Permutations of the Form $x^k - \gamma \mathrm{Tr}(x)$ and Curves over Finite Fields

Nurdagül Anbar

Sabancı University

Boolean Functions and their Applications (BFA)
June 16-21, 2019

Dedicated to the 70th birthday of Claude Carlet

p: a prime number

$\mathbb{F}$: the finite field of order p^n

$\bar{\mathbb{F}}$: the algebraic closure of $\mathbb{F}$

Recall:

$R(X) \in \mathbb{F}[X]$ is called a permutation (polynomial) of $\mathbb{F}$ if the induced map $r: \alpha \mapsto R(\alpha)$ permutes $\mathbb{F}$.

Remark: $R(X), Q(X)$ induce the same map on $\mathbb{F}$ if $R(X) \equiv Q(X) \mod (X^{p^n} - X)$.
Therefore, we suppose that $\deg(R) < p^n$.

Example:

(i) $R(X) = X^k \in \mathbb{F}[X]$
R is a permutation of $\mathbb{F} \iff \gcd(k, p^n - 1) = 1$.

(ii) $R(X) = \sum_{i=0}^{m} a_i X^{p^i} \in \mathbb{F}[X]$
R is a permutation of $\mathbb{F} \iff 0$ is the only root of $R(X)$.

p: a prime number

$\mathbb{F}$: the finite field of order p^n

$\bar{\mathbb{F}}$: the algebraic closure of $\mathbb{F}$

Recall:

$R(X) \in \mathbb{F}[X]$ is called a permutation (polynomial) of $\mathbb{F}$ if the induced map $r: \alpha \mapsto R(\alpha)$ permutes $\mathbb{F}$.

Remark: $R(X), Q(X)$ induce the same map on $\mathbb{F}$ if $R(X) \equiv Q(X) \mod (X^{p^n} - X)$.
Therefore, we suppose that $\deg(R) < p^n$.

Example:

(i) $R(X) = X^k \in \mathbb{F}[X]$
R is a permutation of $\mathbb{F} \iff \gcd(k, p^n - 1) = 1$.

(ii) $R(X) = \sum_{i=0}^{m} a_i X^{p^i} \in \mathbb{F}[X]$
R is a permutation of $\mathbb{F} \iff 0$ is the only root of $R(X)$.

p: a prime number

$\mathbb{F}$: the finite field of order p^n

$\bar{\mathbb{F}}$: the algebraic closure of $\mathbb{F}$

Recall:

$R(X) \in \mathbb{F}[X]$ is called a permutation (polynomial) of $\mathbb{F}$ if the induced map $r: \alpha \mapsto R(\alpha)$ permutes $\mathbb{F}$.

Remark: $R(X), Q(X)$ induce the same map on $\mathbb{F}$ if
$R(X) \equiv Q(X) \mod (X^{p^n} - X)$.
Therefore, we suppose that $\deg(R) < p^n$.

Example:

(i) $R(X) = X^k \in \mathbb{F}[X]$
R is a permutation of $\mathbb{F} \iff \gcd(k, p^n - 1) = 1$.

(ii) $R(X) = \sum_{i=0}^{m} a_i X^{p^i} \in \mathbb{F}[X]$
R is a permutation of $\mathbb{F} \iff 0$ is the only root of $R(X)$.

p: a prime number

$\mathbb{F}$: the finite field of order p^n

$\bar{\mathbb{F}}$: the algebraic closure of $\mathbb{F}$

Recall:

$R(X) \in \mathbb{F}[X]$ is called a permutation (polynomial) of $\mathbb{F}$ if the induced map $r: \alpha \mapsto R(\alpha)$ permutes $\mathbb{F}$.

Remark: $R(X), Q(X)$ induce the same map on $\mathbb{F}$ if $R(X) \equiv Q(X) \mod (X^{p^n} - X)$.
Therefore, we suppose that $\deg(R) < p^n$.

Example:

(i) $R(X) = X^k \in \mathbb{F}[X]$
R is a permutation of $\mathbb{F} \iff \gcd(k, p^n - 1) = 1$.

(ii) $R(X) = \sum_{i=0}^{m} a_i X^{p^i} \in \mathbb{F}[X]$
R is a permutation of $\mathbb{F} \iff 0$ is the only root of $R(X)$.

Special Interest: $R(X) = X^k - \gamma \mathrm{Tr}(X) \in \mathbb{F}[X]$, where $\mathrm{Tr}(X) = X + X^p + \cdots + X^{p^{n-1}}$ is the absolute trace function.

(Charpin, Kyureghyan, Zieve, ...)

Recall: For $\gamma = 0$, $R(X)$ is not a permutation of $\mathbb{F}$ if $\gcd(k, p^n - 1) > 1$.

Observation:

If $t = \gcd(k, p^n - 1) > p$, then $R(X)$ is not a permutation of $\mathbb{F}$.

Proof: For any nonzero $\alpha \in \mathrm{Im}(X^k)$, set $S_\alpha = \{u \in \mathbb{F} \mid u^k = \alpha\}$. Since $|\mathrm{Im}(\mathrm{Tr})| = p$ and $|S_\alpha| = t > p$, there are $u_1, u_2 \in S_\alpha$ with $u_1 \neq u_2$ such that $\mathrm{Tr}(u_1) = \mathrm{Tr}(u_2)$. Therefore, we have $R(u_1) = R(u_2)$.

Problem:

Is $R(X)$ a permutation of $\mathbb{F}$, if $\gcd(k, p^n - 1) > 1$?
If not, can we prove it by the theory of Algebraic Curves?

Special Interest: $R(X) = X^k - \gamma \mathrm{Tr}(X) \in \mathbb{F}[X]$, where $\mathrm{Tr}(X) = X + X^p + \cdots + X^{p^{n-1}}$ is the absolute trace function.

(Charpin, Kyureghyan, Zieve, ...)

Recall: For $\gamma = 0$, $R(X)$ is not a permutation of $\mathbb{F}$ if $\gcd(k, p^n - 1) > 1$.

Observation:

If $t = \gcd(k, p^n - 1) > p$, then $R(X)$ is not a permutation of $\mathbb{F}$.

Proof: For any nonzero $\alpha \in \mathrm{Im}(X^k)$, set $S_\alpha = \{u \in \mathbb{F} \mid u^k = \alpha\}$. Since $|\mathrm{Im}(\mathrm{Tr})| = p$ and $|S_\alpha| = t > p$, there are $u_1, u_2 \in S_\alpha$ with $u_1 \neq u_2$ such that $\mathrm{Tr}(u_1) = \mathrm{Tr}(u_2)$. Therefore, we have $R(u_1) = R(u_2)$.

Problem:

Is $R(X)$ a permutation of $\mathbb{F}$, if $\gcd(k, p^n - 1) > 1$?
If not, can we prove it by the theory of Algebraic Curves?

Special Interest: $R(X) = X^k - \gamma \mathrm{Tr}(X) \in \mathbb{F}[X]$, where $\mathrm{Tr}(X) = X + X^p + \cdots + X^{p^{n-1}}$ is the absolute trace function.

(Charpin, Kyureghyan, Zieve, ...)

Recall: For $\gamma = 0$, $R(X)$ is not a permutation of $\mathbb{F}$ if $\gcd(k, p^n - 1) > 1$.

Observation:

If $t = \gcd(k, p^n - 1) > p$, then $R(X)$ is not a permutation of $\mathbb{F}$.

Proof: For any nonzero $\alpha \in \mathrm{Im}(X^k)$, set $S_\alpha = \{u \in \mathbb{F} \mid u^k = \alpha\}$. Since $|\mathrm{Im}(\mathrm{Tr})| = p$ and $|S_\alpha| = t > p$, there are $u_1, u_2 \in S_\alpha$ with $u_1 \neq u_2$ such that $\mathrm{Tr}(u_1) = \mathrm{Tr}(u_2)$. Therefore, we have $R(u_1) = R(u_2)$.

Problem:

Is $R(X)$ a permutation of $\mathbb{F}$, if $\gcd(k, p^n - 1) > 1$?
If not, can we prove it by the theory of Algebraic Curves?

Definition:

A curve $\mathcal{X}$ is a zero set of a polynomial $f(X,Y) \in \bar{\mathbb{F}}[X,Y]$, i.e.,

$$\mathcal{X} = \{\, (a,b) \in \bar{\mathbb{F}} \times \bar{\mathbb{F}} \;|\; f(a,b) = 0 \,\} =: \mathcal{Z}(f)\ .$$

$\mathcal{X}$ is defined over $\mathbb{F}$ if $f(X,Y) \in \mathbb{F}[X,Y]$.

From now on, we suppose that $\mathcal{X}$ is defined over $\mathbb{F}$.

$P = (a,b) \in \mathcal{X}$ is called rational if $a, b \in \mathbb{F}$.

$P = (a,b) \in \mathcal{X}$ is called singular if

$$f(a,b) = \frac{\partial f(X,Y)}{\partial X}(a,b) = \frac{\partial f(X,Y)}{\partial Y}(a,b) = 0.$$

$\mathcal{X}$ is called absolutely irreducible over $\mathbb{F}$ if $f(X,Y)$ is absolutely irreducible over $\mathbb{F}$.

Definition:

A curve $\mathcal{X}$ is a zero set of a polynomial $f(X,Y) \in \bar{\mathbb{F}}[X,Y]$, i.e.,

$$\mathcal{X} = \{ (a,b) \in \bar{\mathbb{F}} \times \bar{\mathbb{F}} \mid f(a,b) = 0 \} =: \mathcal{Z}(f) .$$

$\mathcal{X}$ is defined over $\mathbb{F}$ if $f(X,Y) \in \mathbb{F}[X,Y]$.

From now on, we suppose that $\mathcal{X}$ is defined over $\mathbb{F}$.

$P = (a,b) \in \mathcal{X}$ is called rational if $a, b \in \mathbb{F}$.

$P = (a,b) \in \mathcal{X}$ is called singular if

$$f(a,b) = \frac{\partial f(X,Y)}{\partial X}(a,b) = \frac{\partial f(X,Y)}{\partial Y}(a,b) = 0.$$

$\mathcal{X}$ is called absolutely irreducible over $\mathbb{F}$ if $f(X,Y)$ is absolutely irreducible over $\mathbb{F}$.

$\mathcal{X} = \mathcal{Z}(f)$

$N(\mathcal{X})$: the number of rational points of $\mathcal{X}$

$g(\mathcal{X})$: the genus of $\mathcal{X}$

Hasse-Weil Bound:

If $\mathcal{X}$ is a projective, non-singular and absolutely irreducible (!) curve defined over $\mathbb{F}$, then

$$|\mathbb{F}| + 1 - 2g(\mathcal{X})\sqrt{|\mathbb{F}|} \leq N(\mathcal{X}) \leq |\mathbb{F}| + 1 + 2g(\mathcal{X})\sqrt{|\mathbb{F}|}.$$

Hasse-Weil Bound $\Longrightarrow$ sufficiently many rational points if $|\mathbb{F}|$ is sufficiently large compared to $g(\mathcal{X})$ (which depends on $\deg(f)$)!

$\mathcal{X} = \mathcal{Z}(f)$

$N(\mathcal{X})$: the number of rational points of $\mathcal{X}$

$g(\mathcal{X})$: the genus of $\mathcal{X}$

Hasse-Weil Bound:

If $\mathcal{X}$ is a projective, non-singular and absolutely irreducible (!) curve defined over $\mathbb{F}$, then

$$|\mathbb{F}| + 1 - 2g(\mathcal{X})\sqrt{|\mathbb{F}|} \leq N(\mathcal{X}) \leq |\mathbb{F}| + 1 + 2g(\mathcal{X})\sqrt{|\mathbb{F}|}.$$

Hasse-Weil Bound $\Longrightarrow$ sufficiently many rational points if $|\mathbb{F}|$ is sufficiently large compared to $g(\mathcal{X})$ (which depends on $\deg(f)$)!

$\mathcal{X} = \mathcal{Z}(f)$

$N(\mathcal{X})$: the number of rational points of $\mathcal{X}$

$g(\mathcal{X})$: the genus of $\mathcal{X}$

Hasse-Weil Bound:

If $\mathcal{X}$ is a projective, non-singular and absolutely irreducible (!) curve defined over $\mathbb{F}$, then

$$|\mathbb{F}| + 1 - 2g(\mathcal{X})\sqrt{|\mathbb{F}|} \leq N(\mathcal{X}) \leq |\mathbb{F}| + 1 + 2g(\mathcal{X})\sqrt{|\mathbb{F}|}.$$

Hasse-Weil Bound $\Longrightarrow$ sufficiently many rational points if $|\mathbb{F}|$ is sufficiently large compared to $g(\mathcal{X})$ (which depends on $\deg(f)$)!

Approach by the Hasse-Weil Bound

Given $R(X) \in \mathbb{F}[X]$, define $g(X,Y) = \frac{R(X)-R(Y)}{X-Y} \in \mathbb{F}[X,Y]$.

$\exists\, (\alpha,\beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha,\beta) = 0$

$\Longrightarrow R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$
$\Longrightarrow R(X)$ is not a permutation.

Common Approach:

(i) $g(X,Y)$ has an absolutely irreducible factor $f(X,Y)$ over $\mathbb{F}$.

(ii) $\mathcal{X} = \mathcal{Z}(f)$ is an absolutely irreducible curve over $\mathbb{F}$.

(iii) $\mathcal{UP}$: the number unwanted rational points (corresponding to ones at infinity + singular + on $X = Y$)

(iv) $|\mathbb{F}| = p^n$ is sufficiently large $\Longrightarrow N(\mathcal{X}) - \mathcal{UP} > 0$

$\Longrightarrow \exists$ a rational point $P = (\alpha,\beta) \in \mathcal{X}$ with $\alpha \neq \beta$

$\Longrightarrow \exists\, (\alpha,\beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha,\beta) = 0$.

Approach by the Hasse-Weil Bound

Given $R(X) \in \mathbb{F}[X]$, define $g(X,Y) = \frac{R(X)-R(Y)}{X-Y} \in \mathbb{F}[X,Y]$.

$\exists\ (\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha, \beta) = 0$

$\implies R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$
$\implies R(X)$ is not a permutation.

Common Approach:

(i) $g(X,Y)$ has an absolutely irreducible factor $f(X,Y)$ over $\mathbb{F}$.

(ii) $\mathcal{X} = \mathcal{Z}(f)$ is an absolutely irreducible curve over $\mathbb{F}$.

(iii) $\mathcal{UP}$: the number unwanted rational points (corresponding to ones at infinity + singular + on $X = Y$)

(iv) $|\mathbb{F}| = p^n$ is sufficiently large $\implies N(\mathcal{X}) - \mathcal{UP} > 0$
$\implies \exists$ a rational point $P = (\alpha, \beta) \in \mathcal{X}$ with $\alpha \neq \beta$
$\implies \exists\ (\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha, \beta) = 0$.

Approach by the Hasse-Weil Bound

Given $R(X) \in \mathbb{F}[X]$, define $g(X, Y) = \frac{R(X)-R(Y)}{X-Y} \in \mathbb{F}[X, Y]$.

$\exists\ (\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha, \beta) = 0$

$\implies R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$
$\implies R(X)$ is not a permutation.

Common Approach:

(i) $g(X, Y)$ has an absolutely irreducible factor $f(X, Y)$ over $\mathbb{F}$.

(ii) $\mathcal{X} = \mathcal{Z}(f)$ is an absolutely irreducible curve over $\mathbb{F}$.

(iii) $\mathcal{UP}$: the number unwanted rational points (corresponding to ones at infinity + singular + on $X = Y$)

(iv) $|\mathbb{F}| = p^n$ is sufficiently large $\implies N(\mathcal{X}) - \mathcal{UP} > 0$

$\implies \exists$ a rational point $P = (\alpha, \beta) \in \mathcal{X}$ with $\alpha \neq \beta$

$\implies \exists\ (\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha, \beta) = 0$.

Approach by the Hasse-Weil Bound

Given $R(X) \in \mathbb{F}[X]$, define $g(X,Y) = \frac{R(X)-R(Y)}{X-Y} \in \mathbb{F}[X,Y]$.

$\exists\ (\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha, \beta) = 0$

$\implies R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$
$\implies R(X)$ is not a permutation.

Common Approach:

(i) $g(X,Y)$ has an absolutely irreducible factor $f(X,Y)$ over $\mathbb{F}$.

(ii) $\mathcal{X} = \mathcal{Z}(f)$ is an absolutely irreducible curve over $\mathbb{F}$.

(iii) $\mathcal{UP}$: the number unwanted rational points (corresponding to ones at infinity + singular + on $X = Y$)

(iv) $|\mathbb{F}| = p^n$ is sufficiently large $\implies N(\mathcal{X}) - \mathcal{UP} > 0$
$\implies \exists$ a rational point $P = (\alpha, \beta) \in \mathcal{X}$ with $\alpha \neq \beta$
$\implies \exists\ (\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha, \beta) = 0$.

Approach by the Hasse-Weil Bound

Given $R(X) \in \mathbb{F}[X]$, define $g(X,Y) = \frac{R(X)-R(Y)}{X-Y} \in \mathbb{F}[X,Y]$.

$\exists\ (\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha, \beta) = 0$

$\Longrightarrow R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$
$\Longrightarrow R(X)$ is not a permutation.

Common Approach:

(i) $g(X,Y)$ has an absolutely irreducible factor $f(X,Y)$ over $\mathbb{F}$.

(ii) $\mathcal{X} = \mathcal{Z}(f)$ is an absolutely irreducible curve over $\mathbb{F}$.

(iii) $\mathcal{UP}$: the number unwanted rational points (corresponding to ones at infinity + singular + on $X = Y$)

(iv) $|\mathbb{F}| = p^n$ is sufficiently large $\Longrightarrow N(\mathcal{X}) - \mathcal{UP} > 0$
$\Longrightarrow \exists$ a rational point $P = (\alpha, \beta) \in \mathcal{X}$ with $\alpha \neq \beta$
$\Longrightarrow \exists\ (\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha, \beta) = 0$.

Approach by the Hasse-Weil Bound

Given $R(X) \in \mathbb{F}[X]$, define $g(X,Y) = \frac{R(X)-R(Y)}{X-Y} \in \mathbb{F}[X,Y]$.

$\exists\ (\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha, \beta) = 0$

$\implies R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$
$\implies R(X)$ is not a permutation.

Common Approach:

(i) $g(X,Y)$ has an absolutely irreducible factor $f(X,Y)$ over $\mathbb{F}$.

(ii) $\mathcal{X} = \mathcal{Z}(f)$ is an absolutely irreducible curve over $\mathbb{F}$.

(iii) $\mathcal{UP}$: the number unwanted rational points (corresponding to ones at infinity + singular + on $X = Y$)

(iv) $|\mathbb{F}| = p^n$ is sufficiently large $\implies N(\mathcal{X}) - \mathcal{UP} > 0$

$\implies \exists$ a rational point $P = (\alpha, \beta) \in \mathcal{X}$ with $\alpha \neq \beta$

$\implies \exists\ (\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha, \beta) = 0$.

Approach by the Hasse-Weil Bound

Given $R(X) \in \mathbb{F}[X]$, define $g(X,Y) = \frac{R(X)-R(Y)}{X-Y} \in \mathbb{F}[X,Y]$.

$\exists\ (\alpha,\beta) \in \mathbb{F}\times\mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha,\beta) = 0$

$\implies R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$
$\implies R(X)$ is not a permutation.

Common Approach:

(i) $g(X,Y)$ has an absolutely irreducible factor $f(X,Y)$ over $\mathbb{F}$.

(ii) $\mathcal{X} = \mathcal{Z}(f)$ is an absolutely irreducible curve over $\mathbb{F}$.

(iii) $\mathcal{UP}$: the number unwanted rational points (corresponding to ones at infinity + singular + on $X = Y$)

(iv) $|\mathbb{F}| = p^n$ is sufficiently large $\implies N(\mathcal{X}) - \mathcal{UP} > 0$
$\implies \exists$ a rational point $P = (\alpha,\beta) \in \mathcal{X}$ with $\alpha \neq \beta$
$\implies \exists\ (\alpha,\beta) \in \mathbb{F}\times\mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha,\beta) = 0$.

Approach by the Hasse-Weil Bound

Given $R(X) \in \mathbb{F}[X]$, define $g(X, Y) = \frac{R(X)-R(Y)}{X-Y} \in \mathbb{F}[X, Y]$.

$\exists\ (\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha, \beta) = 0$

$\implies R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$
$\implies R(X)$ is not a permutation.

Common Approach:

(i) $g(X, Y)$ has an absolutely irreducible factor $f(X, Y)$ over $\mathbb{F}$.

(ii) $\mathcal{X} = \mathcal{Z}(f)$ is an absolutely irreducible curve over $\mathbb{F}$.

(iii) $\mathcal{UP}$: the number unwanted rational points (corresponding to ones at infinity + singular + on $X = Y$)

(iv) $|\mathbb{F}| = p^n$ is sufficiently large $\implies N(\mathcal{X}) - \mathcal{UP} > 0$
$\implies \exists$ a rational point $P = (\alpha, \beta) \in \mathcal{X}$ with $\alpha \neq \beta$
$\implies \exists\ (\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ such that $\alpha \neq \beta$ and $g(\alpha, \beta) = 0$.

Different Approach

Remark: We can not apply the common approach for

$$R(X) = X^k - \gamma \mathrm{Tr}(X) = X^k - \gamma \left(X + X^p + \cdots + X^{p^{n-1}} \right)$$

as $\deg(R(X)) = p^{n-1}$!

Another Approach: We separate the multiplicative and the additive structure of the field to construct curves with many (affine) rational points.

Theorem:

$R(X)$ is not a permutation of $\mathbb{F}$ if $\gcd(k, p^n - 1) > 1$.

Different Approach

Remark: We can not apply the common approach for

$$R(X) = X^k - \gamma \mathrm{Tr}(X) = X^k - \gamma \left(X + X^p + \cdots + X^{p^{n-1}} \right)$$

as $\deg(R(X)) = p^{n-1}$!

Another Approach: We separate the multiplicative and the additive structure of the field to construct curves with many (affine) rational points.

Theorem:

$R(X)$ is not a permutation of $\mathbb{F}$ if $\gcd(k, p^n - 1) > 1$.

Different Approach

Remark: We can not apply the common approach for

$$R(X) = X^k - \gamma \mathrm{Tr}(X) = X^k - \gamma \left(X + X^p + \cdots + X^{p^{n-1}} \right)$$

as $\deg(R(X)) = p^{n-1}$!

Another Approach: We separate the multiplicative and the additive structure of the field to construct curves with many (affine) rational points.

Theorem:

$R(X)$ is not a permutation of $\mathbb{F}$ if $\gcd(k, p^n - 1) > 1$.

Idea of the proof:

Suppose that $\gamma \neq 0$.

Set $t = \gcd(k, p^n - 1) > 1$ and $H = \langle \zeta^t \rangle \leqslant \mathbb{F}_{p^n}^*$, where ζ is the primitive element of $\mathbb{F}_{p^n}$.

Recall: We consider the solutions of $\frac{1}{\gamma} X^k = \mathrm{Tr}(X) + c$ for $c \in \mathbb{F}_{p^n}$.

We define $f_c(X, Y) = \frac{1}{\gamma} X^k - \mathrm{Tr}(Y) - c$ and set $\mathcal{X}_c = \mathcal{Z}(f_c)$.

By Function Field Theory:

$f_c(X, Y)$ is absolutely irreducible over $\mathbb{F}_{p^n}$.

$\exists t p^{n-1}$ (affine) rational points of $\mathcal{X}_c$ for all $\eta \in \left(\frac{1}{\gamma} H\right) \cap (c + \mathbb{F}_p)$.

$\bigcup_{c \in \mathbb{F}_{p^n}} (c + \mathbb{F}_p) = \mathbb{F}_{p^n} \implies \exists c \in \mathbb{F}_{p^n}$ such that $N(\mathcal{X}_c) > p^n$.

Set $\mathcal{X} = \mathcal{X}_c$.

Idea of the proof:

Suppose that $\gamma \neq 0$.

Set $t = \gcd(k, p^n - 1) > 1$ and $H = \langle \zeta^t \rangle \leqslant \mathbb{F}_{p^n}^*$, where ζ is the primitive element of $\mathbb{F}_{p^n}$.

Recall: We consider the solutions of $\frac{1}{\gamma}X^k = \mathrm{Tr}(X) + c$ for $c \in \mathbb{F}_{p^n}$.

We define $f_c(X, Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c$ and set $\mathcal{X}_c = \mathcal{Z}(f_c)$.

By Function Field Theory:

$f_c(X, Y)$ is absolutely irreducible over $\mathbb{F}_{p^n}$.

$\exists tp^{n-1}$ (affine) rational points of $\mathcal{X}_c$ for all $\eta \in \left(\frac{1}{\gamma}H\right) \cap (c + \mathbb{F}_p)$.

$\bigcup_{c \in \mathbb{F}_{p^n}} (c + \mathbb{F}_p) = \mathbb{F}_{p^n} \implies \exists c \in \mathbb{F}_{p^n}$ such that $N(\mathcal{X}_c) > p^n$.

Set $\mathcal{X} = \mathcal{X}_c$.

Idea of the proof:

Suppose that $\gamma \neq 0$.

Set $t = \gcd(k, p^n - 1) > 1$ and $H = \langle \zeta^t \rangle \leqslant \mathbb{F}_{p^n}^*$, where ζ is the primitive element of $\mathbb{F}_{p^n}$.

Recall: We consider the solutions of $\frac{1}{\gamma}X^k = \mathrm{Tr}(X) + c$ for $c \in \mathbb{F}_{p^n}$.

We define $f_c(X, Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c$ and set $\mathcal{X}_c = \mathcal{Z}(f_c)$.

By Function Field Theory:

$f_c(X, Y)$ is absolutely irreducible over $\mathbb{F}_{p^n}$.

$\exists tp^{n-1}$ (affine) rational points of $\mathcal{X}_c$ for all $\eta \in \left(\frac{1}{\gamma}H\right) \cap (c + \mathbb{F}_p)$.

$\bigcup_{c \in \mathbb{F}_{p^n}} (c + \mathbb{F}_p) = \mathbb{F}_{p^n} \Longrightarrow \exists c \in \mathbb{F}_{p^n}$ such that $N(\mathcal{X}_c) > p^n$.

Set $\mathcal{X} = \mathcal{X}_c$.

Idea of the proof:

Suppose that $\gamma \neq 0$.

Set $t = \gcd(k, p^n - 1) > 1$ and $H = \langle \zeta^t \rangle \leqslant \mathbb{F}_{p^n}^*$, where ζ is the primitive element of $\mathbb{F}_{p^n}$.

Recall: We consider the solutions of $\frac{1}{\gamma}X^k = \mathrm{Tr}(X) + c$ for $c \in \mathbb{F}_{p^n}$.

We define $f_c(X, Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c$ and set $\mathcal{X}_c = \mathcal{Z}(f_c)$.

By Function Field Theory:

$f_c(X, Y)$ is absolutely irreducible over $\mathbb{F}_{p^n}$.

$\exists tp^{n-1}$ (affine) rational points of $\mathcal{X}_c$ for all $\eta \in \left(\frac{1}{\gamma}H\right) \cap (c + \mathbb{F}_p)$.

$\bigcup_{c \in \mathbb{F}_{p^n}} (c + \mathbb{F}_p) = \mathbb{F}_{p^n} \implies \exists c \in \mathbb{F}_{p^n}$ such that $N(\mathcal{X}_c) > p^n$.

Set $\mathcal{X} = \mathcal{X}_c$.

Idea of the proof:

Suppose that $\gamma \neq 0$.

Set $t = \gcd(k, p^n - 1) > 1$ and $H = \langle \zeta^t \rangle \leqslant \mathbb{F}_{p^n}^*$, where ζ is the primitive element of $\mathbb{F}_{p^n}$.

Recall: We consider the solutions of $\frac{1}{\gamma}X^k = \mathrm{Tr}(X) + c$ for $c \in \mathbb{F}_{p^n}$.

We define $f_c(X, Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c$ and set $\mathcal{X}_c = \mathcal{Z}(f_c)$.

By Function Field Theory:

$f_c(X, Y)$ is absolutely irreducible over $\mathbb{F}_{p^n}$.

$\exists tp^{n-1}$ (affine) rational points of $\mathcal{X}_c$ for all $\eta \in \left(\frac{1}{\gamma}H\right) \cap (c + \mathbb{F}_p)$.

$\bigcup_{c \in \mathbb{F}_{p^n}} (c + \mathbb{F}_p) = \mathbb{F}_{p^n} \Longrightarrow \exists c \in \mathbb{F}_{p^n}$ such that $N(\mathcal{X}_c) > p^n$.

Set $\mathcal{X} = \mathcal{X}_c$.

Recall:

$\mathcal{X} = \mathcal{Z}(f_c)$, where $f_c(X, Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c$

$R(X) = X^k - \gamma\mathrm{Tr}(X) \in \mathbb{F}_{p^n}$

Set $\mathcal{L} = \{\, \ell_d : Y = X + d \mid d \in \mathbb{F}_{p^n} \,\}$.

Remark: $\bigcup_{\ell_d \in \mathcal{L}} \ell_d \supseteq \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$

We have $|\mathcal{L}| = p^n$ and $N(\mathcal{X}) > p^n$.

$\Longrightarrow \exists d \in \mathbb{F}_{p^n}$ such that $\mathcal{X} \cap \ell_d$ has at least two rational points, say $(\alpha, \alpha + d)$ and $(\beta, \beta + d)$ with $\alpha \neq \beta$.

$\Longrightarrow \frac{1}{\gamma}\alpha^k - \mathrm{Tr}(\alpha + d) - c = \frac{1}{\gamma}\beta^k - \mathrm{Tr}(\beta + d) - c = 0.$

$\Longrightarrow \alpha^k - \gamma\mathrm{Tr}(\alpha) = \beta^k - \gamma\mathrm{Tr}(\beta) = \gamma c + \gamma\mathrm{Tr}(d).$

$\Longrightarrow R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$.

Recall:

$\mathcal{X} = \mathcal{Z}(f_c)$, where $f_c(X,Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c$

$R(X) = X^k - \gamma \mathrm{Tr}(X) \in \mathbb{F}_{p^n}$

Set $\mathcal{L} = \{\, \ell_d : Y = X + d \mid d \in \mathbb{F}_{p^n} \,\}$.

Remark: $\bigcup_{\ell_d \in \mathcal{L}} \ell_d \supseteq \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$

We have $|\mathcal{L}| = p^n$ and $N(\mathcal{X}) > p^n$.

$\implies \exists d \in \mathbb{F}_{p^n}$ such that $\mathcal{X} \cap \ell_d$ has at least two rational points, say $(\alpha, \alpha + d)$ and $(\beta, \beta + d)$ with $\alpha \neq \beta$.

$\implies \frac{1}{\gamma}\alpha^k - \mathrm{Tr}(\alpha + d) - c = \frac{1}{\gamma}\beta^k - \mathrm{Tr}(\beta + d) - c = 0.$

$\implies \alpha^k - \gamma\mathrm{Tr}(\alpha) = \beta^k - \gamma\mathrm{Tr}(\beta) = \gamma c + \gamma\mathrm{Tr}(d).$

$\implies R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$.

Recall:

$\mathcal{X} = \mathcal{Z}(f_c)$, where $f_c(X,Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c$

$R(X) = X^k - \gamma\mathrm{Tr}(X) \in \mathbb{F}_{p^n}$

Set $\mathcal{L} = \{\ \ell_d : Y = X + d \ \mid\ d \in \mathbb{F}_{p^n}\ \}$.

Remark: $\bigcup_{\ell_d \in \mathcal{L}} \ell_d \supseteq \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$

We have $|\mathcal{L}| = p^n$ and $N(\mathcal{X}) > p^n$.

$\implies \exists d \in \mathbb{F}_{p^n}$ such that $\mathcal{X} \cap \ell_d$ has at least two rational points, say $(\alpha, \alpha + d)$ and $(\beta, \beta + d)$ with $\alpha \neq \beta$.

$\implies \frac{1}{\gamma}\alpha^k - \mathrm{Tr}(\alpha + d) - c = \frac{1}{\gamma}\beta^k - \mathrm{Tr}(\beta + d) - c = 0.$

$\implies \alpha^k - \gamma\mathrm{Tr}(\alpha) = \beta^k - \gamma\mathrm{Tr}(\beta) = \gamma c + \gamma\mathrm{Tr}(d).$

$\implies R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$.

Recall:

$\mathcal{X} = \mathcal{Z}(f_c)$, where $f_c(X, Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c$

$R(X) = X^k - \gamma \mathrm{Tr}(X) \in \mathbb{F}_{p^n}$

Set $\mathcal{L} = \{ \ell_d : Y = X + d \mid d \in \mathbb{F}_{p^n} \}$.

Remark: $\bigcup_{\ell_d \in \mathcal{L}} \ell_d \supseteq \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$

We have $|\mathcal{L}| = p^n$ and $N(\mathcal{X}) > p^n$.

$\Longrightarrow \exists d \in \mathbb{F}_{p^n}$ such that $\mathcal{X} \cap \ell_d$ has at least two rational points, say $(\alpha, \alpha + d)$ and $(\beta, \beta + d)$ with $\alpha \neq \beta$.

$\Longrightarrow \frac{1}{\gamma}\alpha^k - \mathrm{Tr}(\alpha + d) - c = \frac{1}{\gamma}\beta^k - \mathrm{Tr}(\beta + d) - c = 0.$

$\Longrightarrow \alpha^k - \gamma\mathrm{Tr}(\alpha) = \beta^k - \gamma\mathrm{Tr}(\beta) = \gamma c + \gamma\mathrm{Tr}(d).$

$\Longrightarrow R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$.

Recall:

$\mathcal{X} = \mathcal{Z}(f_c)$, where $f_c(X, Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c$

$R(X) = X^k - \gamma\mathrm{Tr}(X) \in \mathbb{F}_{p^n}$

Set $\mathcal{L} = \{\, \ell_d : Y = X + d \mid d \in \mathbb{F}_{p^n} \,\}$.

Remark: $\bigcup_{\ell_d \in \mathcal{L}} \ell_d \supseteq \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$

We have $|\mathcal{L}| = p^n$ and $N(\mathcal{X}) > p^n$.

$\implies \exists d \in \mathbb{F}_{p^n}$ such that $\mathcal{X} \cap \ell_d$ has at least two rational points, say $(\alpha, \alpha + d)$ and $(\beta, \beta + d)$ with $\alpha \neq \beta$.

$\implies \frac{1}{\gamma}\alpha^k - \mathrm{Tr}(\alpha + d) - c = \frac{1}{\gamma}\beta^k - \mathrm{Tr}(\beta + d) - c = 0.$

$\implies \alpha^k - \gamma\mathrm{Tr}(\alpha) = \beta^k - \gamma\mathrm{Tr}(\beta) = \gamma c + \gamma\mathrm{Tr}(d).$

$\implies R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$.

Recall:

$\mathcal{X} = \mathcal{Z}(f_c)$, where $f_c(X, Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c$

$R(X) = X^k - \gamma\mathrm{Tr}(X) \in \mathbb{F}_{p^n}$

Set $\mathcal{L} = \{\, \ell_d : Y = X + d \mid d \in \mathbb{F}_{p^n} \,\}$.

Remark: $\bigcup_{\ell_d \in \mathcal{L}} \ell_d \supseteq \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$

We have $|\mathcal{L}| = p^n$ and $N(\mathcal{X}) > p^n$.

$\implies \exists d \in \mathbb{F}_{p^n}$ such that $\mathcal{X} \cap \ell_d$ has at least two rational points, say $(\alpha, \alpha + d)$ and $(\beta, \beta + d)$ with $\alpha \neq \beta$.

$\implies \frac{1}{\gamma}\alpha^k - \mathrm{Tr}(\alpha + d) - c = \frac{1}{\gamma}\beta^k - \mathrm{Tr}(\beta + d) - c = 0.$

$\implies \alpha^k - \gamma\mathrm{Tr}(\alpha) = \beta^k - \gamma\mathrm{Tr}(\beta) = \gamma c + \gamma\mathrm{Tr}(d).$

$\implies R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$.

Recall:

$\mathcal{X} = \mathcal{Z}(f_c)$, where $f_c(X, Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c$

$R(X) = X^k - \gamma\mathrm{Tr}(X) \in \mathbb{F}_{p^n}$

Set $\mathcal{L} = \{\ \ell_d : Y = X + d \ \mid\ d \in \mathbb{F}_{p^n}\ \}$.

Remark: $\bigcup_{\ell_d \in \mathcal{L}} \ell_d \supseteq \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$

We have $|\mathcal{L}| = p^n$ and $N(\mathcal{X}) > p^n$.

$\implies \exists d \in \mathbb{F}_{p^n}$ such that $\mathcal{X} \cap \ell_d$ has at least two rational points, say $(\alpha, \alpha + d)$ and $(\beta, \beta + d)$ with $\alpha \neq \beta$.

$\implies \frac{1}{\gamma}\alpha^k - \mathrm{Tr}(\alpha + d) - c = \frac{1}{\gamma}\beta^k - \mathrm{Tr}(\beta + d) - c = 0.$

$\implies \alpha^k - \gamma\mathrm{Tr}(\alpha) = \beta^k - \gamma\mathrm{Tr}(\beta) = \gamma c + \gamma\mathrm{Tr}(d).$

$\implies R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$.

Recall:

$\mathcal{X} = \mathcal{Z}(f_c)$, where $f_c(X,Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c$

$R(X) = X^k - \gamma\mathrm{Tr}(X) \in \mathbb{F}_{p^n}$

Set $\mathcal{L} = \{\, \ell_d : Y = X + d \mid d \in \mathbb{F}_{p^n} \,\}$.

Remark: $\bigcup_{\ell_d \in \mathcal{L}} \ell_d \supseteq \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$

We have $|\mathcal{L}| = p^n$ and $N(\mathcal{X}) > p^n$.

$\implies \exists d \in \mathbb{F}_{p^n}$ such that $\mathcal{X} \cap \ell_d$ has at least two rational points, say $(\alpha, \alpha + d)$ and $(\beta, \beta + d)$ with $\alpha \neq \beta$.

$\implies \frac{1}{\gamma}\alpha^k - \mathrm{Tr}(\alpha + d) - c = \frac{1}{\gamma}\beta^k - \mathrm{Tr}(\beta + d) - c = 0.$

$\implies \alpha^k - \gamma\mathrm{Tr}(\alpha) = \beta^k - \gamma\mathrm{Tr}(\beta) = \gamma c + \gamma\mathrm{Tr}(d).$

$\implies R(\alpha) = R(\beta)$ such that $\alpha \neq \beta$.

$\square$

Remark: We can generalize the result for any prime power!

Theorem:

Let $q = p^m$ and $R(X) = X^k - \gamma \mathrm{Tr}_m^n(X) \in \mathbb{F}_{q^n}[X]$, where $\mathrm{Tr}_m^n(X) = X + X^q + \cdots + X^{q^{n-1}}$, $m, n, k \in \mathbb{Z}_{>0}$ and $\gamma \in \mathbb{F}_{q^n}$. If $\gcd(k, q^n - 1) > 1$, then $R(X)$ is not a permutation of $\mathbb{F}_{q^n}$.

Corollary:

(i) Let $q = 2^m$ with $m = 2s$, $s \geq 1$, and $R(X) = X^{3t} - \gamma \mathrm{Tr}_m^n(X) \in \mathbb{F}_{q^n}[X]$. Then $R(X)$ is not a permutation of $\mathbb{F}_{q^n}$ for all $n \geq 1$.

(ii) Let p be an odd prime, $q = p^m$, $m \geq 1$, and $R(X) = X^{2t} - \gamma \mathrm{Tr}_m^n(X) \in \mathbb{F}_{q^n}[X]$. Then $R(X)$ is not a permutation of $\mathbb{F}_{q^n}$ for all $n \geq 1$.

Remark: We can generalize the result for any prime power!

Theorem:

Let $q = p^m$ and $R(X) = X^k - \gamma \mathrm{Tr}_m^n(X) \in \mathbb{F}_{q^n}[X]$, where $\mathrm{Tr}_m^n(X) = X + X^q + \cdots + X^{q^{n-1}}$, $m, n, k \in \mathbb{Z}_{>0}$ and $\gamma \in \mathbb{F}_{q^n}$. If $\gcd(k, q^n - 1) > 1$, then $R(X)$ is not a permutation of $\mathbb{F}_{q^n}$.

Corollary:

(i) Let $q = 2^m$ with $m = 2s$, $s \geq 1$, and $R(X) = X^{3t} - \gamma \mathrm{Tr}_m^n(X) \in \mathbb{F}_{q^n}[X]$. Then $R(X)$ is not a permutation of $\mathbb{F}_{q^n}$ for all $n \geq 1$.

(ii) Let p be an odd prime, $q = p^m$, $m \geq 1$, and $R(X) = X^{2t} - \gamma \mathrm{Tr}_m^n(X) \in \mathbb{F}_{q^n}[X]$. Then $R(X)$ is not a permutation of $\mathbb{F}_{q^n}$ for all $n \geq 1$.

Remark: We can generalize the result for any prime power!

Theorem:

Let $q = p^m$ and $R(X) = X^k - \gamma \mathrm{Tr}_m^n(X) \in \mathbb{F}_{q^n}[X]$, where $\mathrm{Tr}_m^n(X) = X + X^q + \cdots + X^{q^{n-1}}$, $m, n, k \in \mathbb{Z}_{>0}$ and $\gamma \in \mathbb{F}_{q^n}$. If $\gcd(k, q^n - 1) > 1$, then $R(X)$ is not a permutation of $\mathbb{F}_{q^n}$.

Corollary:

(i) Let $q = 2^m$ with $m = 2s$, $s \geq 1$, and $R(X) = X^{3t} - \gamma \mathrm{Tr}_m^n(X) \in \mathbb{F}_{q^n}[X]$. Then $R(X)$ is not a permutation of $\mathbb{F}_{q^n}$ for all $n \geq 1$.

(ii) Let p be an odd prime, $q = p^m$, $m \geq 1$, and $R(X) = X^{2t} - \gamma \mathrm{Tr}_m^n(X) \in \mathbb{F}_{q^n}[X]$. Then $R(X)$ is not a permutation of $\mathbb{F}_{q^n}$ for all $n \geq 1$.

Thanks for your attention!