On polynomials free of binomials over $\mathbb{F}_q$

Conference on Rings and Polynomials

TU Graz, Graz, Austria

Sávio Ribas*

Joint work with F.E. Brochero Martínez and L. Reis

*Partially supported by FAPEMIG (grant APQ-01712-23)

Universidade Federal de Ouro Preto, Brazil

July 14–19, 2025

Contents

Primitive elements

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime p.

The group $\mathbb{F}_q^*$ is cyclic and any of its generators is called *primitive element*.

Primitive elements are widely used in coding theory, cryptography, and pseudorandom generation because they simplify multiplication to modular addition of exponents.

Normal elements

For $n \in \mathbb{N}$, let $\mathbb{F}_{q^n}$ be the unique n-degree extension of $\mathbb{F}_q$.

$\mathbb{F}_{q^n}$ can also be viewed as a $\mathbb{F}_q$-vector space of dimension n.

If it admits a $\mathbb{F}_q$-basis of the form $\{\beta, \beta^q, \ldots, \beta^{q^{n-1}}\}$ for some $\beta \in \mathbb{F}_{q^n}$, β is called *normal element* over $\mathbb{F}_q$.

Proposition

$\beta \in \mathbb{F}_{q^n}$ *is normal* $\iff$

$$\gcd\left(\beta x^{n-1} + \beta^q x^{n-2} + \cdots + \beta^{q^{n-2}} x + \beta^{q^{n-1}},\ x^n - 1\right) = 1.$$

Normal elements have several applications, since they simplify computation of powers and other field operations through simple linear transformations.

Primitive Normal Basis Theorem

Primitive normal elements combine the benefits of both structures, enabling efficient implementation of arithmetic operations in $\mathbb{F}_q$.

Theorem (Lenstra & Schoof 1987, Cohen & Huczynska 2003)

For every $q \geq 2$ and $n \geq 1$, there exists a primitive element $\alpha \in \mathbb{F}_{q^n}$ that is normal over $\mathbb{F}_q$.

k-normal elements

$\beta \in \mathbb{F}_{q^n}$ is a *k-normal element* if their $\mathbb{F}_q$-Galois conjugates

$$\beta, \beta^q, \ldots, \beta^{q^{n-1}}$$

generate a $\mathbb{F}_q$-vector space of dimension $n-k$.

Proposition

$\beta \in \mathbb{F}_{q^n}$ is k-normal $\iff$

$$\gcd\left(\beta x^{n-1} + \beta^q x^{n-2} + \cdots + \beta^{q^{n-2}} x + \beta^{q^{n-1}},\ x^n - 1\right)$$

has degree k.

For $\alpha \in \mathbb{F}_{q^n}$ and $f(x) = \sum_{i=0}^{r} a_i x^i \in \mathbb{F}_q[x]$, let $f \circ \alpha = \sum_{i=0}^{r} a_i \alpha^{q^i}$.

Proposition

Let $\alpha \in \mathbb{F}_{q^n}$ be a normal element and $f \in \mathbb{F}_q[x]$ be a divisor of $x^n - 1$ of degree k. Then $\beta = f \circ \alpha$ is k-normal.

Existence of primitive k-normal elements

Problem

Determine (n, k) such that there exist primitive k-normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Partial results:

i. $k = 0$: Primitive normal basis thm.

ii. $k = 1$: Reis & Thomson 2018.

iii. $k = 2$: Aguirre & Neumann 2021.

iv. $0 \leq k \leq n$: Huczynska, Mullen, Panario & Thomson 2013. There exists $\alpha \in \mathbb{F}_{q^n}$ that is k-normal over $\mathbb{F}_q \iff x^n - 1$ has a monic k-degree divisor $f \in \mathbb{F}_q[x]$ (this has nothing to do with primitivity...).

Existence of primitive k-normal elements

Theorem (Reis 2022)

Let $n \in \mathbb{N}$. There exists $C > 0$ such that, for every $q > C$ and every $0 \leq k \leq n$, TFAE:

1. *there exist primitive elements in $\mathbb{F}_{q^n}$ that are k-normal over $\mathbb{F}_q$;*
2. *the polynomial $x^n - 1$ admits a monic divisor $f \in \mathbb{F}_q[x]$ of degree $n-k$ such that $f(x)$ does not divide any binomial $x^d - \delta \in \mathbb{F}_q[x]$ with $d < n$.*

The proof relies on character sums estimates.

Order and polynomials free of binomials

Let $f \in \mathbb{F}_q[x]$ that is not divisible by x. There exists $e \in \mathbb{N}$ such that $f(x) \mid x^e - 1$ and e is minimal. This is the *order* of f and we write $e = \mathrm{ord}(f)$.

In this case, we say that f is *free of binomials* if $f(x)$ does not divide any binomial $x^d - \delta \in \mathbb{F}_q[x]$ with $d < \mathrm{ord}(f)$.

If f is free of binomials and divides $x^n - 1$, then $n = \mathrm{ord}(f)$.

Finding $f \in \mathbb{F}_{q^n}[x]$ that satisfies Condition 2. in previous theorem is equivalent to finding a monic polynomial $f \in \mathbb{F}_q[x]$ such that $\mathrm{ord}(f) = n$, f is free of binomials and $\deg(f) = n - k$.

The main results

Goal: To describe the set of degrees of $f \in \mathbb{F}_q[x]$ that are free of binomials and have a fixed order. We completely describe this set when the order equals a positive integer $n > 1$ whose prime factors divide $p(q-1)$.

Theorem (Brochero Martínez, Reis & Ribas 2025)

Let $n \in \mathbb{N}$ and let $0 \leq k \leq n$. Then there exists $f \in \mathbb{F}_q[x]$ monic such that $ord(f) = n$, f is free of binomials and $\deg(f) = n-k$ $\iff$ one of the following hold:

1. *There exists $h \in \mathbb{F}_q[x]$ monic with at least two distinct irreducible factors such that $ord(h) = n$ and $\deg(h) = n - k$;*

2. *$n = p^\alpha u$, with $\gcd(u, p) = \gcd(u, q-1) = 1$ and $k = n - MN$, where $p^{\alpha-1} < M \leq p^\alpha$ and $N = ord_u(q)$.*

Theorem (Brochero Martínez, Reis & Ribas 2025)

Let $n \in \mathbb{N}_{\geq 2}$ whose prime factors divide $p(q-1)$ and let $0 \leq k \leq n$. Write $n = p^{\alpha} \cdot p_1^{\alpha_1} \dots p_s^{\alpha_s}$, where $\alpha, s \geq 0$ and $p_1, \dots, p_s$ are distinct prime factors of $q-1$. Then there exists $f \in \mathbb{F}_q[x]$ monic such that $ord(f) = n$, f is free of binomials and $\deg(f) = n - k \iff n - k \geq g(q,n)$, where $g(q,n)$ is given as follows:

1. *If $s = 0$, then $g(q,n) = p^{\alpha-1} + 1$;*
2. *If $s \geq 1$, set $u = n/p^{\alpha}$. WLOG assume that $\{1, \dots, t\}$ is the set of integers $1 \leq i \leq s$ such that $p_i^{\alpha_i} \nmid q-1$ ($t = 0$ if the latter does not hold for any $1 \leq i \leq s$).*

   2.1. *If $t \leq 1$, then* $g(q,n) = ord_u(q) + \begin{cases} 1 & \text{if } \alpha = 0, \\ p^{\alpha-1}+1 & \text{if } \alpha > 0; \end{cases}$

   2.2. *If $t > 1$, then*

$$g(q,n) = \sum_{i=1}^{t} ord_{p_i^{\alpha_i}}(q) + \begin{cases} 0 & \text{if } \alpha = 0, \\ p^{\alpha-1}+1 & \text{if } \alpha > 0. \end{cases}$$

The proof considers some cases and subcases according to the factorization of n, and in each of them we build the polynomials with the required properties.

Corollary

Let $n \in \mathbb{N}$ and let S_n be set of prime powers $q = p^s$ such that every prime factor of n divides $p(q-1)$. Then there exists $C > 0$ such that, for every $q \in S_n$ with $q > C$ and every $0 \leq k \leq n$, TFAE:

1. *there exist primitive k-normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$;*
2. *$n - k \geq g(q, n)$, where $g(q, n)$ is as in the previous theorem.*

Known results on cyclotomic polynomials

For $n \in \mathbb{N}$ with $\gcd(n, q) = 1$, the *n-th cyclotomic polynomial* $\Phi_n(x)$ is defined recursively by $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

If $p = \text{char}(\mathbb{F}_q)$, then $x^{np^\ell} - 1 = \prod_{d|n} \Phi_d(x)^{p^\ell}$ when $p \nmid n$.

$x^n - 1$ is squarefree $\iff$ $p \nmid n$.

Lemma

Let $d \in \mathbb{N}$ such that $\gcd(d, q) = 1$. Then $\Phi_d(x)$ splits into $\frac{\varphi(d)}{ord_d(q)}$ irreducible monic polynomials over $\mathbb{F}_q[x]$ of the same degree $ord_d(q)$, where φ is the Euler Totient function.

In this case, $\Phi_d(x)$ is the product of all monic irreducible polynomials of order d.

Known results on orders

If $f(x) \neq x$ is irreducible of order E, then

$$\deg(f) = \mathrm{ord}_E(q).$$

For pairwise coprime $f_1, \ldots, f_r \in \mathbb{F}_q[x]$ not divisible by x,

$$\mathrm{ord}(f_1 \ldots f_r) = \mathrm{lcm}_{1 \leq i \leq r}\{\mathrm{ord}(f_i)\}.$$

For an irreducible $g \in \mathbb{F}_q[x]$ with $x \nmid g$, let $f = g^r$. If $e = \mathrm{ord}(g)$ and $t \in \mathbb{N}$ is the smallest for which $p^t \geq r$, then

$$\mathrm{ord}(f) = ep^t.$$

Properties of polynomials free of binomials

Lemma

Let $f \in \mathbb{F}_q[x]$ be squarefree not free of binomials with $x \nmid f(x)$. Set $n = ord(f)$ and let $d \in \mathbb{N}$ be the smallest such that $f(x) \mid x^d - \delta \in \mathbb{F}_q[x]$. If $f(x) \mid x^D - \alpha \in \mathbb{F}_q[x]$, there exists $k \in \mathbb{N}$ such that $D = dk$. In particular, $d \mid n$, $ord(\delta) = \frac{n}{d}$ and $\alpha = \delta^k$.

Lemma

Let $f \in \mathbb{F}_q[x]$ with $x \nmid f(x)$ and let F be its squarefree part. Then f is free of binomials $\iff$ F is free of binomials.

Lemma

Let $f, g \in \mathbb{F}_q[x]$ be coprime and free of binomials. Then so is fg.

Lemma

Let $f \in \mathbb{F}_q[x]$ be squarefree whose order equals n, a prime power. If f is not free of binomials, then $f(x) \mid \Phi_n(x)$.

Proposition

Let $n \geq 2$ not divisible by p. Suppose that there exist $m \geq 2$ and distinct monic irreducible $g_1, \ldots, g_m \in \mathbb{F}_q[x]$, such that:

1. *$F = g_1 \ldots g_m$ has degree k and order n;*
2. *if n is even, there exists $1 \leq i \leq n$ such that $e_i = \frac{n}{ord(g_i)}$ is even.*

Then there exists a monic irreducible polynomial g such that $F_0 = g \cdot g_2 \ldots g_m$ has degree k, order n and it is free of binomials.

The result below implies the second theorem when $x^n - 1$ has a divisor of degree k, order n and at least two distinct irreducible factors.

Proposition

Let $n \geq 2$ and suppose that $x^n - 1$ has a k-degree divisor of order n which has at least two distinct irreducible factors. Then $x^n - 1$ has a k-degree divisor of order n that is free of binomials.

A relation with coding theory

Let $\mathcal{C}, \mathcal{C}_\lambda$ be vector subspaces of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

$\mathcal{C}$ is a *cyclic code* if, for every $c = (c_1, \ldots, c_n) \in \mathcal{C}$, we have

$$c' = (c_n, c_1, \ldots, c_{n-1}) \in \mathcal{C}.$$

$\mathcal{C}_\lambda$ is a λ-*constacyclic code* if, for every $c = (c_1, \ldots, c_n) \in \mathcal{C}_\lambda$, we have

$$c' = (\lambda c_n, c_1, \ldots, c_{n-1}) \in \mathcal{C}_\lambda.$$

If $\mathcal{C} \subset \mathbb{F}_q^n$ is a cyclic code, then

$$(c_1, \ldots, c_n) \in \mathcal{C} \mapsto c_1 + c_2 x + \cdots + c_n x^{n-1} \in I,$$

where I is a nontrivial ideal of the ring $\frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$. The shifts correspond to multiplications by x.

Similarly, the words in a constacyclic code $\mathcal{C}_\lambda \subset \mathbb{F}_q^d$ can be naturally identified as polynomials that belong to a nontrivial ideal J of the ring $\frac{\mathbb{F}_q[x]}{\langle x^d - \lambda \rangle}$.

Since these rings are PID, $I = \langle f \rangle$ and $J = \langle g \rangle$, where $f(x) \mid x^n - 1$ and $g(x) \mid x^d - \lambda$.

Suppose that $\operatorname{ord}(f) = n$ and f is free of binomials. Then $f(x)$ does not divide any binomial $x^d - \lambda \in \mathbb{F}_q[x]$ with $d < n$. Therefore $\mathcal{C}_\lambda \not\subset \mathcal{C}$ for any constacyclic code $\mathcal{C}_\lambda$.

References

[1] J.J.R. Aguirre, V.G.L. Neumann, Existence of primitive 2-normal elements in finite fields. Finite Fields Appl. 73, 101864 (2021).

[2] F.E. Brochero Martínez, L. Reis, S. Ribas, On polynomials over finite fields that are free of binomials, Des. Codes Cryptogr. (2025). Available at https://doi.org/10.1007/s10623-025-01573-4.

[3] S.D. Cohen, S. Huczynska, The primitive normal basis theorem – without a computer. J. Lond. Math. Soc. 67(1), 41–56 (2003).

[4] S. Huczynska, G.L. Mullen, D. Panario, D. Thomson, Existence and properties of k-normal elements over finite fields. Finite Fields Appl. 24, 170–183 (2013).

[5] H.W. Lenstra Jr., R.J. Schoof, Primitive normal bases for finite fields. Math. Comp. 48(177), 217–231 (1987).

References

[6] R. Lidl, H. Niederreiter, Finite Fields, vol. 20. Encyclopedia of Mathematics and Its Applications. Addison-Wesley, Boston (1983).

[7] L. Reis, D. Thomson, Existence of primitive 1-normal elements in finite fields. Finite Fields Appl. 51, 238–269 (2018).

[8] L. Reis, Existence results on k-normal elements over finite fields, Rev. Mat. Iberoam. 35(3) (2019), 805–822.

[9] L. Reis, Character sums over affine spaces and applications. Finite Fields Appl. 83, 102067 (2022).

That's all Folks! Thank you!

savio.ribas@ufop.edu.br