Polynomials with special properties over finite fields

Giorgos Kapetanakis

Wednesday, 24 February 2016

Our purpose is to prove some existence results for irreducible polynomials over finite fields, with special properties. These properties include combinations of

- primitiveness,
- freeness (a root of the polynomial forms a normal basis) and
- having some coefficients prescribed.

The main idea behind our techniques dates back to the 50's and the work of Carlitz and remains popular among authors. Roughly, our method is:

1. We express the characteristic or a characteristic-like function for a polynomial (or its roots) with the desired properties with help of characters,
2. this leads us to a sufficient condition for the existence of our desired polynomial.
3. With the the help of characters sum estimates, we end up with asymptotic results, for the existence of the elements we seek.
4. If necessary and desirable, we deal with the remaining cases with a case-by-case approach.

Part I: The Hansen-Mullen conjecture for self-reciprocal irreducible polynomials

This work is joint work with Theodoulos Garefalakis and published:

T. Garefalakis and G. Kapetanakis.
On the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials.
Finite Fields Appl., 18(4):832–841, 2012.

T. Garefalakis and G. Kapetanakis.
A note on the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials.
Finite Fields Appl., 35(C):61–63, 2015.

Hansen and Mullen (1992) conjectured that there exists an irreducible polynomial of $\mathbb{F}_q$ with a coefficient prescribed, with some exceptions. Wan (1997) proved that the conjecture holds, for $q > 19$ or $n \geq 36$ and Ham and Mullen (1998) proved the remaining cases with the help of computers.

Theorem (Hansen-Mullen conjecture)

Let $a \in \mathbb{F}_q$, let $n \geq 2$ and fix $0 \leq j < n$. Then there exists an irreducible polynomial $P(X) = X^n + \sum_{k=0}^{n-1} P_k X^k$ over $\mathbb{F}_q$ with $P_j = a$ except when $j = a = 0$ or q even, $n = 2$, $j = 1$, and $a = 0$.

Given a polynomial $Q \in \mathbb{F}_q[X]$, its reciprocal Q^R is defined as

$$Q^R(X) = X^{\deg(Q)} Q(1/X).$$

One class of polynomials that has been intensively investigatedis that of self-reciprocal irreducible polynomials, that is, irreducible polynomials that satisfy $Q^R(X) = Q(X)$. Besides their theoretical interest, self-reciprocal irreducible polynomials have been useful in applications, and in particular in the construction of error-correcting codes.

It is natural to expect that self-reciprocal monic irreducible polynomials over finite fields, with some coefficient fixed, exist.

- Carlitz (1967) characterized self-reciprocal irreducible monic polynomials over $\mathbb{F}_q$ (srimp): Q is a srimp iff

$$Q(X) = X^n \hat{P}(X + X^{-1})$$

for some monic irreducible $\hat{P}$ of degree n, such that $\psi(\hat{P}) = -1$, where ψ, the Jacobi symbol modulo $X^2 - 4$.
- Which (after some computations) implies

$$Q_k = \sum_{j=0}^{k} \delta_j P_j,$$

where P is an irreducible polynomial with constant term equal to 1 and $\psi(P) = \varepsilon$.

We define $\tau_{n,k} : \mathbb{G}_k \to \mathbb{F}_q,\ H \mapsto \sum_{j=0}^{k} \delta_j H_j$. We have proved:

Proposition

If there exists an irreducible $P \in \mathbb{F}_q[X]$ with $P_0 = 1$, such that $\psi(P) = \varepsilon$ and $P \equiv H \pmod{X^{k+1}}$ for some $H \in \mathbb{G}_k$ with $\tau_{n,k}(H) = a$. Then there exists a srimp Q, of degree $2n$, with $Q_k = a$.

Next, we need to correlate the inverse image of $\tau_{n,k}$ with $\mathbb{G}_{k-1}$. In this direction, we prove.

Proposition

There exists a polynomial F (defined appropriately) such that the map $\tau_{n,k}^{-1}(a) \to \mathbb{G}_{k-1}\ :\ H \mapsto HF \pmod{X^{k+1}}$ is a bijection.

Inspired by Wan's work (1997) we introduce the following weighted sum.

$$w_a(n,k) = \sum_{H \in \tau_{n,k}^{-1}(a)} \Lambda(FH) \sum_{\psi(P)=\varepsilon,\ P \equiv H \pmod{X^{k+1}}} 1.$$

If $w_a(n,k) > 0$, then there exists a srimp Q, of degree $2n$ with $Q_k = a$.

Let U be the subgroup of $(\mathbb{F}_q[X]/X^{k+1}\mathbb{F}_q[X])^*$ that contains classes of polynomials with constant term equal to 1. Using the orthogonality relations, we eventually get that

$$w_a(n,k) = \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \in \mathbb{J}_n \\ \psi(P)=\varepsilon}} \chi(P)\bar{\chi}(G) \sum_{H \in \mathbb{G}_{k-1}} \Lambda(H)\bar{\chi}(H),$$

where G is the inverse of F modulo X^{k+1}.

We separate the term that corresponds to χ_0 and we get

$$\left| w_a(n,k) - \frac{\pi_q(n,\varepsilon)}{q^k} \sum_{H \in \mathbb{G}_{k-1}} \Lambda(H) \right| \leq \frac{1}{q^k} \sum_{\chi \neq \chi_o} \left| \sum_{P \in \mathbb{J}_n,\ \psi(P)=\varepsilon} \chi(P) \right| \left| \sum_{H \in \mathbb{G}_{k-1}} \Lambda(H) \bar{\chi}(H) \right|,$$

where $\pi_q(n,\varepsilon) = |\{P \text{ irreducible of degree } n : \psi(P) = \varepsilon\}|$.

Then we use estimates for $\sum_{H\in\mathbb{G}_{k-1}} \Lambda(H)$, $\sum_{H\in\mathbb{G}_{k-1}} \Lambda(H)\bar{\chi}(H)$ and $\pi_q(n,-1)$, we conclude that:

Theorem

Let $n \geq 2$, $1 \leq k \leq n$, and $a \in \mathbb{F}_q$. There exists a srimp $Q \in \mathbb{F}_q[X]$, of degree $2n$ with $Q_k = a$ if the following bound holds.

$$q^{\frac{n-k-1}{2}} \geq \frac{16}{5}k(k+5) + \frac{1}{2}.$$

Our final step is to content ourselves for $k \leq n/2$ and solve the resulting problem. Using the theory developed earlier, we conclude that there exists a srimp over $\mathbb{F}_q$ of degree $2n$ with its k-th coefficient prescribed, if

$$\pi_q(n, -1) > \frac{\lfloor n/2 \rfloor (\lfloor n/2 \rfloor + 5)}{n} (\sqrt{q} + 1)(q^{\lfloor n/2 \rfloor /2} - 1) q^{n/2}.$$

This bound is always true for $n \geq 27$. For $n < 27$ this bound is satisfied for the pairs (q, n) described below

n	3	4	5	6	7	8	9	10
q	≥ 149	≥ 839	≥ 37	≥ 59	≥ 17	≥ 23	≥ 11	≥ 13
n	11	12	13	14	15	16	17	18
q	≥ 9	≥ 9	≥ 7	≥ 7	≥ 5	≥ 7	≥ 5	≥ 5
n	19	20	21	22	23	24	25	26
q	≥ 5	≥ 5	≥ 5	≥ 5	≥ 5	≥ 5	≥ 3	≥ 5

For the remaining cases, computers searches have been employed. The computer results, combined with the above imply the following.

Theorem

Let $n \geq 3$ an integer and q a power of an odd prime. If $k \leq n/2$ and $a \in \mathbb{F}_q$, then there exists a srimp of degree $2n$ such that any of its k-th coefficient is prescribed to a, unless

1. $q = 3$, $n = 3$, $a = 0$ *and* $k = 1$ *or*
2. $q = 3$, $n = 4$, $a = 0$ *and* $k = 2$.

Part II: Extending the (strong) primitive normal basis theorem I

This work is published in:

G. Kapetanakis.
Normal bases and primitive elements over finite fields.
Finite Fields Appl., 26:123–143, 2014.

- A generator of the multiplicative group $\mathbb{F}_{q^m}^*$ is called primitive. It is well-known that primitive elements exist for every q and m. Primitive elements are used in various applications, such as the Diffie-Hellman key exchange and the construction of Costas arrays, used in sonar and radar technology.
- An element $x \in \mathbb{F}_{q^m}$ is called free over $\mathbb{F}_q$ (or just 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. Hensel (1888) proved the existence of normal basis (normal basis theorem). He also observed their computational advantages for fast arithmetic. Naturally, software and hardware implementations, used mostly in coding theory and cryptography, use normal bases.
- Both primitiveness and freeness are properties common to either all or none of the roots of an irreducible polynomial, hence one can define primitive polynomials and free polynomials naturally.

Both primitive and free elements exist for every q and m. The existence of elements that are simultaneously primitive and free is also well-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 over $\mathbb{F}_q$.

Lenstra and Schoof (1987) were the first prove this result. Cohen and Huczynska (2003) provided a computer-free proof, using sieving techniques. 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 over $\mathbb{F}_q$, unless the pair (q, m) is one of $(2, 3)$, $(2, 4)$, $(3, 4)$, $(4, 3)$ or $(5, 4)$.

Cohen and Huczynska (2010) proved this result in its stated form, using sieving techniques.

The problem we are considering here is the following.

Problem

Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$*. Does there exist some primitive* $x \in \mathbb{F}_{q^m}$ *such that both* x *and* $(ax+b)/(cx+d)$ *are free over* $\mathbb{F}_q$*?*

- We solve this problem completely.
- Although not quite clear, this problem qualifies as an extension of the strong primitive normal basis theorem.

We call Order of $x \in \mathbb{F}_{q^m}$ (note the big 'O') its additive order. For $G \mid X^m - 1$, we call x G-free, if $x = H \circ y$ for some $y \in \mathbb{F}_{q^m}$ and $H \mid G$, implies $H = 1$. Then the characteristic function of G-free elements is

$$\Omega_G(x) := \theta(G') \sum_{F \mid G,\, F \text{ monic}} \frac{\mu(F)}{\phi(F)} \sum_{\psi \in \widehat{\mathbb{F}_{q^m}},\, \mathrm{Ord}(\psi) = F} \psi(x),$$

where G' is the square-free part of G. Also, free elements are exactly those of Order $X^m - 1$, i.e. those that are F_0-free, where F_0 is the square-free part of $X^m - 1$.

Similarly, order of $x \in \mathbb{F}_{q^m}^*$ (note the small 'o') is the multiplicative order of x. Also, for $r \mid q^m - 1$, we call x r-free, if $w \mid r$ and $x = y^w$ implies $w = 1$. The characteristic function of r-free elements is

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

where r' is the square-free part of r. Further, primitive elements are exactly those that have order equal to $q^m - 1$, that is those that are $(q^m - 1)$-free, or q_0-free, where q_0 is the square-free part of $q^m - 1$.

- Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, $q_1 \mid q_0$ and $F_i \mid F_0$, for $i = 1, 2$. Set $\mathbf{k} := (q_1, F_1, F_2)$ and call it a divisor triple. We call $x \in \mathbb{F}_{q^m}$ $\mathbf{k}_A$-free, if x is q_1-free and F_1-free and $(ax + b)/(cx + d)$ is F_2-free. Also, $N_A(\mathbf{k})$ stands for the number of $x \in \mathbb{F}_{q^m}$ that are $\mathbf{k}_A$-free.
- Set t_r to be the number of prime (or irreducible) divisors of r and $W(r) := 2^{t_r}$. It follows that $\sum_{d|r} |\mu(d)| = W(r)$.
- For $\mathbf{k} = (q_1, F_1, F_2)$ we will 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.

Lemma

For any $r \in \mathbb{N}$, $W(r) \le c_{r,a} r^{1/a}$, where $c_{r,a} = 2^s/(p_1 \cdots p_s)^{1/a}$ and $p_1, \ldots, p_s$ are the primes $\le 2^a$ that divide r.

Clearly our aim is to prove that $N_A(\mathbf{w}) > 0$. The proposition below is our first step towards this.

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* $q^{m/2} \geq 3\,W(\mathbf{k})$, *then* $N_A(\mathbf{k}) > 0$.

- If $q = 2$ and $c = 0$, then $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, hence we are looking for some free x, such that $x + 1$ is also free, impossible for odd m and always true for even m.
- The proof is divided in two parts, $c \neq 0$ and $c = 0$, since different types of character sums arise in each case.

Following Cohen and Huczynska (2003 and 2010), we introduce a sieve that will help us get improved results.

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* $\delta > 0$ *and* $\mathbf{k}_0 = (q_1, F_1, F_1)$*. If* $(q, c) \neq (2, 0)$ *and* $q^{m/2} > 3\,W(\mathbf{k}_0)\Delta$*, then* $N_A(\mathbf{k}) > 0$*.*

It follows from well-known results about the way that F_0 splits into irreducible factors that

Proposition

Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, $(q,c) \neq (2,0)$, $\{l_1, \ldots l_t\}$ *be a set of distinct primes (this set may be* $\emptyset$*, in which case* $t = 0$*) 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 that the above denominator is positive.*

Using previous results, we begin to prove that $N_A(\mathbf{w}) > 0$, by distinguishing the following special cases:

- $m_0 \leq 4$.
- $m_0 = q - 1$.
- $m_0 \mid q - 1$.
- $m = 2$: This is a special case altogether, treated separately.
- None of the above.

We explicitly check each of the cases described above and we deduce the following.

Theorem

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$*. If* $q \neq 2$ *or* $A \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$*, there exist some primitive* $x \in \mathbb{F}_{q^m}$*, such that both* x *and* $(ax+b)/(cx+d)$ *produce a normal* $\mathbb{F}_q$*-basis of* $\mathbb{F}_{q^m}$*, unless* (q, m) *is one of the 70 pairs listed below.*

Case	Possible exception pairs (q, m)	#
$m_0 \leq 4$	$(8,6)$, $(5,5)$, $(4,6)$, $(3,12)$, $(3,6)$, $(2,12)$, $(2,8)$, $(2,6)$, $(2,4)$, $(4,4)$, $(8,4)$, $(3,4)$, $(7,4)$, $(11,4)$, $(19,4)$, $(23,4)$, $(2,3)$, $(3,3)$, $(5,3)$, $(8,3)$, $(9,3)$, $(11,3)$, $(23,3)$	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
$\rho \leq 1/3$	$(5,6)$, $(5,12)$, $(7,5)$, $(11,6)$	4
$q < 5$	$(4,5)$, $(4,7)$, $(4,9)$, $(4,15)$, $(3,5)$, $(3,7)$, $(3,8)$, $(3,10)$, $(3,16)$, $(2,5)$, $(2,7)$, $(2,9)$, $(2,11)$, $(2,15)$, $(2,21)$	15
$m = 2$	$(2,2)$, $(3,2)$, $(4,2)$, $(5,2)$, $(7,2)$, $(11,2)$	6
	Total:	**70**

Our final step is to examine the remaining cases one-by-one and identify the true exceptions to our problem. In order to perform all the necessary tests, a computer program was written in Sage. These are the results.

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	$X^2 + X + 1$	β for $i = 0, 1, 2$
3	$X^3 + X + 1$	$\beta + 1$ for $i = 0, 2$; **None** for $i = 1$
4	$X^4 + X + 1$	**None** for $i = 0$; $\beta^3 + 1$ for $i = 1, 2$
5	$X^5 + X^2 + 1$	β^3 for $i = 0$; $\beta + 1$ for $i = 1$; $\beta^2 + \beta + 1$ for $i = 2$
6	$X^6 + X^4 + X^3 + X + 1$	$\beta^3 + 1$ for $i = 0$; $\beta^3 + \beta + 1$ for $i = 1, 2$
7	$X^7 + X + 1$	$\beta^3 + \beta + 1$ for $i = 0$; $\beta^3 + \beta^2 + 1$ for $i = 1$; $\beta^3 + 1$ for $i = 2$
8	$X^8 + X^4 + X^3 + X^2 + 1$	$\beta^5 + \beta$ for $i = 0$; $\beta^5 + \beta + 1$ for $i = 1, 2$
9	$X^9 + X^4 + 1$	$\beta^4 + \beta + 1$ for $i = 0$; $\beta + 1$ for $i = 1$; $\beta^2 + \beta + 1$ for $i = 2$
11	$X^11 + X^2 + 1$	$\beta^3 + 1$ for $i = 0$; $\beta + 1$ for $i = 1$; $\beta^2 + \beta + 1$ for $i = 2$
12	$X^{12} + X^7 + X^6 + X^5 + X^3 + X + 1$	$\beta^5 + 1$ for $i = 0, 1, 2$
15	$X^{15} + X^5 + X^4 + X^2 + 1$	$\beta^3 + 1$ for $i = 0$; $\beta + 1$ for $i = 1$; $\beta^4 + \beta^3 + \beta^2 + \beta + 1$ for $i = 2$
21	$X^{21} + X^6 + X^5 + X^2 + 1$	$\beta^5 + \beta^2 + \beta + 1$ for $i = 0$; $\beta^3 + \beta + 1$ for $i = 1$; $\beta^4 + \beta^3 + \beta + 1$ for $i = 2$

Table: $q = 3$.

m	$f \in \mathbb{F}_3[X]$ irreducible	$x \in \mathbb{F}_{3^m}$ primitive, such that x and $A \circ x$ free
2	$X^2 + 2X + 2$	$\beta + 2$ (4); β (6)
3	$X^3 + 2X + 1$	$2\beta^2 + 1$ (3); $\beta^2 + 1$ (7)
4	$X^4 + 2X^3 + 2$	β (7); 2β (3)
5	$X^5 + 2X + 1$	$\beta + 1$ (6); $\beta + 2$ (3); $\beta + 2$ (1)
6	$X^6 + 2X^4 + X^2 + 2X + 2$	$\beta^2 + 1$ (5); $\beta^2 + \beta + 2$ (3); $\beta^4 + 2\beta^2$ (2)
7	$X^7 + 2X^2 + 1$	$\beta^2 + 1$ (2); $2\beta + 2$ (2); $\beta + 2$ (6)
8	$X^8 + 2X^5 + X^4 + 2X^2 + 2X + 2$	$\beta^4 + \beta + 1$ (4); $\beta^4 + \beta^2 + 2\beta + 1$ (3); $\beta^4 + \beta^3 + 1$ (1); $\beta^4 + 2\beta$ (2)
10	$X^{10} + 2X^6 + 2X^5 + 2X^4 + X + 2$	$\beta^3 + 2\beta + 1$ (7); $\beta^3 + 2\beta^2 + 1$ (1); $2\beta^3 + \beta + 2$ (2)
12	$X^{12} + X^6 + X^5 + X^4 + X^2 + 2$	$\beta^7 + 2\beta + 2$ (5); $\beta^7 + \beta^2 + \beta$ (3); $\beta^7 + \beta^2 + \beta + 2$ (2)
16	$X^{16} + 2X^7 + 2X^6 + 2X^4 + 2X^3 + 2X^2 + X + 2$	$\beta + 2$ (3); $2\beta + 1$ (3); $\beta^2 + 2$ (1); $2\beta^2 + 1$ (1); $2\beta^3 + \beta^2 + 1$ (1); $\beta^3 + 2\beta^2 + 2$ (1)

Table: $q = 5$.

m	$f \in \mathbb{F}_5[X]$ irreducible	$x \in \mathbb{F}_{5^m}$ primitive, such that x and $A \circ x$ free
2	$X^2 + 4X + 2$	β (22); $\beta + 4$ (6)
3	$X^3 + 3X + 3$	$\beta + 3$ (23); $2\beta + 4$ (1); $\beta + 4$ (4)
4	$X^4 + 4X^2 + 4X + 2$	$\beta^2 + \beta + 1$ (15); $\beta^2 + 3\beta + 3$ (5); $\beta^2 + 3\beta + 4$ (1); **None** (4); $\beta^2 + 4\beta$ (1); $2\beta^2 + \beta + 1$ (1); $2\beta^2 + 3\beta$ (1)
5	$X^5 + 4X + 3$	$\beta^4 + 1$ (23); $\beta^4 + 2$ (5)
6	$X^6 + X^4 + 4X^3 + X^2 + 2$	$\beta^2 + 1$ (11); $2\beta^2 + 4\beta + 3$ (4); $\beta^2 + 2\beta + 4$ (5); $\beta^2 + \beta$ (6); $2\beta^2 + 2\beta$ (1); $3\beta^2 + 3$ (1)
8	$X^8 + X^4 + 3X^2 + 4X + 2$	$\beta^3 + 2\beta + 2$ (9); $\beta^3 + 3\beta + 2$ (5); $\beta^3 + 2\beta + 1$ (10); $\beta^3 + 4\beta + 3$ (2); $\beta^3 + 3\beta + 4$ (1); $\beta^3 + 4\beta + 4$ (1)
12	$X^{12} + X^7 + X^6 + 4X^4 + 4X^3 + 3X^2 + 2X + 2$	$\beta + 4$ (14); $3\beta + 2$ (5); $2\beta + 3$ (7); $4\beta + 1$ (2)
16	$X^{16} + X^8 + 4X^7 + 4X^6 + 4X^5 + 2X^4 + 4X^3 + 4X^2 + X + 2$	$2\beta^2 + 4\beta + 1$ (1); $\beta^2 + 2\beta + 3$ (7); $\beta^2 + 2$ (10); $\beta^2 + 4\beta + 3$ (8); $3\beta^2 + 2\beta + 4$ (1); $2\beta^2 + 4$ (1)

Table: $q \in \{7, 11\}$.

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	2	$X^2 + 6X + 3$	β (46); $\beta + 1$ (8)
	3	$X^3 + 6X^2 + 4$	$\beta + 1$ (16); $\beta + 6$ (3); β (35)
	4	$X^4 + 5X^2 + 4X + 3$	$\beta + 1$ (46); $\beta + 3$ (8)
	5	$X^5 + X + 4$	$\beta + 1$ (46); $3\beta + 4$ (8)
	6	$X^6 + X^4 + 5X^3 + 4X^2 + 6X + 3$	$\beta^2 + 5\beta$ (8); $\beta^2 + 4\beta$ (9); $\beta^2 + 4\beta + 2$ (12); $\beta^2 + 5\beta + 4$ (6); $\beta^2 + 3\beta + 6$ (16); $2\beta^2 + \beta$ (1); $\beta^2 + 6\beta + 6$ (1); $\beta^2 + 6\beta + 1$ (1)
	12	$X^{12} + 2X^8 + 5X^7 + 3X^6 + 2X^5 + 4X^4 + 5X^2 + 3$	$\beta^2 + 4\beta + 1$ (15); $3\beta^2 + 3\beta + 4$ (1); $2\beta^2 + \beta + 2$ (1); $\beta^2 + \beta + 6$ (29); $\beta^2 + 5\beta + 4$ (5); $2\beta^2 + 3\beta + 1$ (1); $\beta^2 + 5\beta + 3$ (2)
11	2	$X^2 + 7X + 2$	β (118); $\beta + 7$ (12)
	3	$X^3 + 2X + 9$	$\beta + 7$ (12); $\beta + 4$ (118)
	4	$X^4 + 8X^2 + 10X + 2$	$\beta + 2$ (118); $\beta + 5$ (10); $\beta + 6$ (2)
	5	$X^5 + 10X^2 + 9$	$\beta + 7$ (6); $\beta + 4$ (78); $\beta + 5$ (35); $\beta + 10$ (1); $\beta + 9$ (10)
	6	$X^6 + 3X^4 + 4X^3 + 6X^2 + 7X + 2$	$\beta + 3$ (118); $\beta + 8$ (10); $2\beta + 5$ (2)
	10	$X^{10} + 7X^5 + 8X^4 + 10X^3 + 6X^2 + 6X + 2$	$\beta + 10$ (22); $\beta + 4$ (59); $\beta + 7$ (33); $2\beta + 3$ (13); $2\beta + 9$ (2); $2\beta + 8$ (1)

Table: q is a prime ≥ 13.

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	$X^3 + 2X + 11$	$\beta + 5$ (142); $2\beta + 6$ (15); $2\beta + 3$ (21); $2\beta + 8$ (1); $2\beta + 9$ (1)
	4	$X^4 + 3X^2 + 12X + 2$	$\beta + 2$ (142); $\beta + 4$ (32); $\beta + 11$ (6)
	6	$X^6 + 10X^3 + 11X^2 + 11X + 2$	$\beta^3 + \beta + 9$ (3); $\beta^3 + \beta + 3$ (31); $\beta^3 + \beta$ (118); $\beta^3 + \beta + 7$ (28)
	8	$X^8 + 8X^4 + 12X^3 + 2X^2 + 3X + 2$	$\beta + 1$ (131); $\beta + 3$ (42); $\beta + 5$ (6); $\beta + 11$ (1)
	12	$X^{12} + X^8 + 5X^7 + 8X^6 + 11X^5 + 3X^4 + X^3 + X^2 + 4X + 2$	$\beta + 11$ (37); $\beta + 3$ (59); $2\beta + 1$ (13); $\beta + 7$ (37); $\beta + 6$ (15); $3\beta + 5$ (1); $2\beta + 5$ (2); $\beta + 9$ (13); $2\beta + 9$ (2); $3\beta + 7$ (1)
17	4	$X^4 + 7X^2 + 10X + 3$	$\beta + 9$ (222); $\beta + 10$ (58); $\beta + 13$ (21); $2\beta + 3$ (1); $2\beta + 3$ (2)
19	3	$X^3 + 4X + 17$	$\beta + 3$ (322); $\beta + 5$ (52); $\beta + 6$ (4)
	4	$X^4 + 2X^2 + 11X + 2$	$\beta + 1$ (322); $\beta + 5$ (50); $\beta + 8$ (5); $\beta + 9$ (1)
23	3	$X^3 + 2X + 18$	$\beta + 9$ (526); $\beta + 3$ (24)
	4	$X^4 + 3X^2 + 19X + 5$	$\beta + 7$ (526); $\beta + 9$ (23); $\beta + 11$ (1)

Table: $q = 4$.

In that case, $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, where α is a root of $X^2 + X + 1 \in \mathbb{F}_2[X]$.

m	$f \in \mathbb{F}_q[X]$	$x \in \mathbb{F}_q m$
2	$X^2 + X + \alpha$	$\alpha\beta + \alpha + 1$ (18)
3	$X^3 + \alpha X^2 + (\alpha+1)X + \alpha$	$\alpha\beta^2 + (\alpha+1)\beta + \alpha + 1$ (3); $\alpha\beta^2 + \alpha\beta$ (8); $\alpha\beta^2 + \alpha\beta + \alpha + 1$ (3); **None** (3); $\alpha\beta^2 + (\alpha+1)\beta + 1$ (1)
4	$X^4 + X^2 + (\alpha+1)X + \alpha$	$\alpha\beta^3$ (15); $\alpha\beta^3 + \alpha$ (3)
5	$X^5 + (\alpha+1)X^4 + X + \alpha$	$\alpha\beta + \alpha$ (14); $(\alpha+1)\beta$ (4)
6	$X^6 + (\alpha+1)X^5 + (\alpha+1)X^4 + X^3 + X + \alpha + 1$	$\alpha\beta^3 + \alpha\beta$ (11); $\alpha\beta^3 + \alpha$ (7)
7	$X^7 + \alpha X^6 + X^5 + (\alpha+1)X^3 + X^2 + \alpha X + 1$	$\alpha\beta$ (13); $\alpha\beta + 1$ (5)
9	$X^9 + (\alpha+1)X^8 + \alpha X^7 + X^6 + (\alpha+1)X^5 + \alpha X^4 + X^3 + (\alpha+1)X + 1$	$\alpha\beta^2 + \alpha\beta$ (8); $\alpha\beta^2 + \alpha\beta + 1$ (2); $(\alpha+1)\beta^2 + \alpha\beta + 1$ (1); $\alpha\beta^2 + \alpha\beta + \alpha + 1$ (6); $\alpha\beta^2 + \beta + \alpha + 1$ (1)
15	$X^{15} + \alpha X^1 4 + (\alpha+1)X^1 3 + X^1 2 + \alpha X^1 1 + \alpha X^1 0 + X^8 + X^7 + X^6 + X^4 + (\alpha+1)X^3 + \alpha X + 1$	$(\alpha+1)\beta^2 + \alpha\beta + \alpha$ (4); $\alpha\beta^2 + \alpha\beta + 1$ (8); $\alpha\beta^2 + (\alpha+1)\beta + 1$ (1); $\beta^2 + \beta + \alpha + 1$ (1); $\alpha\beta^2 + \beta + 1$ (2); $\beta^2 + \alpha\beta + \alpha + 1$ (1); $(\alpha+1)\beta^2 + (\alpha+1)\beta + \alpha$ (1)

Table: $q \in \{8, 9\}$.

q	$h \in \mathbb{F}_p[X]$	m	$f \in \mathbb{F}_q[X]$	$x \in \mathbb{F}_{q^m}$
8	$X^3 + X + 1$	3	$X^3+(\alpha^2+\alpha+1)X^2+(\alpha^2+1)X+\alpha^2+\alpha+1$	$\alpha\beta$ (61); $\alpha\beta+\alpha$ (9)
		4	$X^4+(\alpha^2+1)X^3+(\alpha^2+\alpha)X^2+(\alpha^2+\alpha)X+\alpha^2+1$	$\alpha\beta$ (62); $\alpha\beta+\alpha+1$ (8)
		6	$X^6+(\alpha^2+\alpha+1)X^5+(\alpha^2+\alpha+1)X^3+X^2+(\alpha^2+\alpha+1)X+1$	$\alpha\beta$ (70)
		7	$X^7+(\alpha^2+\alpha+1)X^6+(\alpha+1)X^5+(\alpha^2+1)X^4+\alpha^2X^3+(\alpha+1)X^2+(\alpha+1)X+\alpha^2+1$	$\alpha\beta^2+\alpha\beta+\alpha^2+\alpha$ (9); $\alpha\beta^2+\alpha\beta+\alpha^2$ (8); $\alpha\beta^2+\alpha\beta+\alpha$ (22); $\alpha\beta^2+\alpha\beta$ (27); $\alpha\beta^2+\alpha\beta+\alpha^2+1$ (2); $\alpha\beta^2+\alpha\beta+\alpha^2+\alpha+1$ (2)
9	$X^2 + 2X + 2$	3	$X^3+X^2+\alpha+1$	$\alpha\beta$ (80); $\alpha\beta+\alpha$ (8)
		4	$X^4+(\alpha+2)X^3+2X^2+(\alpha+1)X+2\alpha+1$	$\alpha\beta+\alpha+1$ (63); $\alpha\beta+\alpha+2$ (15); $\alpha\beta^2+\alpha\beta+\alpha+1$ (7); $(\alpha+1)\beta+2\alpha+1$ (1); $\alpha\beta^2+(\alpha+2)\beta+2$ (1); $(\alpha+1)\beta+1)$ (1)
		8	$X^8+(2\alpha+2)X^7+2\alpha X^5+2\alpha X^4+2X^3+(2\alpha+1)X^2+(2\alpha+2)X+\alpha+2$	$\alpha\beta^2+\alpha\beta+2\alpha+1$ (47); $\alpha\beta^2+\alpha\beta+\alpha+2$ (19); $\alpha\beta^2+(2\alpha+1)\beta+1$ (8); $\alpha\beta^2+\alpha\beta+2\alpha+2$ (11); $\alpha\beta^2+(2\alpha+1)\beta$ (2); $\alpha\beta^2+2\beta+2\alpha+1$ (1)

Table: $q \in \{16, 25\}$.

q	$h \in \mathbb{F}_p[X]$	m	$f \in \mathbb{F}_q[X]$	$x \in \mathbb{F}_{q^m}$
16	$X^4 + X + 1$	3	$X^3 + (\alpha + 1)X + \alpha^2$	$\alpha\beta + \alpha$ (223); $\alpha\beta + \alpha + 1$ (41); $\alpha\beta + \alpha^2 + \alpha + 1$ (6)
		15	$X^{15} + (\alpha^3 + 1)X^{14} + (\alpha^3 + \alpha^2 + \alpha + 1)X^{13} + \alpha^3 X^{12} + \alpha X^{11} + (\alpha^2 + \alpha + 1)X^{10} + (\alpha^3 + \alpha^2)X^9 + \alpha X^8 + (\alpha^2 + \alpha)X^7 + (\alpha^2 + 1)X^6 + (\alpha^3 + \alpha)X^5 + (\alpha^2 + \alpha + 1)X^4 + \alpha^2 X^3 + (\alpha^3 + \alpha^2)X^2 + (\alpha^2 + \alpha)X + \alpha^3 + \alpha$	$\alpha\beta + \alpha^3$ (93); $\alpha\beta + \alpha + 1$ (21); $\alpha\beta + \alpha$ (133); $\alpha\beta + \alpha^2 + 1$ (17); $\alpha\beta + \alpha^3 + \alpha + 1$ (4); $\alpha\beta + \alpha^3 + \alpha$ (2)
25	$X^2 + 4X + 2$	3	$X^3 + (3\alpha + 3)X^2 + 2\alpha X + 2\alpha + 2$	$\alpha\beta$ (575); $\alpha\beta + \alpha$ (67); $\alpha\beta + 2\alpha + 2$ (5); $\alpha\beta + 2\alpha + 1$ (1)

Summing up, we have proved:

Theorem

Let q be a prime power, $m \geq 2$ an integer and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, where $A \neq \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ if $q = 2$ and m is odd. There exists some primitive $x \in \mathbb{F}_{q^m}$, such that both x and $(ax+b)/(cx+d)$ produce a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, unless one of the following hold:

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

- We have exactly the exceptions appearing in the strong primitive normal basis theorem.
- We have no exceptions at all if all of the entries of A are non-zero!
- All the exceptions described above are genuine (not just possible).

Part III: Extending the (strong) primitive normal basis theorem II

This work is published in:

G. Kapetanakis.
An extension of the (strong) primitive normal basis theorem.
Appl. Algebra Engrg. Comm. Comput., 25(5):311–337, 2014.

The problem we consider here is the following.

Problem

Let q be a prime power, m a positive integer and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$. Does there exist some $x \in \mathbb{F}_{q^m}$ such that both x and $(ax+b)/(cx+d)$ are simultaneously primitive and free over $\mathbb{F}_q$?

- This problem and the problem we considered in Part II, are similar, but not identical, i.e. in Part II we had three conditions (x is primitive, x is free over $\mathbb{F}_q$ and $(ax+b)/(cx+d)$ is free over $\mathbb{F}_q$), while here we also demand $(ax+b)/(cx+d)$ to be primitive. Still both problems are natural extensions of the primitive normal basis theorem and its strong version.
- We do not solve this problem completely, but we show that it is true, provided that q and m are large enough.

Theorem

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

Muito obrigado!