Normal bases and primitive elements over finite fields

Giorgos Kapetanakis

Department of Mathematics, University of Crete

11th International Conference on Finite Fields and their Applications

Let q be a power of the prime p. We denote by $\mathbb{F}_q$ the finite field of q elements and by $\mathbb{F}_{q^m}$ its extension of degree m. A generator of the multiplicative group $\mathbb{F}_{q^m}^*$ is called primitive and an element $x \in \mathbb{F}_{q^m}$ is called free, if the set $\{x, x^q, x^{q^2}, \ldots, x^{q^{m-1}}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. Such a basis is called normal.

- It is well-known that both primitive and free elements exist.
- The existence of elements that are simultaneously primitive and free is also known:

Theorem (Primitive Normal Basis Theorem)

Let q be a prime power and m a positive integer. There exists some $x \in \mathbb{F}_{q^m}$ that is simultaneously primitive and free.

- Lenstra and Schoof (1987) were the first to provide a complete proof of the above, completing partial proofs of Carlitz (1952) and Davenport (1968).
- Cohen and Huczynska (2003) provided a computer-free proof, with the introduction of sieving techniques.

Recently, an even stronger result was shown.

Theorem (Strong Primitive Normal Basis Theorem)

Let q be a prime power and m a positive integer. There exists some $x \in \mathbb{F}_{q^m}$ such that x and x^{-1} are both simultaneously primitive and free, unless the pair (q, m) is one of $(2, 3)$, $(2, 4)$, $(3, 4)$, $(4, 3)$ or $(5, 4)$.

- Tian and Qi (2006) were the first to prove this result for $m \geq 32$.
- Cohen and Huczynska (2010) were those who extended it to its stated form, using their sieving techniques.
- Since x is primitive if and only if x^{-1} is primitive, the above has three genuine conditions instead of four.

More recently, an extension of both theorems was considered:

Theorem (K.)

Let $q \geq 23$, $m \geq 17$ and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(q)$ such that if A has exactly two non-zero entries and q is odd, then the quotient of these entries is a square in $\mathbb{F}_{q^m}$. There exists some $x \in \mathbb{F}_{q^m}$ such that both x and $(-dx+b)/(cx-a)$ are simultaneously primitive and free.

- It s clear, that even though the above is a natural extension of the previous theorems, the large number of possible exceptions leaves room for improvement. On the other hand we have four genuine conditions, which implies that a pursue to a complete solution is too optimistic.
- Thanks to a notice of Stephen Cohen, if the condition of $(-dx+b)/(cx-a)$ to be primitive was missing from the above, the resulting problem would still be an extension the Primitive Normal Basis Theorem and its Strong version. In this work we ommit that condition and solve the resulting problem completely.

- The additive group of $\mathbb{F}_{q^m}$ is an $\mathbb{F}_q[X]$-module, under the rule $F \circ x := \sum_{i=0}^{n} f_i x^{q^i}$, for $x \in \mathbb{F}_{q^m}$ and $F \in \mathbb{F}_q[X]$.
- The monic generator of the annihilator of x is called Order of x and denoted by $\mathrm{Ord}(x)$.
- Suppose $G \mid X^m - 1$. We call $x \in \mathbb{F}_{q^m}$ G-free if $x = H \circ y$ for some $y \in \mathbb{F}_{q^m}$ and some $H \mid G$ implies $H = 1$. It is not hard to see that free elements are exactly those that are $(X^m - 1)$-free.
- $x \in \mathbb{F}_{q^m}^*$ is primitive if $\mathrm{ord}(x) = q^m - 1$, where $\mathrm{ord}(x)$ stands for the multiplicative order of x.
- Let $d \mid q^m - 1$, we call $x \in \mathbb{F}_{q^m}^*$ d-free if and only if, for $w \mid d$, $x = y^w$ implies $w = 1$. It is not hard to see that primitive elements are exactly those that are $(q^m - 1)$-free.
- It follows from the definitions that $q^m - 1$ may be freely replaced by its radical q_0 and $X^m - 1$ may be replaced by its radical, $F_0 := X^{m_0} - 1$, where m_0 such that $m = m_0 p^b$ and $\gcd(m_0, p) = 1$.

Let $r \mid q_0$ and $F \mid F_0$. Following Cohen and Huczynska (2003 and 2010), we define:

$$\omega_r : \ \mathbb{F}_{q^m} \to \mathbb{C}, \ x \mapsto \theta(r) \sum_{d|r} \frac{\mu(d)}{\phi(d)} \sum_{\chi \in \widehat{\mathbb{F}^*_{q^m}}, \ \mathrm{ord}(\chi)=d} \chi(x)$$

and

$$\Omega_F : \ \mathbb{F}_{q^m} \to \mathbb{C}, \ x \mapsto \theta(F) \sum_{G|F, G \text{ monic}} \frac{\mu(G)}{\phi(G)} \sum_{\psi \in \widehat{\mathbb{F}_{q^m}}, \mathrm{Ord}(\psi)=G} \psi(x).$$

- Here μ denotes the Möbius function, ϕ the Euler function, $\theta(r) := \phi(r)/r$ and $\theta(F) := \phi(F)/q^{\deg(F)}$.
- Those functions can be shown to be characteristic functions of r-free and F-free elements respectively.

The following well-known character sum estimates will prove to be useful

- (Orthogonality relations) Let χ be a non-trivial character of a group $\mathfrak{G}$ and g a non-trivial element of $\mathfrak{G}$. Then $\sum_{x\in\mathfrak{G}}\chi(x)=0$ and $\sum_{\chi\in\widehat{\mathfrak{G}}}\chi(g)=0$.
- (Perel'muter 1969, Castro-Moreno 2000) Let χ be a non-trivial multiplicative character of order n and ψ a non-trivial additive character. Let $\mathcal{F},\mathcal{G}\in\mathbb{F}_{q^m}(X)$ such that $\mathcal{F}\neq y\mathcal{H}^n$, for any $y\in\mathbb{F}_{q^m}$ and $\mathcal{H}\in\mathbb{F}_{q^m}(X)$, and $\mathcal{G}\neq\mathcal{H}^p-\mathcal{H}+y$, for any $y\in\mathbb{F}_{q^m}$ and $\mathcal{H}\in\mathbb{F}_{q^m}(X)$. Then

$$\left|\sum_{x\in\mathbb{F}_{q^m}\setminus S}\chi(\mathcal{F}(x))\psi(\mathcal{G}(x))\right|\leq(\deg(\mathcal{G})_\infty+l+l'-l''-2)q^{m/2},$$

where S is the set of poles of $\mathcal{F}$ and $\mathcal{G}$, $(\mathcal{G})_\infty$ is the pole divisor of $\mathcal{G}$, l is the number of distinct zeros and finite poles of $\mathcal{F}$ in $\bar{\mathbb{F}}_q$, l' is the number of distinct poles of $\mathcal{G}$ (including ∞) and l'' is the number of finite poles of $\mathcal{F}$ that are poles or zeros of $\mathcal{G}$.

- Let $q_1 \mid q_0$ and $F_1, F_2 \mid F_0$. We denote by $\mathbf{k}$ the triple (q_1, F_1, F_2) and call it a divisor triple.
- A special divisor triple is $\mathbf{w} := (q_0, F_0, F_0)$.
- We write $\mathbf{l} \mid \mathbf{k}$, if $\mathbf{l} = (d_1, G_1, G_2)$ and $d_1 \mid q_1$ and $G_i \mid F_i$ for $i = 1, 2$.
- The greatest common divisor and the least common multiple of a set of divisor triples are defined pointwise.
- A divisor triple $\mathbf{p}$ is called prime if it has exactly one entry that is $\neq 1$ and this entry is either a prime number or an irreducible polynomial.
- If two divisor triples are co-prime, then their product can be defined naturally.

- We call an element $x \in \mathbb{F}_{q^m}$ $\mathbf{k}_A$-free, if x is q_1-free and F_1-free and $(-dx+b)/(cx-a)$ is F_2-free. Also we denote by $N_A(\mathbf{k})$ the number of $x \in \mathbb{F}_{q^m}$ that are $\mathbf{k}_A$-free.
- From the fact that ω and Ω are characteristic functions we have that:

$$N_A(\mathbf{k}) = \sum_x \omega_{q_1}(x)\Omega_{F_1}(x)\Omega_{F_2}\left(\frac{-dx+b}{cx-a}\right),$$

  where the sum runs over $\mathbb{F}_{q^m}$, except a/c if $c \neq 0$.
- For $r \in \mathbb{N}$, set $W(r)$ to be the number of square-free divisors of r and $W(F)$ the number of monic square-free divisors of $F \in \mathbb{F}_q[X]$.
- We denote by $f(\mathbf{k})$ the product $f(q_1)f(F_1)f(F_2)$, where f may be θ, ϕ, μ or W

Next, we prove the following.

Proposition

Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$ *and* $\mathbf{k}$ *be a divisor triple. If* $(q, c) \neq (2, 0)$ *and* $q^{m/2} \geq 3W(\mathbf{k})$, *then* $N_A(\mathbf{k}) > 0$.

Proof (sketch).

First, assume $c \neq 0$. Following our definitions, we conclude

$$N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{\mathbf{l}|\mathbf{k}} \frac{\mu(\mathbf{l})}{\phi(\mathbf{l})} \sum_{\chi_1, \psi_1, \psi_2} \mathcal{X}_A(\chi_1, \psi_1, \psi_2),$$

where $\mathcal{X}_A(\chi_1, \psi_1, \psi_2) := \sum_{x \neq \frac{a}{c}} \chi_g(x^{n_1}) \psi_g(\mathcal{G}(x))$, for some $\mathcal{G} \in \mathbb{F}_q(X)$. Using the character sum estimates presented earlier, we show that if $(\chi_1, \psi_1, \psi_2) \neq (\chi_o, \psi_o, \psi_o)$, then $|\mathcal{X}_A(\chi_1, \psi_1, \psi_2)| \leq 3q^{m/2}$. By separating the term that corresponds to (χ_o, ψ_o, ψ_o) from the sum and employing the latter estimate, we eventually get our result. The case $c = 0$ is similar. □

The above proposition is enough to give us results, but without the sieve of Cohen and Huczynska (2003 and 2010) those results would be much weaker and a pursue to a complete solution would probably be impossible.

Definition

Let $\mathbf{k}$ be a divisor triple. A set of complementary divisor triples of $\mathbf{k}$, with common divisor $\mathbf{k}_0$ is a set $\{\mathbf{k}_1, \ldots, \mathbf{k}_r\}$, where $\mathbf{k}_i \mid \mathbf{k}$ for every i, their least common multiple is divided by $\mathbf{k}$ and $(\mathbf{k}_i, \mathbf{k}_j) = \mathbf{k}_0$ for every $i \neq j$.

Definition

If $\mathbf{k}_1, \ldots, \mathbf{k}_r$ are such that $\mathbf{k}_i = \mathbf{k}_0 \mathbf{p}_i$, where $\mathbf{p}_1, \ldots, \mathbf{p}_r$ are distinct prime divisor triples, co-prime to $\mathbf{k}_0$, then this particular set of complementary divisors is called a $(\mathbf{k}_0, r)$-decomposition of $\mathbf{k}$.

For a $(\mathbf{k}_0, r)$-decomposition of $\mathbf{k}$ define $\delta := 1 - \sum_{i=1}^{r} 1/|\mathbf{p}_i|$, where $|\mathbf{p}_i|$ stands for the absolute value of the unique entry $\neq 1$ of $\mathbf{p}_i$, if this entry is a number, and $q^{\deg(F)}$, if this entry is $F \in \mathbb{F}_q[X]$ and $\Delta := (r-1)/\delta + 2$.

Proposition (Sieving inequality)

Let $A \in \mathrm{GL}_2(\mathbb{F}_q)$, $\mathbf{k}$ be a divisor triple and $\{\mathbf{k}_1, \ldots, \mathbf{k}_r\}$ be a set of complementary divisors of $\mathbf{k}$ with common divisor $\mathbf{k}_0$. Then

$$N_A(\mathbf{k}) \geq \sum_{i=1}^{r} N_A(\mathbf{k}_i) - (r-1)N_A(\mathbf{k}_0).$$

Proposition

Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, $\mathbf{k}$ be a divisor triple with a $(\mathbf{k}_0, r)$-decomposition, such that $\delta > 0$. If $(q, c) \neq (2, 0)$ and $q^{m/2} > 3W(\mathbf{k}_0)\Delta$, then $N_A(\mathbf{k}) > 0$.

Well-known results imply that F_0 splits into $\phi(m_0)/s$ monic irreducible polynomials of degree s and some polynomials of degree dividing s, where s is minimal such that $m_0 \mid q^s - 1$. We denote the product of those with degree s by G_0.

Proposition

Let $A \in \mathrm{GL}_2(\mathbb{F}_q)$, $(q, c) \neq (2, 0)$, $\{l_1, \dots l_t\}$ be a set of distinct primes dividing q_0 and $r_0 := \deg(F_0/G_0)$. If

$$q^{m/2} > \frac{3}{2^t} W(q_0) W^2(F_0/G_0) \left(\frac{q^s(2(m_0 - r_0) + s(t-1))}{sq^s\left(1 - \sum_{i=1}^{t} 1/l_i\right) - 2(m_0 - r_0)} + 2 \right),$$

then $N_A(\mathbf{w}) > 0$, provided the denominator of the inequality is > 0.

Lemma

For any $r \in \mathbb{N}$, $W(r) \leq c_r r^{1/4}$, where $c_r = 2^s/(p_1 \cdots p_s)^{1/4}$ and $p_1, \dots, p_s$ are the primes ≤ 16 that divide r, whilst for all $r \in \mathbb{N}$, $c_r < 4.9$.

From now on we assume that $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$ has at most one entry $= 0$ and that $(q, c) \neq (2, 0)$. First, we consider the following cases:

1. $m > 2$, $m_0 \leq 4$ and if $m = 3$ or $m = 4$ then $m \nmid q - 1$.
2. $m_0 = q - 1$ and $m > 2$.
3. $m_0 \mid q - 1$, $m_0 \neq q - 1$ and $m > 2$.
4. $m = 2$.

We show, utilizing the theory developed earlier, that $N_A(\mathbf{w}) > 0$ for all but a finite number of pairs (q, m), which we list explicitly. We can assume from now on that $m_0 > 4$ and $s \neq 1$.

We define $\rho := t_{F_0/G_0}/m_0$, where t_{F_0/G_0} stands for the number of monic irreducible factors of F_0/G_0. Furthermore, $N_A(\mathbf{w}) > 0$, if

$$q^{m/2} > 3 \cdot 4^{\rho m_0} W(q_0) \left(\frac{2q^s(1-\rho)m_0 - sq^s}{sq^s - 2(1-\rho)m_0} + 2 \right).$$

Lemma (Cohen-Huczynska, 2003)

Assume $m_0 > 4$ *and* $q > 4$.

1. *If* $m_0 = 2\gcd(m, q-1)$ *with* q *odd, then* $s = 2$ *and* $\rho = 1/2$.
2. *If* $m_0 = 4\gcd(m, q-1)$ *with* $q \equiv 1 \pmod 4$, *then* $s = 4$ *and* $\rho = 3/8$.
3. *If* $m_0 = 6\gcd(m, q-1)$ *with* $q \equiv 1 \pmod 6$, *then* $s = 6$ *and* $\rho = 13/36$.
4. *Otherwise* $\rho \leq 1/3$.

Suppose $m_0 \geq 4$. *If* $q = 4$ *and* $m \notin \{9, 45\}$, *then* $\rho \leq 1/5$. *If* $q = 3$ *and* $m \neq 16$, *then* $\rho \leq 1/4$. *If* $q = 2$ *and* $m \notin \{5, 9, 21\}$, *then* $\rho \leq 1/6$.

Next, we prove that $N_A(\mathbf{w}) > 0$ for all but a finite number of pairs (q, m), based on the previous lemma and explicitly list all possible exceptions. We consider the following cases:

1. $m_0 > 4$, $q > 4$, $s \neq 1$ and $\rho > 1/3$.
2. $m_0 > 4$, $q > 4$, $s \neq 1$ and $\rho \leq 1/3$.
3. $m_0 > 4$, $q \leq 4$ and $s \neq 1$.

Summing up, so far we have proved:

Theorem

Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$. *If* $(q, c) \neq (2, 0)$, *there exist some primitive* $x \in \mathbb{F}_{q^m}$, *such that both* x *and* $(-dx + b)/(cx - a)$ *produce a normal* $\mathbb{F}_q$*-basis of* $\mathbb{F}_{q^m}$, *unless* (q, m) *is one of the pairs listed below.*

	Possible exception pairs (q, m)	#
$m_0 \leq 4$	$(2,3)$, $(2,4)$, $(2,6)$, $(2,8)$, $(2,12)$, $(3,3)$, $(3,4)$, $(3,6)$, $(3,12)$, $(4,4)$, $(4,6)$, $(5,3)$, $(5,5)$, $(7,4)$, $(8,3)$, $(8,4)$, $(8,6)$, $(9,3)$, $(11,3)$, $(11,4)$, $(19,4)$, $(23,3)$, $(23,4)$	*23*
$m_0 = q - 1$	$(4,3)$, $(5,4)$, $(7,6)$, $(8,7)$, $(9,8)$, $(11,10)$, $(13,12)$, $(16,15)$	*8*
$m_0 \mid q - 1$	$(7,3)$, $(9,4)$, $(11,5)$, $(13,3)$, $(13,4)$, $(13,6)$, $(16,3)$, $(17,4)$, $(19,3)$, $(25,3)$	*10*
$\rho > 1/3$	$(5,8)$, $(7,12)$, $(13,8)$, $(5,16)$	*4*
$\rho \leq 1/3$	$(5,6)$, $(7,5)$	*2*
$q \leq 4$	$(4,5)$, $(3,5)$, $(3,7)$	*3*
$m = 2$	$(2,2)$, $(3,2)$, $(4,2)$, $(5,2)$, $(7,2)$, $(8,2)$, $(9,2)$, $(11,2)$, $(13,2)$, $(16,2)$, $(17,2)$, $(19,2)$, $(23,2)$, $(25,2)$, $(27,2)$, $(29,2)$, $(31,2)$, $(37,2)$, $(41,2)$, $(43,2)$, $(59,2)$, $(61,2)$, $(71,2)$	*23*
	Total:	*73*

For the remaining cases a computer program was written in C, using Victor Shoup's NTL library. The results follow:

Table: $q = 2$.

m	$f \in \mathbb{F}_2[X]$ irreducible	$x \in \mathbb{F}_{2^m}$ primitive, such that x and $A_i \circ x$ free
2	$1 + X + X^2$	β for $i = 0, 1, 2$
3	$1 + X + X^3$	$1 + \beta$ for $i = 0, 2$; None for $i = 1$
4	$1 + X + X^4$	None for $i = 0$; $1 + \beta^3$ for $i = 1, 2$
6	$1 + X + X^6$	β^5 for $i = 0$; $1 + \beta^5$ for $i = 1, 2$
8	$1 + X + X^3 + X^4 + X^8$	$1 + \beta^5$ for $i = 0, 1, 2$
12	$1 + X^3 + X^{12}$	$\beta + \beta^2 + \beta^3 + \beta^9$ for $i = 0$; $1 + \beta + \beta^9$ for $i = 1, 2$

Table: q is an odd prime and $m = 2$.

q	$f \in \mathbb{F}_q[X]$ irreducible	$x \in \mathbb{F}_{q^m}$ primitive, such that x and $A \circ x$ free
3	$2 + X + X^2$	β (6); $1 + \beta$ (4)
5	$4 + 3X + X^2$	$1 + \beta$ (22); $2 + \beta$ (6)
7	$4 + X + X^2$	$3 + \beta$ (46); $5 + \beta$ (8)
11	$7 + 4X + X^2$	β (118); $4 + \beta$ (12)
13	$6 + 4X + X^2$	β (166); $4 + \beta$ (14)
17	$13 + 15X + X^2$	$3 + \beta$ (286); $6 + \beta$ (2); $4 + \beta$ (16)
19	$8 + 17X + X^2$	$4 + \beta$ (358); $13 + \beta$ (20)
23	$3 + X^2$	$2 + \beta$ (526); $8 + \beta$ (22); $9 + \beta$ (2)
29	$17 + 10X + X^2$	$13 + \beta$ (838); $14 + \beta$ (30)
31	$11 + 2X + X^2$	β (958); $2 + \beta$ (32)
37	$16 + 9X + X^2$	$2 + \beta$ (1366); $3 + \beta$ (36); $6 + \beta$ (2)
41	$3 + 3X + X^2$	$4 + \beta$ (1678); $12 + \beta$ (42)
43	$28 + 3X + X^2$	β (1846); $1 + \beta$ (44)
59	$10 + 17X + X^2$	$2 + \beta$ (3478); $8 + \beta$ (60)
61	$47 + 34X + X^2$	$2 + \beta$ (3718); $10 + \beta$ (62)
71	$24 + 23X + X^2$	$2 + \beta$ (5038); $21 + \beta$ (72)

Table: $q = 3$ or $q = 5$ and $m > 2$.

q	m	$f \in \mathbb{F}_q[X]$ irreducible	$x \in \mathbb{F}_{q^m}$ primitive, such that x and $A \circ x$ free
3	3	$2 + 2X + 2X^2 + X^3$	$1 + \beta$ (7); $2 + \beta$ (3)
	4	$2 + 2X + X^2 + X^3 + X^4$	$2 + 2\beta + \beta^2$ (3); $1 + \beta + 2\beta^2$ (1); β (3); 2β (3)
	5	$1 + X^2 + 2X^3 + X^5$	$1 + 2\beta$ (6); $2 + 2\beta$ (3); $\beta + \beta^2$ (1)
	6	$1 + 2X + 2X^2 + 2X^3 + 2X^4 + X^5 + X^6$	$2\beta + \beta^2$ (3); $2 + \beta + \beta^2$ (7)
	7	$1+X+2X^2+X^4+X^5+X^6+X^7$	β (6); $1 + 2\beta$ (3); $\beta + \beta^2$ (1)
	12	$1+2X+X^2+2X^4+X^9+2X^{10}+X^{12}$	$2 + \beta + \beta^5$ (5); $1 + 2\beta + \beta^5$ (5)
5	3	$1 + 3X + X^2 + X^3$	$1 + \beta$ (22); $2 + \beta$ (5); $1 + 2\beta$ (1)
	4	$4+3X+X^2+2X^3+X^4$	$4 + 2\beta$ (7); $2 + \beta$ (15); $1 + 3\beta$ (2); None (4)
	5	$1 + 2X + 4X^2 + 3X^3 + 2X^4 + X^5$	$4 + \beta$ (23); $1 + 2\beta$ (5)
	6	$3 + 2X + X^3 + 3X^4 + 2X^5 + X^6$	$4 + 2\beta + \beta^2$ (18); $3\beta + \beta^2$ (4); $2 + 3\beta + \beta^2$ (5); $4 + \beta + 2\beta^2$ (1)
	8	$3 + 2X + 3X^3 + 2X^4 + 3X^5 + 4X^6 + X^8$	$3 + 2\beta$ (7); $2 + 3\beta$ (2); $4 + \beta$ (15); $4 + \beta^3$ (4)
	16	$1 + 2X + 3X^4 + X^5 + 3X^6+3X^8+3X^9+X^{10}+ 3X^{11} + X^{12} + 4X^{13} + 4X^{14} + 2X^{15} + X^{16}$	$4 + 3\beta + \beta^3$ (3); $3\beta + \beta^3$ (10); $1 + 3\beta + \beta^3$(8); $4 + 2\beta + \beta^3$ (7)

Table: $q \in \{7, 11\}$ and $m > 2$.

q	m	$f \in \mathbb{F}_q[X]$ irreducible	$x \in \mathbb{F}_{q^m}$ primitive, such that x and $A \circ x$ free
7	3	$6 + 5X^2 + X^3$	$2 + \beta$ (34); $4 + 2\beta$ (15); $3 + 3\beta$ (2); $2 + 3\beta$ (2); $4 + 3\beta$ (1)
	4	$3 + X^2 + 4X^3 + X^4$	β (35); $4 + \beta$ (4); $2 + \beta$ (14); $1 + 2\beta$ (1)
	5	$4+X+3X^2+2X^3+5X^4+X^5$	β (46); $2 + \beta$ (7); $6 + \beta$ (1)
	6	$6 + 2X + 4X^3 + 5X^4 + X^6$	$6 + \beta + \beta^2$ (17); $3 + 4\beta + \beta^2$ (10); $5 + 4\beta + \beta^2$ (2); $1 + 4\beta + \beta^2$ (25)
	12	$3+6X+X^2+5X^3+4X^5+3X^7+2X^8+3X^9+2X^{10}+X^{11}+X^{12}$	$1+6\beta+\beta^2$ (7); $4+3\beta+3\beta^2$ (1); $6+2\beta+2\beta^2$ (7); $6+\beta+\beta^2$ (14); $3+\beta+\beta^2$ (22); $5+2\beta+2\beta^2$ (1); $3+5\beta+2\beta^2$ (1); $5+6\beta+\beta^2$ (1)
11	3	$10 + 2X + X^2 + X^3$	$6 + \beta$ (118); $2 + 2\beta$ (2); $10 + \beta$ (10)
	4	$5 + 7X + 4X^2 + 2X^3 + X^4$	$2 + \beta$ (118); $4 + 2\beta$ (12)
	5	$8+9X+8X^2+6X^3+2X^4+X^5$	$5 + \beta + \beta^2$ (13); $6 + \beta + \beta^2$ (3); $1 + \beta + \beta^2$ (78); $4 + \beta + \beta^2$ (35); $7 + \beta + \beta^2$ (1)
	10	$9+8X+9X^2+7X^3+4X^4+7X^5+7X^6+2X^7+X^8+8X^9+X^{10}$	$4 + \beta + \beta^2$ (11); $4 + 3\beta + \beta^2$ (1); $1 + \beta^2$ (48); $9 + \beta + \beta^2$ (2); $6 + \beta + \beta^2$ (21); $7 + \beta + \beta^2$ (1); $4 + \beta^2$ (32); $9 + \beta^2$ (13); $2 + 3\beta + \beta^2$ (1)

Table: $q > 11$ is an odd prime and $m > 2$.

q	m	$f \in \mathbb{F}_q[X]$ irreducible	$x \in \mathbb{F}_{q^m}$ primitive, such that x and $A \circ x$ free
13	3	$3 + X + 6X^2 + X^3$	$1 + \beta$ (142); $9 + \beta$ (33); $11 + \beta$ (4); $12 + \beta$ (1)
	4	$4+8X+7X^2+9X^3+X^4$	$6 + \beta$ (33); $4 + \beta$ (142); $11 + \beta$ (5)
	6	$10 + 11X + X^2 + 3X^3 + X^4 + 3X^5 + X^6$	$4+2\beta+\beta^2$ (119); $8+2\beta+\beta^2$ (43); $4+3\beta+\beta^2$ (14); $8+3\beta+\beta^2$ (2); $8 + 5\beta + \beta^2$ (1); $5 + 5\beta + \beta^2$ (1)
	8	$6 + 8X + 7X^2 + 2X^3 + 12X^4 + 2X^5 + 4X^6 + 2X^7 + X^8$	$4 + \beta$ (33); β (130); $5 + 2\beta$ (13); $8 + 2\beta$ (1); 2β (3)
	12	$4 + 11X + 3X^2 + 8X^3 + 7X^4+3X^5+2X^6+3X^7+ 9X^8 + 9X^9 + 3X^{10} + 10X^{11} + X^{12}$	$5+\beta+\beta^2$ (94); $8+3\beta+\beta^2$ (2); $2+2\beta+\beta^2$ (2); $7+\beta+\beta^2$ (41); $9+\beta+\beta^2$ (27); $4+3\beta+\beta^2$ (1); $4+2\beta+\beta^2$ (1); $7+2\beta+\beta^2$ (12)
17	4	$4 + 12X + 5X^2 + X^4$	$5 + \beta$ (58); $10 + \beta$ (22); $4 + \beta$ (222); $13 + \beta$ (2)
19	3	$5 + 3X + 4X^2 + X^3$	β (322); $1 + \beta$ (51); $3 + \beta$ (5)
	4	$3 + 6X + 10X^2 + X^4$	$4 + \beta$ (358); $7 + \beta$ (20)
23	3	$1 + 4X + 7X^2 + X^3$	$1 + \beta$ (526); $2 + \beta$ (23); $3 + \beta$ (1)
	4	$13+8X+18X^2+8X^3+ X^4$	$6 + \beta^2$ (482); $7 + \beta^2$ (63); $17 + \beta^2$ (4); $18 + \beta^2$ (1)

Table: $q \in \{4, 8\}$.

$q = p^n$	$h \in \mathbb{F}_p[X]$	m	$f \in \mathbb{F}_q[X]$	$x \in \mathbb{F}_q m$
$4 = 2^2$	$1 + X + X^2$	2	$\alpha + \alpha X + X^2$	β (18)
		3	$1 + \alpha + X^3$	$1 + \alpha + \beta + \beta^2$ (3); $1 + \beta + \beta^2$ (8); $\alpha + \alpha\beta + \beta^2$ (3); $1 + \alpha + \alpha\beta + \beta^2$ (1); None (3)
		4	$\alpha + X + (1 + \alpha)X^3 + X^4$	β (14); $\alpha\beta$ (4)
		5	$1 + \alpha X^3 + X^4 + X^5$	$\alpha + \beta$ (10); $1 + \alpha + \beta$ (6); $\alpha\beta$ (1); $1 + \beta + \beta^2$ (1)
		6	$\alpha + X + \alpha X^2 + X^3 + \alpha X^4 + X^5 + X^6$	$1 + \beta^3$ (14); $1 + \alpha + (1 + \alpha)\beta + \beta^3$ (4)
$8 = 2^3$	$1 + X + X^3$	2	$\alpha + \alpha X + X^2$	β (70)
		3	$\alpha^2 + (1+\alpha^2)X + (\alpha+\alpha^2)X^2 + X^3$	$1 + \beta$ (9); β (61)
		4	$\alpha^2 + \alpha X + (1+\alpha+\alpha^2)X^2 + X^3 + X^4$	$1 + \alpha + \beta$ (62); $\alpha^2 + \beta$ (8)
		6	$\alpha + (1+\alpha+\alpha^2)X + (1+\alpha^2)X^2 + (1+\alpha)X^3 + (\alpha+\alpha^2)X^4 + \alpha X^5 + X^6$	$\alpha + \beta^3$ (70)
		7	$1 + X + (1 + \alpha^2)X^2 + \alpha X^3 + \alpha X^4 + \alpha^2 X^5 + \alpha^2 X^6 + X^7$	$1 + \beta + \beta^2$ (40); $1 + \alpha + \beta + \beta^2$ (24); $1 + \alpha^2 + \beta + \beta^2$ (1); $\alpha + \alpha^2 + \beta + \beta^2$ (1); $\alpha^2 + \beta + \beta^2$ (4)

Table: $q > 8$ is composite.

$q = p^n$	$h \in \mathbb{F}_p[X]$	m	$f \in \mathbb{F}_q[X]$	$x \in \mathbb{F}_q m$
$9 = 3^2$	$2+X+X^2$	2	$\alpha + 2\alpha X + X^2$	β (78); $1 + \beta$ (10)
		3	$2 + 2\alpha + 2\alpha X^2 + X^3$	β (80); $1 + \beta$ (8)
		4	$2+\alpha+\alpha X+(1+\alpha)X^2+\alpha X^3+X^4$	β^2 (62); $2 + \beta^2$ (22); $\alpha + \beta^2$ (4)
		8	$2+(1+\alpha)X+(2+2\alpha)X^2+(2+2\alpha)X^3+(1+\alpha)X^5+2X^6+(2+\alpha)X^7+X^8$	$1 + \beta$ (27); $\alpha + \beta$ (2); $2 + \beta$ (12); β (46); $1 + \alpha + \beta$ (1)
$16 = 2^4$	$1+X+X^4$	2	$\alpha + \alpha X + X^2$	β (270)
		3	$1 + \alpha + \alpha^3 + (1 + \alpha^2 + \alpha^3)X + X^2 + X^3$	β (223); $\alpha+\beta$ (41); $\alpha+\alpha^2+\beta$ (4); $1\alpha + \beta$ (2)
		15	$(\alpha + \alpha^2 + \alpha^3) + (1 + \alpha + \alpha^2 + \alpha^3)X + (1 + \alpha + \alpha^2 + \alpha^3)X^2 + (\alpha+\alpha^2)X^3+(1+\alpha^2)X^4+(1+\alpha+\alpha^2+\alpha^3)X^5+(\alpha+\alpha^2)X^6+\alpha^3X^7+(\alpha^2+\alpha^3)X^8+(\alpha+\alpha^2)X^9+(1+\alpha^3)X^{10}+(1+\alpha+\alpha^2)X^{11}+(1+\alpha+\alpha^2+\alpha^3)X^{12}+(\alpha+\alpha^2)X^{13}+(\alpha+\alpha^2+\alpha^3)X^{14}+X^{15}$	$\alpha + \beta^3$ (103); $\alpha + \alpha^3 + \beta^3$ (62); $1 + \alpha^2 + \alpha^3 + \beta^3$ (4); $1 + \alpha + (1 + \alpha^2)\beta + \beta^3$ (15); $1 + alpha + (1 + \alpha + \alpha^2)\beta + \beta^3$ (1); $1 + \alpha^2 + \alpha^3 + \alpha\beta + \beta^3$ (1); $\alpha + \alpha^2 + \beta^3$ (63); $1+\alpha^3+\alpha\beta+\beta^3$ (1); $1+\alpha+\alpha^2+\alpha\beta+\beta^3$ (2); $\alpha^3 + \alpha\beta + \beta^3$ (3); $\alpha + \alpha\beta + \beta^3$ (15)
$25 = 5^2$	$4 + 3X + X^2$	2	$3 + 2\alpha + 4\alpha X + X^2$	β (622); $1 + \beta$ (26)
		3	$\alpha+(2+4\alpha)X+(4+4\alpha)X^2+X^3$	β (574); $1 + \beta$ (68); $2 + \beta$ (6)
$27 = 3^3$	$2 + 2X + 2X^2 + X^3$	2	$1 + \alpha + (1 + \alpha)X + X^2$	β (726); $1 + \beta$ (26); $2 + \beta$ (2)

Summing up, we proved:

Theorem

Let q be a prime power, $m \geq 2$ an integer and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$. There exists some primitive $x \in \mathbb{F}_{q^m}$, such that both x and $(-dx+b)/(cx-a)$ produce a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, unless one of the following hold:

1. $q = 2$, m *is odd and* $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$,
2. $q = 2$, $m = 3$ *and* $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ *or* $A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$,
3. $q = 3$, $m = 4$ *and* A *is anti-diagonal or*
4. (q, m) *is* $(2, 4)$, $(4, 3)$ *or* $(5, 4)$ *and* $a = 0$.

One can make two unexpected observations:

- Our exception pairs are exactly those appearing in the Strong Primitive Normal Basis Theorem.
- If none of the entries of A is zero, there are no exceptions at all!

THANK YOU!