enumeration, divisibility and gcd checks in dense polynomial arithmetic.

For the sharp degree-seven boundary, take

$$F = X^8 + X^4 + X^3 + X + 1, \quad g = X^7 + X^3 + X^2 + 1.$$

Then $Xg + 1 = F$, so Proposition 2 applies. One can check F 's irreducibility directly: modulo F , $X^{256} \equiv X$ and $X^{16} - X \equiv R := X^6 + X^4 + X^3 + X^2$, while

$$(X^4 + X + 1)F + (X^6 + X^4 + 1)R = 1.$$

These are the Frobenius irreducibility conditions for degree eight. The bit implementation further checks every degree- n irreducible for $2 \leq n \leq 12$ at each negative residue $-j$, $1 \leq j < n$. The second implementation tests additional complete small-degree domains over $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_7$. These bounded checks are regression evidence, not a substitute for Theorem 1.

3 What the obstruction does not settle

Gao’s original Conjecture 1.3 [2] fixes the exponent $\bar{n} = q^{\lceil \log_q n \rceil}$. The same restriction is explicit in Popovych’s discussion [3, pp. 296–297], and Young’s rational-function extension also uses $\bar{n}$ [4, Conjecture 4.2]. Our exponent 254 for $(q, n) = (2, 8)$ is neither that exponent nor a power of two. The argument therefore does not refute those conjectures. It also does not decide the $m = n$ question, the large- q regime with m, n fixed, or the separate AIM remarks on sparse polynomials of degree at most $2n$ with a primitive factor.

The contribution of this note is the explicit correction of the unrestricted-exponent statement and its sharp uniform degree threshold. The finite-field facts and polynomial-division argument are elementary and are not claimed as new machinery. A targeted primary-literature search did not locate this particular correction; absolute priority is not claimed. This unrefereed note was developed with AI assistance in derivation, source checking, exact computation and drafting. No independent specialist review or proof-assistant verification is claimed.

References

- [1] American Institute of Mathematics, *Future directions in algorithmic number theory*, workshop problem list, Question 7, p. 27. <https://aimath.org/WWN/primesinp/primesinp.pdf>. Accessed 4 October 2026.
- [2] S. Gao, Elements of provable high orders in finite fields, *Proc. Amer. Math. Soc.* **127** (1999), 1615–1623. doi:10.1090/S0002-9939-99-04795-4.
- [3] R. Popovych, On elements of high order in general finite fields, *Algebra Discrete Math.* **18** (2014), no. 2, 295–300. <https://admjournal.luguniv.edu.ua/index.php/adm/article/view/1062>.
- [4] M. Young, On multiplicative independence of rational function iterates, *Monatsh. Math.* **192** (2020), 225–247. doi:10.1007/s00605-020-01393-9.