An Extension of the Strong Primitive Normal Basis Theorem

Giorgos Kapetanakis

University of Crete

RICAM Workshop on Finite Fields and Their Applications:
Character Sums and Polynomials

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* over $\mathbb{F}_q$ 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 over $\mathbb{F}_q$.

- 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.

More 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 over $\mathbb{F}_q$, 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.

The question we are interested is:

Question

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 exists some $x \in \mathbb{F}_{q^m}$ such that both x and $(-dx+b)/(cx-a)$ are simultaneously primitive and free over $\mathbb{F}_q$?

- Clearly, the Primitive Normal Basis Theorem and the Strong Primitive Normal Basis Theorem answer the above question for some special matrices.
- We prove that the above question can be answered positively for every $A \in \mathrm{GL}_2(\mathbb{F}_q)$, if $q \geq 23$ and $m \geq 17$, providing an extension to these powerful and important Theorems.

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 $F \in \mathbb{F}_q[X]$.

Definition

The monic generator of the annihilator of x is called *Order* of x and denoted by $\mathrm{Ord}(x)$.

- Clearly, $\mathrm{Ord}(x) \mid X^m - 1$ and the elements of $\mathbb{F}_{q^m}$ that are free over $\mathbb{F}_q$ are exactly those of Order $X^m - 1$.
- Suppose $G \mid X^m - 1$. We call $x \in \mathbb{F}_{q^m}$ *G-free* over $\mathbb{F}_q$ if $x = H \circ y$ for some $y \in \mathbb{F}_{q^m}$ and some $H \mid G$ implies $H = 1$.

- $x \in \mathbb{F}_{q^m}^*$ 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 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 $\gcd(m_0, p) = 1$.

- We will call the characters of the multiplicative and the additive group of $\mathbb{F}_{q^m}$ *multiplicative* and *additive* characters respectively and we will extend the multiplicative characters to zero with the rule

$$\chi(0) := \begin{cases} 0, & \text{if } \chi \in \widehat{\mathbb{F}_{q^m}^*} \setminus \{\chi_o\}, \\ 1, & \text{if } \chi = \chi_o. \end{cases}$$

- We will denote by χ_o and ψ_o the trivial multiplicative and additive character respectively, by χ_g a generator of $\widehat{\mathbb{F}_{q^m}^*}$ and by ψ_g the canonical additive character.

Let $r \mid q_0$. Following Cohen and Huczynska (2003 and 2010), we define the characteristic function of the r-free elements of $\mathbb{F}_{q^m}$ as follows:

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

where μ denotes the Möbius function, ϕ the Euler function and $\theta(r) := \phi(r)/r = \prod_{l \mid r, l \text{ prime}} (1 - l^{-1})$.

For $F \mid F_0$ we define

$$\Omega_F : \mathbb{F}_{q^m} \to \mathbb{C},$$

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

which can be shown (Cohen and Huczynska 2003 and 2010) to be the characteristic function of the elements of $\mathbb{F}_{q^m}$ that are F-free over $\mathbb{F}_q$. Here $\phi(F) := |(\mathbb{F}_q[X]/F\mathbb{F}_q[X])^*|$, the Euler function,

$$\mu(F) := \begin{cases} (-1)^r, & \text{if } F \text{ is divisible by } r \text{ distinct monic irreducibles,} \\ 0, & \text{otherwise,} \end{cases}$$

the Möbius function and $\theta(F) := \phi(F)/q^{\deg(F)}$.

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

$$\sum_{x\in\mathfrak{G}}\chi(x)=0 \quad \text{and} \quad \sum_{\chi\in\widehat{\mathfrak{G}}}\chi(g)=0.$$

- Kloosterman sums: Let χ be a multiplicative character (may be trivial or non-trivial) and ψ a non trivial additive character. If $y_1, y_2 \in \mathbb{F}_{q^m}$ are not both zero, then

$$\left|\sum_{x\in\mathbb{F}^*_{q^m}}\chi(x)\psi(y_1x+y_2x^{-1})\right|\leq 2q^{m/2}.$$

- Let χ be a non-trivial multiplicative character of order n, and $F\in\mathbb{F}_{q^m}[X]$ such that $F\neq yH^{q^m-1}$, for any $y\in\mathbb{F}_{q^m}$ and $H\in\mathbb{F}_{q^m}[X]$. If F has l distinct roots, then

$$\left|\sum_{x\in\mathbb{F}_{q^m}}\chi(F(x))\right|\leq (l-1)q^{m/2}.$$

Theorem

Let χ be a non-trivial multiplicative character of order n and ψ a non-trivial additive character. Let $\mathcal{F}, \mathcal{G}$ be rational functions 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 $\mathcal{G}$.

A slightly weaker (lacking the term l'') version of the above result was initially proved by Perel'muter (1969), but Castro and Moreno (2000) improved the result to its stated form. Recently, Cochraine and Pinner (2006) presented an elementary proof.

- Let $q_i \mid q_0$ and $F_i \mid F_0$, for $i = 1, 2$. We denote by $\mathbf{k}$ the quadruple (q_1, q_2, F_1, F_2) and call it a *divisor quadruple*.
- A special divisor quadruple is $\mathbf{w} := (q_0, q_0, F_0, F_0)$.
- We write $\mathbf{l} \mid \mathbf{k}$, if $\mathbf{l} = (d_1, d_2, G_1, G_2)$ and $d_i \mid q_i$ and $G_i \mid F_i$ for $i = 1, 2$.
- The greatest common divisor and the least common multiple of a set of divisor quadruples are defined pointwise.
- A divisor quadruple $\mathbf{p}$ 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 quadruples are co-prime, then their product can be defined naturally.

- We call an element $x \in \mathbb{F}_{q^m}$ $\mathbf{k}_A$-*free* over $\mathbb{F}_q$, if x is q_1-free and F_1-free over $\mathbb{F}_q$ and $(-dx+b)/(cx-a)$ is q_2-free and F_2-free over $\mathbb{F}_q$. Also we denote by $N_A(\mathbf{k})$ the number of $x \in \mathbb{F}_{q^m}$ that are $\mathbf{k}_A$-free over $\mathbb{F}_q$.
- From the fact that ω and Ω are characteristic functions we have that:

$$N_A(\mathbf{k}) = \sum_x \omega_{q_1}(x)\Omega_{F_1}(x)\omega_{q_2}\left(\frac{-dx+b}{cx-a}\right)\Omega_{F_2}\left(\frac{-dx+b}{cx-a}\right),$$

  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 $f(q_1)f(q_2)f(F_1)f(F_2)$, where f may be θ, ϕ, μ or W

Next, we prove the following.

Proposition

Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, $q \neq 2$ *and* $\mathbf{k}$ *be a divisor quadruple. If* $q^{m/2} > 4W(\mathbf{k})$, *then* $N_A(\mathbf{k})$ *is positive.*

We consider four cases, depending on the form of A:

1. matrices that are neither upper triangular nor anti-diagonal,
2. upper triangular matrices that are not diagonal,
3. anti-diagonal matrices and
4. diagonal matrices.

Sketch of the proof for the first case.

From the definitions it follows that

$$N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{\mathbf{l}|\mathbf{k}} \frac{\mu(\mathbf{l})}{\phi(\mathbf{l})} \sum_{\chi_i, \psi_i} \mathcal{X}_A(\chi_1, \chi_2, \psi_1, \psi_2),$$

where

$$\mathcal{X}_A(\chi_1, \chi_2, \psi_1, \psi_2) = \sum_{x \neq a/c} \chi_g(\mathcal{F}(x)) \psi_g(\mathcal{G}(x)),$$

for some $\mathcal{F}, \mathcal{G} \in \mathbb{F}_q(X)$. With the help of the character sum estimates presented previously, we show that if $(\chi_1, \chi_2, \psi_1, \psi_2) \neq (\chi_o, \chi_o, \psi_o, \psi_o)$, then $|\mathcal{X}_A(\chi_1, \chi_2, \psi_1, \psi_2)| \leq 4q^{m/2}$. Next, we separate the term that corresponds to $(\chi_o, \chi_o, \psi_o, \psi_o)$ and with the help of the identities $\sum_{d|r} |\mu(d)| = W(r)$ and $\sum_{G|F} |\mu(G)| = W(F)$ (for $r \in \mathbb{N}$ and $F \in \mathbb{F}_q[X]$) we show that if

$$q^{m/2} > 4W(\mathbf{k}) - \frac{7}{2},$$

then $N_A(\mathbf{k}) > 0$, which clearly implies the desired result. □

1. The proof of our proposition for the other forms of A is not that straightforward, but in the end we get slightly better results. In particular, if A is upper triangular, but not diagonal, then our condition would be $q^{m/2}\frac{q(q-2)}{(q-1)^2} > 2W(\mathbf{k}) - 4$; if A is anti-diagonal, then our condition would be $q^{m/2} \geq 4W(\mathbf{k}) - 15$ and if A is diagonal, then our condition would be $q^{m/2} \geq 2W(q_1)W(q_2)W(\mathrm{lcm}(F_1, F_2)) - 12$.
2. This proposition is enough to give us results, but without the sieve of Cohen and Huczynska (2003 and 2010) those results would be much weaker.

Definition

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

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

Proposition

Let $\mathbf{k}$ *be a divisor quadruple with a* $(\mathbf{k}_0, r)$*-decomposition, such that* $\delta > 0$ *and* $\mathbf{k}_0 = (q_1, q_1, F_1, F_1)$ *for some* $q_1 \mid q_0$ *and* $F_1 \mid F_0$*. If* $A \in \mathrm{GL}_2(\mathbb{F}_q)$*,* $q > 2$ *and* $q^{m/2} > 4W(\mathbf{k}_0)\Delta$*, 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 $\{l_1, \ldots l_t\}$ be a set of distinct primes dividing q_0 and $r_0 := \deg(F_0/G_0)$. If

$$q^{m/2} > 4^{1-t} W^2(q_0) W^2(F_0/G_0) \left(\frac{q^s(2(m_0 - r_0) + s(2t-1))}{sq^s\left(1 - 2\sum_{i=1}^{t} 1/l_i\right) - 2(m_0 - r_0)} + 2 \right),$$

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

The lemma below will prove to be useful.

Lemma

For any $r \in \mathbb{N}$, $W(r) \leq c_r r^{1/8}$, where $c_r = 2^s/(p_1 \cdots p_s)^{1/8}$ and $p_1, \ldots, p_s$ are the primes $\leq 2^8$ that divide r. Furthermore, for all $r \in \mathbb{N}$, $c_r < 4514.7$.

We begin with some special cases:

- First we deal with the case $m_0 \leq 4$, where sieving is unnecessary. Here $W(F_0) \leq 4^4$.
- We continue with the case $m_0 = q - 1$. Here we rely on the fact that F_0 splits into $q - 1$ linear factors and we use sieving on roughly half of them.
- Next, we show our result when $m_0 \mid q - 1$ and $m_0 \neq q - 1$. Here we rely on the fact that $G_0 = F_0$.

Now, we focus on the remaining cases, i.e. when $m_0 > 4$ 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. The lemma below provides an estimation of ρ.

Lemma (Cohen and 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 $\rho \leq 1/3$.*

Furthermore, the last proposition of the sieve implies that $N_A(\mathbf{w}) > 0$, if

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

With the help of this inequality we prove our desired result for all cases described in the above lemma.

A rough description of the proofs:

1. Using the theory developed earlier appropriately we get a sufficient condition for $N_A(\mathbf{w}) > 0$ of the form

$$q^{m/4} > 4c_{q_0}^2(\cdots).$$

2. We substitude c_{q_0} with 4514.7, which is enough to prove our result for all but a finite number of couples (q, m).
3. For what remains we explicitely compute c_{q_0}. In most cases, the exact value of c_{q_0} is significally smaller that 4514.7; however this procedure may not be enough to complete our proof.
4. If there are still couples (q, m) that appear as possible exceptions, exact evaluations of $W(q_0)$ further reduce their number.
5. As a measure of last resort we may use multiplicative sieving as well.

A few notes on the proofs:

1. Computers have been used for our evaluations (using MAPLE v. 13).
2. It would take less that a minute or two for a modern computer to perform all necessary calculations.

Summing up, we have proved:

Theorem

Let $q \geq 23$ be a prime power, $m \geq 17$ an integer and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$. There exists some $x \in \mathbb{F}_{q^m}$ such that both x and $(-dx+b)/(cx-a)$ are simultaneously primitive and free over $\mathbb{F}_q$.

- Can we improve our result?
- Can we answer our question completely, i.e. determine which couples (q, m) are true exceptions?

THANK YOU!