On Permutation Polynomials of Prescribed Shape

Amir Akbary

University of Lethbridge

July 2010
Permutation Polynomials

Definition

A polynomial \( f \in \mathbb{F}_q[x] \) is called a permutation polynomial of \( \mathbb{F}_q \) if the associated polynomial function \( f : \mathbb{F}_q \to \mathbb{F}_q \) from \( \mathbb{F}_q \) to \( \mathbb{F}_q \) is a permutation of \( \mathbb{F}_q \).

Example

1. \( f(x) = ax + b, a \neq 0 \) is a permutation polynomial.

2. \( f(x) = x^n \) is a permutation polynomial of \( \mathbb{F}_q \) \( \iff \) \((n, q - 1) = 1\).
Permutation Polynomials

- $F_q := \text{finite field of } q = p^m \text{ elements.}$
Permutation Polynomials

- $\mathbb{F}_q :=$ finite field of $q = p^m$ elements.
- **Definition** A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* of $\mathbb{F}_q$ if the associated polynomial function $f : c \to f(c)$ from $\mathbb{F}_q$ to $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$. 

Example 1: $f(x) = ax + b$, $a \neq 0$ is a permutation polynomial.

Example 2: $f(x) = x^n$ is a permutation polynomial of $\mathbb{F}_q \iff (n, q - 1) = 1$. 

Two Problems
- Counting permutation polynomials of $\mathbb{F}_q$
- Constructing permutation polynomials of $\mathbb{F}_q$. 

Permutation Polynomials

- \( \mathbb{F}_q :\) finite field of \( q = p^m \) elements.

- **Definition** A polynomial \( f \in \mathbb{F}_q[x] \) is called a *permutation polynomial* of \( \mathbb{F}_q \) if the associated polynomial function \( f : c \rightarrow f(c) \) from \( \mathbb{F}_q \) to \( \mathbb{F}_q \) is a permutation of \( \mathbb{F}_q \).

- **Example**
  1. \( f(x) = ax + b, \ a \neq 0 \) is a permutation polynomial.
Permutation Polynomials

- $\mathbb{F}_q := \text{finite field of } q = p^m \text{ elements.}$
- **Definition** A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* of $\mathbb{F}_q$ if the associated polynomial function $f : c \to f(c)$ from $\mathbb{F}_q$ to $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$.
- **Example**
  1. $f(x) = ax + b$, $a \neq 0$ is a permutation polynomial.
  2. $f(x) = x^n$ is a permutation polynomial of $\mathbb{F}_q$
     $\iff (n, q - 1) = 1$. 

Permutation Polynomials

- $\mathbb{F}_q :=$ finite field of $q = p^m$ elements.

- **Definition** A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* of $\mathbb{F}_q$ if the associated polynomial function $f : c \rightarrow f(c)$ from $\mathbb{F}_q$ to $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$.

- **Example**
  1. $f(x) = ax + b$, $a \neq 0$ is a permutation polynomial.
  2. $f(x) = x^n$ is a permutation polynomial of $\mathbb{F}_q$ if
     \[ (n, q - 1) = 1. \]

- **Two Problems** Counting permutation polynomials of $\mathbb{F}_q$ and Constructing permutation polynomials of $\mathbb{F}_q$. 
By Lagrange's interpolation, every mapping $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ can be expressed uniquely by a polynomial of degree $\leq q - 1$.

$g(x) = \sum_{c \in \mathbb{F}_q} f(c)(1 - (x - c)^{q-1})$

We assume each polynomial defined over $\mathbb{F}_q$ has degree at most $(q-1)$ because $x^q = x$ for each $x \in \mathbb{F}_q$.

(Kayal, 2004) There exists a deterministic polynomial-time algorithm that given a polynomial $f(x)$ determines whether it is a permutation polynomial or not.

Permutation polynomials are rare.

$$\lim_{q \to \infty} \frac{q!}{q^q} = 0$$
By Lagrange’s interpolation, every mapping $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ can be expressed uniquely by a polynomial of degree $\leq q - 1$. 

\[
\sum_{c \in \mathbb{F}_q} f(c)(1 - (x - c)^q - 1)
\]

We assume each polynomial defined over $\mathbb{F}_q$ has degree at most $(q - 1)$ because $x^q = x$ for each $x \in \mathbb{F}_q$. 

(Kayal, 2004) There exists a deterministic polynomial-time algorithm that given a polynomial $f(x)$ determines whether it is a permutation polynomial or not. 

Permutation polynomials are rare.

\[
\lim_{q \to \infty} \frac{q!}{q^q} = 0
\]
By Lagrange’s interpolation, every mapping $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ can be expressed uniquely by a polynomial of degree $\leq q - 1$.

\[
g(x) = \sum_{c \in \mathbb{F}_q} f(c) \left(1 - (x - c)^{q-1}\right)
\]
By Lagrange’s interpolation, every mapping \( f : \mathbb{F}_q \rightarrow \mathbb{F}_q \) can be expressed uniquely by a polynomial of degree \( \leq q - 1 \).

\[
g(x) = \sum_{c \in \mathbb{F}_q} f(c) \left(1 - (x - c)^{q-1}\right)
\]

We assume each polynomial defined over \( \mathbb{F}_q \) has degree at most \( (q - 1) \) because \( x^q = x \) for each \( x \in \mathbb{F}_q \).
Counting and Constructing Permutation Polynomials

- By Lagrange’s interpolation, every mapping $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ can be expressed uniquely by a polynomial of degree $\leq q - 1$.

$$g(x) = \sum_{c \in \mathbb{F}_q} f(c) \left(1 - (x - c)^{q-1}\right)$$

- We assume each polynomial defined over $\mathbb{F}_q$ has degree at most $(q - 1)$ because $x^q = x$ for each $x \in \mathbb{F}_q$.

- (Kayal, 2004) There exists a deterministic polynomial-time algorithm that given a polynomial $f(x)$ determines whether it is a permutation polynomial or not.
Counting and Constructing Permutation Polynomials

By Lagrange’s interpolation, every mapping $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ can be expressed uniquely by a polynomial of degree $\leq q - 1$.

$$g(x) = \sum_{c \in \mathbb{F}_q} f(c) \left(1 - (x - c)^{q-1}\right)$$

We assume each polynomial defined over $\mathbb{F}_q$ has degree at most $(q - 1)$ because $x^q = x$ for each $x \in \mathbb{F}_q$.

(Kayal, 2004) There exists a deterministic polynomial-time algorithm that given a polynomial $f(x)$ determines whether it is a permutation polynomial or not.

Permutation polynomials are rare.
Counting and Constructing Permutation Polynomials

- By Lagrange’s interpolation, every mapping $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ can be expressed uniquely by a polynomial of degree $\leq q - 1$.

$$g(x) = \sum_{c \in \mathbb{F}_q} f(c) \left(1 - (x - c)^{q-1}\right)$$

- We assume each polynomial defined over $\mathbb{F}_q$ has degree at most $(q - 1)$ because $x^q = x$ for each $x \in \mathbb{F}_q$.

- (Kayal, 2004) There exists a deterministic polynomial-time algorithm that given a polynomial $f(x)$ determines whether it is a permutation polynomial or not.

- Permutation polynomials are rare.

- $$\lim_{q \rightarrow \infty} \frac{q!}{q^q} = 0$$
Analogy With Primes

There is a deterministic polynomial time for primality testing.

The density of the set of primes in the set of integers is zero.

There are many open problems regarding primes of prescribed shapes, such as Mersenne primes, Fermat primes, and twin primes.

Similarly it is not always easy to count and construct permutation polynomials of a prescribed shape.
Analogy With Primes

- There is a deterministic polynomial time for primality testing.
Analogy With Primes

- There is a deterministic polynomial time for primality testing.
- The density of the set of primes in the set of integers is zero.


Analogy With Primes

- There is a deterministic polynomial time for primality testing.
- The density of the set of primes in the set of integers is zero.
- There are many open problems regarding primes of prescribed shapes, such as Mersenne primes, Fermat primes, and twin primes.
Analogy With Primes

- There is a deterministic polynomial time for primality testing.
- The density of the set of primes in the set of integers is zero.
- There are many open problems regarding primes of prescribed shapes, such as Mersenne primes, Fermat primes, and twin primes.
- Similarly it is not always easy to count and construct permutation polynomials of a prescribed shape.
Hermite Criterion

$f \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if

(i) $f$ has exactly one root in $\mathbb{F}_q$.

(ii) For each integer $t$ with $1 \leq t < q - 1$, $t \not\equiv 0 \pmod{p}$, the reduction of $(f(x))^t \mod (x^q - x)$ has degree $\leq q - 2$.

Corollary

If $d > 1$ is a divisor of $q - 1$ then there is no permutation polynomial of $\mathbb{F}_q$ of degree $d$. 
Hermite Criterion

- (Hermite, 1863) \( f \in \mathbb{F}_q[x] \) is a permutation polynomial if and only if
  
  (i) \( f \) has exactly one root in \( \mathbb{F}_q \).
  
  (ii) For each integer \( t \) with \( 1 \leq t < q - 1 \), \( t \not\equiv 0 \pmod{p} \), the reduction of \( (f(x))^t \mod (x^q - x) \) has degree \( \leq q - 2 \).
Hermite Criterion

- (Hermite, 1863) $f \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if
  (i) $f$ has exactly one root in $\mathbb{F}_q$. 

Corollary

If $d > 1$ is a divisor of $q - 1$ then there is no permutation polynomial of $\mathbb{F}_q$ of degree $d$. 

Hermite Criterion

- (Hermite, 1863) $f \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if
  (i) $f$ has exactly one root in $\mathbb{F}_q$.
  (ii) For each integer $t$ with $1 \leq t < q - 1$, $t \not\equiv 0 \pmod{p}$, the reduction of $(f(x))^t \mod (x^q - x)$ has degree $\leq q - 2$. 

Corollary

If $d > 1$ is a divisor of $q - 1$ then there is no permutation polynomial of $\mathbb{F}_q$ of degree $d$. 

Hermite Criterion

- (Hermite, 1863) \( f \in \mathbb{F}_q[x] \) is a permutation polynomial if and only if
  (i) \( f \) has exactly one root in \( \mathbb{F}_q \).
  (ii) For each integer \( t \) with \( 1 \leq t < q - 1 \), \( t \not\equiv 0 \pmod{p} \), the reduction of \( (f(x))^t \mod (x^q - x) \) has degree \( \leq q - 2 \).

- Corollary If \( d > 1 \) is a divisor of \( q - 1 \) then there is no permutation polynomial of \( \mathbb{F}_q \) of degree \( d \).
Counting Permutation Polynomials by Degree

Problem (Lidl-Mullen) Let $N_d(q)$ denote the number of permutation polynomials of $F_q$ which have degree $d$.

We have the trivial boundary conditions:

(i) $N_{1}(q) = q(q-1)$.

(ii) $N_{d}(q) = 0$ if $d$ is a divisor of $(q-1)$ larger than 1.

(iii) $\sum N_{d}(q) = q!$ where the sum is over all $1 \leq d < q-1$ such that $d$ is either 1 or it is not a divisor of $(q-1)$.

Find $N_{d}(q)$. 
Problem (Lidl-Mullen) Let $N_d(q)$ denote the number of permutation polynomials of $\mathbb{F}_q$ which have degree $d$. 

(i) $N_1(q) = q(q-1)$.

(ii) $N_d(q) = 0$ if $d$ is a divisor of $(q-1)$ larger than 1.

(iii) $\sum N_d(q) = q!$ where the sum is over all $1 \leq d < q-1$ such that $d$ is either 1 or it is not a divisor of $(q-1)$. 

Find $N_d(q)$. 
Counting Permutation Polynomials by Degree

Problem (Lidl-Mullen) Let $N_d(q)$ denote the number of permutation polynomials of $\mathbb{F}_q$ which have degree $d$. We have the trivial boundary conditions:

(i) $N_1(q) = q(q - 1)$. 


Problem (Lidl-Mullen) Let $N_d(q)$ denote the number of permutation polynomials of $\mathbb{F}_q$ which have degree $d$. We have the trivial boundary conditions:

(i) $N_1(q) = q(q - 1)$.
(ii) $N_d(q) = 0$ if $d$ is a divisor of $(q - 1)$ larger than 1.
Problem (Lidl-Mullen) Let $N_d(q)$ denote the number of permutation polynomials of $\mathbb{F}_q$ which have degree $d$. We have the trivial boundary conditions:

(i) $N_1(q) = q(q - 1)$.

(ii) $N_d(q) = 0$ if $d$ is a divisor of $(q - 1)$ larger than 1.

(iii) $\sum N_d(q) = q!$ where the sum is over all $1 \leq d < q - 1$ such that $d$ is either 1 or it is not a divisor of $(q - 1)$. 
Problem (Lidl-Mullen) Let $N_d(q)$ denote the number of permutation polynomials of $\mathbb{F}_q$ which have degree $d$. We have the trivial boundary conditions:

(i) $N_1(q) = q(q - 1)$.

(ii) $N_d(q) = 0$ if $d$ is a divisor of $(q - 1)$ larger than 1.

(iii) $\sum N_d(q) = q!$ where the sum is over all $1 \leq d < q - 1$ such that $d$ is either 1 or it is not a divisor of $(q - 1)$. Find $N_d(q)$. 
Some Known Results

\[
N_p - 2 \left( \frac{p}{p} \right) \sim (1 - \frac{1}{p})^p \text{ as } p \to \infty.
\]

Almost all permutation polynomials of \( F_p \) have degree \( p - 2 \).

Konyagin and Pappalardi (2002)

\[
\left| N_q - 2 \left( \frac{q}{q} \right) - \varphi(q) q^q \right| \leq \sqrt{2e\pi q^2}.
\]
Some Known Results

- Das (2002) $N_{p-2}(p) \sim (1 - \frac{1}{p})p!$ as $p \to \infty$. 
Some Known Results

- **Das (2002)** $N_{p-2}(p) \sim (1 - \frac{1}{p})p!$ as $p \to \infty$.
- Almost all permutation polynomials of $\mathbb{F}_p$ have degree $p - 2$. 
Some Known Results

- **Das (2002)** \( N_{p-2}(p) \sim (1 - \frac{1}{p})p! \) as \( p \to \infty \).
- Almost all permutation polynomials of \( \mathbb{F}_p \) have degree \( p - 2 \).
- **Konyagin and Pappalardi (2002)**

\[
\left| N_{q-2}(q) - \frac{\varphi(q)}{q} q! \right| \leq \sqrt{\frac{2e}{\pi}} q^{\frac{3}{2}}.
\]
Terminology

- $g(x) \in \mathbb{F}_q[x]$ is a monic polynomial of degree $\leq q - 1$ with $g(0) = 0$.
- $r$ is the vanishing order of $g(x)$ at zero.
- Let $f_1(x) := g(x)/x^r$.
- Let $s$ be the largest divisor of $q - 1$ with the property that there exists a polynomial $f(x)$ of degree $\deg(f_1)/s$ such that $f_1(x) = f(x^s)$.
- $\ell = (q - 1)/s$.
- We call $\ell$ the index of $g$.

Any polynomial $h(x) \in \mathbb{F}_q[x]$ of degree $\leq q - 1$ can be written uniquely as $a(x^r f(x^{(q - 1)/\ell})) + b$. 
Terminology

- $g(x) \in \mathbb{F}_q[x]$ is a monic polynomial of degree $\leq q - 1$ with $g(0) = 0$. 
Terminology

- $g(x) \in \mathbb{F}_q[x]$ is a monic polynomial of degree $\leq q - 1$ with $g(0) = 0$.
- $r$ is the vanishing order of $g(x)$ at zero.
Terminology

- $g(x) \in \mathbb{F}_q[x]$ is a monic polynomial of degree $\leq q - 1$ with $g(0) = 0$.
- $r$ is the vanishing order of $g(x)$ at zero.
- Let $f_1(x) := g(x)/x^r$. 
Terminology

- $g(x) \in \mathbb{F}_q[x]$ is a monic polynomial of degree $\leq q - 1$ with $g(0) = 0$.
- $r$ is the vanishing order of $g(x)$ at zero.
- Let $f_1(x) := g(x)/x^r$.
- Let $s$ be the largest divisor of $q - 1$ with the property that there exists a polynomial $f(x)$ of degree $\deg(f_1)/s$ such that $f_1(x) = f(x^s)$.

\[ \ell = \frac{q - 1}{s} \]

We call $\ell$ the index of $g$. Any polynomial $h(x) \in \mathbb{F}_q[x]$ of degree $\leq q - 1$ can be written uniquely as $a(x^r f(x) \left( \frac{q - 1}{\ell} \right)) + b$. 
Terminology

- $g(x) \in \mathbb{F}_q[x]$ is a monic polynomial of degree $\leq q - 1$ with $g(0) = 0$.
- $r$ is the vanishing order of $g(x)$ at zero.
- Let $f_1(x) := g(x)/x^r$.
- Let $s$ be the largest divisor of $q - 1$ with the property that there exists a polynomial $f(x)$ of degree $\deg(f_1)/s$ such that $f_1(x) = f(x^s)$.
- $\ell = (q - 1)/s$. 

g(x) ∈ \mathbb{F}_q[x] is a monic polynomial of degree ≤ q − 1 with g(0) = 0.

r is the vanishing order of g(x) at zero.

Let \( f_1(x) := \frac{g(x)}{x^r} \).

Let s be the largest divisor of q − 1 with the property that there exists a polynomial f(x) of degree \( \deg(f_1)/s \) such that \( f_1(x) = f(x^s) \).

\( \ell = (q - 1)/s \).

We call \( \ell \) the index of g.
Terminology

- \( g(x) \in \mathbb{F}_q[x] \) is a monic polynomial of degree \( \leq q - 1 \) with \( g(0) = 0 \).
- \( r \) is the vanishing order of \( g(x) \) at zero.
- Let \( f_1(x) := g(x)/x^r \).
- Let \( s \) be the largest divisor of \( q - 1 \) with the property that there exists a polynomial \( f(x) \) of degree \( \deg(f_1)/s \) such that \( f_1(x) = f(x^s) \).
- \( \ell = (q - 1)/s \).
- We call \( \ell \) the index of \( g \).
- Any polynomial \( h(x) \in \mathbb{F}_q[x] \) of degree \( \leq q - 1 \) can be written uniquely as
  \[
a(x^r f(x^{(q-1)/\ell})) + b.
  \]
Example

In $\mathbb{F}_{17}$ we have

\begin{align*}
h(x) & = 3 \cdot x^{15} + 6x^9 + 12x^3 + 5 \\
& = 3 \cdot x^3(x^{12} + 2x^6 + 4) + 5
\end{align*}
Example

In $\mathbb{F}_{17}$ we have

\[
h(x) = 3 \cdot x^{15} + 6 \cdot x^9 + 12 \cdot x^3 + 5 \\
= 3 \cdot x^3 \cdot (x^9 + 2 \cdot x^6 + 4) + 5
\]

$(17 - 1, 12, 6) = 2.$
Example

In \( \mathbb{F}_{17} \) we have

\[
h(x) = 3x^{15} + 6x^9 + 12x^3 + 5
\]
\[
= 3x^3(x^{12} + 2x^6 + 4) + 5
\]

\((17 - 1, 12, 6) = 2.\)

\[
h(x) = 3x^3((x^2)^6 + 2(x^2)^3 + 4) + 5
\]
\[
= 3x^3f(x^2) + 5,
\]
Example

In $\mathbb{F}_{17}$ we have

$$h(x) = 3x^{15} + 6x^9 + 12x^3 + 5$$

$$= 3x^3(x^{12} + 2x^6 + 4) + 5$$

$$(17 - 1, 12, 6) = 2.$$ 

$$h(x) = 3x^3((x^2)^6 + 2(x^2)^3 + 4) + 5$$

$$= 3x^3f(x^2) + 5,$$

where $f(x) = x^6 + 2x^3 + 4$. So $\ell = 8$ and

$$h(x) = 3x^3f(x^{\frac{17-1}{8}}) + 5.$$
Rogers-Dickson Polynomials

\[ \text{Rogers-Dickson} \ x^r_f(x^{q-1}) \ell \text{ is a permutation polynomial if and only if } (r, q-1) = 1, \text{ and } f(x^{q-1}) \text{ has no non-zero root in } \mathbb{F}_{q^\ell}. \]
Rogers-Dickson Polynomials

- (Rogers-Dickson) $x^r f\left(x^{\frac{q-1}{\ell}}\right)^\ell$ is a permutation polynomial if and only if $(r, q - 1) = 1$, and $f\left(x^{\frac{q-1}{\ell}}\right)$ has no non-zero root in $\mathbb{F}_q$. 
Let $\ell \geq 2$ be a divisor of $q - 1$. Let $s := (q - 1)/\ell$. Let $m, r$ be positive integers, and $\bar{e} = (e_1, \ldots, e_m)$ be an $m$-tuple of integers that satisfy the following conditions:

(i) $0 < e_1 < e_2 \cdots < e_m \leq \ell - 1$,

(ii) $(e_1, \ldots, e_m, \ell) = 1$,

(iii) $r + e_ms \leq q - 1$.

For a tuple $\bar{a} := (a_1, \ldots, a_m) \in (F^*_q)^m$, we let

$$g_{\bar{a}r, \bar{e}}(x) := x^r x^{e_ms} + a_1 x^{e_m - 1} s + \cdots + a_{m - 1} x^{e_1} s + a_m.$$

If $g_{\bar{a}r, \bar{e}}(x)$ is a permutation polynomial then $(r, s) = 1$. 

Notations
Let $\ell \geq 2$ be a divisor of $q - 1$. Let $s := (q - 1)/\ell$. Let $m, r$ be positive integers, and $\bar{e} = (e_1, \ldots, e_m)$ be an $m$-tuple of integers that satisfy the following conditions:
Let $\ell \geq 2$ be a divisor of $q - 1$. Let $s := (q - 1)/\ell$. Let $m$, $r$ be positive integers, and $\bar{e} = (e_1, \ldots, e_m)$ be an $m$-tuple of integers that satisfy the following conditions:

(i) $0 < e_1 < e_2 \cdots < e_m \leq \ell - 1$, 

(ii) $(e_1, \ldots, e_m, \ell) = 1$, 

(iii) $r + e_m s \leq q - 1$. 

For a tuple $\bar{a} := (a_1, \ldots, a_m) \in (\mathbb{F}_q^*)^m$, we let $g_{\bar{a}, \bar{e}}(x) := x^r (x^{e_m s} + a_1 x^{e_{m-1} s} + \cdots + a_{m-1} x^{e_1 s} + a_m)$. 

If $g_{\bar{a}, \bar{e}}(x)$ is a permutation polynomial then $(r, s) = 1$. 

Notations
Let $\ell \geq 2$ be a divisor of $q - 1$. Let $s := (q - 1)/\ell$. Let $m, r$ be positive integers, and $\bar{e} = (e_1, \ldots, e_m)$ be an $m$-tuple of integers that satisfy the following conditions:

(i) $0 < e_1 < e_2 \cdots < e_m \leq \ell - 1$,
(ii) $(e_1, \ldots, e_m, \ell) = 1$, 

Let $\ell \geq 2$ be a divisor of $q - 1$. Let $s := (q - 1)/\ell$. Let $m$, $r$ be positive integers, and $\overline{e} = (e_1, \ldots, e_m)$ be an $m$-tuple of integers that satisfy the following conditions:

(i) $0 < e_1 < e_2 \cdots < e_m \leq \ell - 1$,
(ii) $(e_1, \ldots, e_m, \ell) = 1$,
(iii) $r + e_ms \leq q - 1$. 
Let $\ell \geq 2$ be a divisor of $q - 1$. Let $s := (q - 1)/\ell$. Let $m$, $r$ be positive integers, and $\vec{e} = (e_1, \ldots, e_m)$ be an $m$-tuple of integers that satisfy the following conditions:

(i) $0 < e_1 < e_2 \cdots < e_m \leq \ell - 1$,
(ii) $(e_1, \ldots, e_m, \ell) = 1$,
(iii) $r + e_ms \leq q - 1$.

For a tuple $\vec{a} := (a_1, \ldots, a_m) \in (\mathbb{F}_q^*)^m$, we let

$$g_{r, \vec{e}}(x) := x^r \left( x^{e_ms} + a_1 x^{e_m-1s} + \cdots + a_{m-1} x^{es} + a_m \right).$$
Notations

Let $\ell \geq 2$ be a divisor of $q - 1$. Let $s := (q - 1)/\ell$. Let $m$, $r$ be positive integers, and $\bar{e} = (e_1, \ldots, e_m)$ be an $m$-tuple of integers that satisfy the following conditions:

(i) $0 < e_1 < e_2 \cdots < e_m \leq \ell - 1$,
(ii) $(e_1, \ldots, e_m, \ell) = 1$,
(iii) $r + e_ms \leq q - 1$.

For a tuple $\bar{a} := (a_1, \ldots, a_m) \in (\mathbb{F}_q^*)^m$, we let

$$g_{\bar{r}, \bar{e}}(x) := x^r (x^{e_ms} + a_1 x^{e_{m-1}s} + \cdots + a_{m-1} x^{e_1s} + a_m).$$

If $g_{\bar{r}, \bar{e}}(x)$ is a permutation polynomial then $(r, s) = 1$. 
The Main Result
The Main Result

- For admissible $m$, $r$, $\bar{e}$, $\ell$, and $q$, define

$$N_{r,\bar{e}}^m(\ell, q)$$

the number of all monic permutation $(m + 1)$-nomial

$$g_{r,\bar{e}}(x) := x^r (x^{em^s} + a_1x^{em^{-1}s} + \cdots + a_{m-1}x^{e_1s} + a_m).$$
The Main Result

For admissible \( m, r, \bar{e}, \ell, \) and \( q, \) define

\[
N_{r, \bar{e}}^m(\ell, q)
\]

the number of all monic permutation \((m + 1)\)-nomial

\[
g_{r, \bar{e}}^\alpha(x) := x^r (x^{e_ms} + a_1 x^{e_{m-1}s} + \cdots + a_{m-1} x^{e_1s} + a_m).
\]


\[
\left| N_{r, \bar{e}}^m(\ell, q) - \frac{\ell!}{\ell^\ell} q^m \right| < \ell \cdot \ell! q^{m-\frac{1}{2}}.
\]
Existence of Permutation Polynomials

(i) Let $\ell > 1$. Then for $q$ sufficiently large, there exists $a \in \mathbb{F}_q$ such that the polynomial $x (x^{(q-1)/\ell} + a)$ is a permutation polynomial of $\mathbb{F}_q$.

(ii) Let $\ell > 1$, $(r, q-1) = 1$, and $k$ be a positive integer. Then for $q$ sufficiently large, there exists $a \in \mathbb{F}_q$ such that the polynomial $x^r (x^{(q-1)/\ell} + a)^k$ is a permutation polynomial of $\mathbb{F}_q$.

Laigle-Chapuy (2007) The first assertion of Carlitz-Wells' theorem is true for $q > \ell^2 + 2(1 + \ell + 1/\ell + 1/\ell + 2)^2$.

Masuda and Zieve (2007) For more general binomials of the form $x^r (x^{e_1 (q-1)/\ell} + a)$, the first assertion of Carlitz-Wells' theorem is true for $q > \ell^2 + 2$. 

Existence of Permutation Polynomials

- **Carlitz-Wells (1966)** (i) Let $\ell > 1$. Then for $q$ sufficiently large, there exists $a \in \mathbb{F}_q$ such that the polynomial $x(x^{(q-1)/\ell} + a)$ is a permutation polynomial of $\mathbb{F}_q$. 
Existence of Permutation Polynomials

- **Carlitz-Wells (1966)** (i) Let $\ell > 1$. Then for $q$ sufficiently large, there exists $a \in \mathbb{F}_q$ such that the polynomial $x(x^{(q-1)/\ell} + a)$ is a permutation polynomial of $\mathbb{F}_q$.
(ii) Let $\ell > 1$, $(r, q - 1) = 1$, and $k$ be a positive integer. Then for $q$ sufficiently large, there exists $a \in \mathbb{F}_q$ such that the polynomial $x^r(x^{(q-1)/\ell} + a)^k$ is a permutation polynomial of $\mathbb{F}_q$. 

---

Laigle-Chapuy (2007) The first assertion of Carlitz-Wells’ theorem is true for $q > \ell^2 + 2(1 + \ell + 2\ell^2)^2$.

Masuda and Zieve (2007) For more general binomials of the form $x^r(x^{(q-1)/\ell} + a)$, the first assertion of Carlitz-Wells’ theorem is true for $q > \ell^2 + 2$. 
Existence of Permutation Polynomials

- **Carlitz-Wells (1966)** (i) Let $\ell > 1$. Then for $q$ sufficiently large, there exists $a \in \mathbb{F}_q$ such that the polynomial $x(x^{(q-1)/\ell} + a)$ is a permutation polynomial of $\mathbb{F}_q$.

(ii) Let $\ell > 1$, $(r, q - 1) = 1$, and $k$ be a positive integer. Then for $q$ sufficiently large, there exists $a \in \mathbb{F}_q$ such that the polynomial $x^r(x^{(q-1)/\ell} + a)^k$ is a permutation polynomial of $\mathbb{F}_q$.

- **Laigle-Chapuy (2007)** The first assertion of Carlitz-Wells’ theorem is true for $q > \ell^{2\ell+2} \left(1 + \frac{\ell+1}{\ell+2}\right)^2$. 

Existence of Permutation Polynomials

- **Carlitz-Wells (1966)** (i) Let $\ell > 1$. Then for $q$ sufficiently large, there exists $a \in \mathbb{F}_q$ such that the polynomial $x(x^{(q-1)/\ell} + a)$ is a permutation polynomial of $\mathbb{F}_q$.

(ii) Let $\ell > 1$, $(r, q - 1) = 1$, and $k$ be a positive integer. Then for $q$ sufficiently large, there exists $a \in \mathbb{F}_q$ such that the polynomial $x^r(x^{(q-1)/\ell} + a)^k$ is a permutation polynomial of $\mathbb{F}_q$.

- **Laigle-Chapuy (2007)** The first assertion of Carlitz-Wells’ theorem is true for $q > \ell^{2\ell + 2} (1 + \frac{\ell+1}{\ell\ell+2})^2$.

- **Masuda and Zieve (2007)** For more general binomials of the form $x^r(x^{e_1(q-1)/\ell} + a)$ The first assertion of Carlitz-Wells’ theorem is true for $q > \ell^{2\ell+2}$. 
Application

The Main Result

\[ N_m r, \bar{e}(\ell, q) - \ell^! \ell \cdot q^m < \ell \cdot q^m - \frac{1}{2}. \]

Corollary

For any admissible \( q, r, \bar{e}, m, \ell, \) and \( q > \frac{\ell}{2\ell + 2}, \)

there exists an \( \bar{a} \in (\mathbb{F}_q^*)^m \) such that the \((m+1)\)-nomial

\[ g_{\bar{a}} r, \bar{e}(x) = x^r(x^e m s + a_1 x^e m - 1 s + \cdots + a_{m-1} x^e 1 s + a_m)). \]

is a permutation polynomial of \( \mathbb{F}_q. \)

For \( q \geq 7 \) we have \( \ell^2 \ell + 2 < q \) as long as \( \ell < \log q \cdot 2 \log \log q. \)
Application

The Main Result

\[ \left| N_{r,e}(\ell, q) - \frac{\ell!}{\ell^\ell} q^m \right| < \ell \cdot \ell! q^{m - \frac{1}{2}}. \]
The Main Result

\[ |N^m_{r, \bar{e}}(\ell, q) - \frac{\ell!}{\ell^\ell} q^m| < \ell \cdot \ell! q^{m-\frac{1}{2}}. \]

Corollary For any admissible \( q, r, \bar{e}, m, \ell \), and \( q > \ell^{2\ell+2} \), there exists an \( \bar{a} \in (\mathbb{F}_{q}^*)^m \) such that the \((m+1)\)-nomial

\[ g^\bar{a}_{r, \bar{e}}(x) = x^r (x^{em} + a_1x^{e_{m-1}} + \cdots + a_{m-1}x^{e_1} + a_m) \]

is a permutation polynomial of \( \mathbb{F}_q \).
Application

▶ The Main Result

\[ \left| N_{r, \bar{e}}^m(\ell, q) - \frac{\ell!}{\ell^\ell} q^m \right| < \ell \cdot \ell! q^{m-\frac{1}{2}}. \]

▶ Corollary For any admissible \( q, r, \bar{e}, m, \ell \), and \( q > \ell^{2\ell+2} \), there exists an \( \bar{a} \in (\mathbb{F}_q^*)^m \) such that the \((m+1)\)-nomial

\[ g_{r, \bar{e}}^{\bar{a}}(x) = x^r (x^{em^s} + a_1 x^{e_{m-1}^s} + \cdots + a_{m-1} x^{e_1^s} + a_m) \]

is a permutation polynomial of \( \mathbb{F}_q \).

▶ For \( q \geq 7 \) we have \( \ell^{2\ell+2} < q \) as long as \( \ell < \frac{\log q}{2 \log \log q} \).
Wan-Lidl Criterion

References

Wan-Lidl (1991)
Wan-Lidl Criterion

- \( \mu_\ell := \text{The set of all } \ell\text{-th roots of unity in } \mathbb{F}_q^*. \)
Wan-Lidl Criterion

- $\mu_\ell := \text{The set of all } \ell\text{-th roots of unity in } \mathbb{F}_q^*.$
- $s = (q - 1)/\ell, \ (r, s) = 1.$
Wan-Lidl Criterion

- $\mu_\ell :=$ The set of all $\ell$-th roots of unity in $\mathbb{F}_q^*$.
- $s = (q - 1)/\ell$, $(r, s) = 1$.
- **Wan-Lidl (1991)** $g(x) = x^r f(x^s)$ permutes $\mathbb{F}_q$ if and only if $x^r f(x)^s$ permutes $\mu_\ell$. 
Notations

$\zeta := \text{an } \ell\text{-th root of unity in } \mathbb{C}$

$\zeta^1 + \zeta + \zeta^2 + \cdots + \zeta^{\ell-1} = \begin{cases} 0 & \text{if } \zeta \neq 1 \\ \ell & \text{if } \zeta = 1 \end{cases}$

$\alpha := \text{a generator of } \mathbb{F}^*_{q}$

$\psi := \text{a multiplicative character of order } \ell \text{ of } \mu_{\ell}$

$\omega := \text{a primitive } \ell\text{-th root of unity in } \mathbb{C}$

Define $\psi(\alpha s) = \omega$, and extend it with $\psi(0) = 0$. 
Notations

- \( \zeta := \) an \( \ell \)-th root of unity in \( \mathbb{C} \)

\[ 1 + \zeta + \zeta^2 + \cdots + \zeta^{\ell-1} = \begin{cases} 0 & \text{if } \zeta \neq 1 \\ \ell & \text{if } \zeta = 1. \end{cases} \]
Notations

- $\zeta := \text{an } \ell\text{-th root of unity in } \mathbb{C}$

\[1 + \zeta + \zeta^2 + \cdots + \zeta^{\ell-1} = \begin{cases} 0 & \text{if } \zeta \neq 1 \\ \ell & \text{if } \zeta = 1. \end{cases}\]

- $\alpha := \text{A generator of } \mathbb{F}_q^*$. 
Notations

- $\zeta := \text{an } \ell\text{-th root of unity in } \mathbb{C}$

\[ 1 + \zeta + \zeta^2 + \cdots + \zeta^{\ell-1} = \begin{cases} 0 & \text{if } \zeta \neq 1 \\ \ell & \text{if } \zeta = 1 \end{cases} \]

- $\alpha := \text{A generator of } \mathbb{F}_q^*.$

- $\psi := \text{A multiplicative character of order } \ell \text{ of } \mu_\ell.$
Notations

- $\zeta := \text{an } \ell\text{-th root of unity in } \mathbb{C}$
  \[1 + \zeta + \zeta^2 + \cdots + \zeta^{\ell-1} = \begin{cases} 0 & \text{if } \zeta \neq 1 \\ \ell & \text{if } \zeta = 1. \end{cases}\]

- $\alpha := \text{A generator of } \mathbb{F}^*_q$.

- $\psi := \text{A multiplicative character of order } \ell \text{ of } \mu_\ell$.

- $\omega := \text{A primitive } \ell\text{-th root of unity in } \mathbb{C}$.
Notations

- $\zeta := \text{an } \ell\text{-th root of unity in } \mathbb{C}$
  
  \[
  1 + \zeta + \zeta^2 + \cdots + \zeta^{\ell-1} = \begin{cases} 
  0 & \text{if } \zeta \neq 1 \\
  \ell & \text{if } \zeta = 1.
  \end{cases}
  \]

- $\alpha := \text{A generator of } \mathbb{F}_q^\ast$.
- $\psi := \text{A multiplicative character of order } \ell \text{ of } \mu_\ell$.
- $\omega := \text{A primitive } \ell\text{-th root of unity in } \mathbb{C}$.
- Define $\psi(\alpha^s) = \omega$, and extend it with $\psi(0) = 0$. 
Detecting Permutations of $\mu_\ell$

For any permutation $\sigma \in S_\ell$, and any $\beta_1, \ldots, \beta_\ell \in \mu_\ell$, we define $P_\sigma(\beta_1, \ldots, \beta_\ell) = \ell \prod_{i=1}^{\ell} \left( \sum_{j=0}^{\ell-1} \left( \psi(\beta_i) \psi(\alpha_s) - \sigma(i) \right)^j \right)$.  

$\{\beta_1, \ldots, \beta_\ell\} = \mu_\ell$ if and only if there exists a unique $\sigma \in S_\ell$ such that $P_\sigma(\beta_1, \ldots, \beta_\ell) = \ell$. 
Detecting Permutations of $\mu_\ell$

- For any permutation $\sigma \in S_\ell$, and any $\beta_1, \ldots, \beta_\ell \in \mu_\ell$, we define

$$P_\sigma(\beta_1, \ldots, \beta_\ell) = \prod_{i=1}^{\ell} \left( \sum_{j=0}^{\ell-1} \left( \psi(\beta_i) \psi(\alpha^s)^{-\sigma(i)} \right)^j \right).$$
Detecting Permutations of $\mu_\ell$

For any permutation $\sigma \in S_\ell$, and any $\beta_1, \ldots, \beta_\ell \in \mu_\ell$, we define

$$P_\sigma(\beta_1, \ldots, \beta_\ell) = \prod_{i=1}^{\ell} \left( \sum_{j=0}^{\ell-1} \left( \psi(\beta_i)\psi(\alpha^s)^{-\sigma(i)} \right)^j \right).$$

$\{\beta_1, \ldots, \beta_\ell\} = \mu_\ell$ if and only if there exists a unique $\sigma \in S_\ell$ such that $P_\sigma(\beta_1, \ldots, \beta_\ell) = \ell^\ell$. 

A Formula for the Number of Permutation Polynomials

\[
g_{\bar{a}}(x) = x^{r + (m + a_1)x^{e - 1} + \cdots + a_{m-1}x^1 + a_m}
\]

The polynomial \(g_{\bar{a}}\) permutes \(\mathbb{F}_q\) if and only if the following two conditions are satisfied:

(i) \(\alpha_i^{ie_m + a_1\alpha_i^{e-1} + \cdots + a_{m-1}\alpha_i^1 + a_m} \neq 0\), for each \(i = 1, \ldots, \ell\);

(ii) \(g_{\bar{a}}(\alpha_i) \neq g_{\bar{a}}(\alpha_j)\), for \(1 \leq i < j \leq \ell\).

\[
N_{m,r,\bar{e}}(\ell, q) = \frac{1}{\ell!} \sum_{\bar{a} \in (\mathbb{F}_q^*)^m} \sum_{\sigma \in S_\ell} \prod_{i=1}^\ell \prod_{j=1}^\ell \frac{P_{\sigma}(g_{\bar{a}}(\alpha_{i,j}))}{P_{\sigma}(g_{\bar{a}}(\alpha_{i,j})^s)}.
\]
A Formula for the Number of Permutation Polynomials

\[ g_{\tilde{a}}(x) = x^r(x^{e_m s} + a_1 x^{e_{m-1} s} + \cdots + a_{m-1} x^{e_1 s} + a_m). \]
A Formula for the Number of Permutation Polynomials

\[ g^\bar{a}(x) = x'^r(x^{e_m s} + a_1 x^{e_{m-1}s} + \cdots + a_{m-1} x^{e_1 s} + a_m). \]

The polynomial \( g^\bar{a} \) permutes \( \mathbb{F}_q \) if and only if the following two conditions are satisfied:

(i) \( \alpha^{i e_m s} + a_1 \alpha^{i e_{m-1}s} + \cdots + a_{m-1} \alpha^{i e_1 s} + a_m \neq 0 \), for each \( i = 1, \ldots, \ell \);

(ii) \( g^\bar{a}(\alpha^i)^s \neq g^\bar{a}(\alpha^j)^s \), for \( 1 \leq i < j \leq \ell \).
A Formula for the Number of Permutation Polynomials

\[ g^\bar{a}(x) = x^s (x^{e_1s} + a_1 x^{e_{m-1}s} + \cdots + a_{m-1} x^{e_1s} + a_m). \]

The polynomial \( g^\bar{a} \) permutes \( \mathbb{F}_q \) if and only if the following two conditions are satisfied:

(i) \( \alpha^{i e_1 s} + a_1 \alpha^{i e_{m-1} s} + \cdots + a_{m-1} \alpha^{i e_1 s} + a_m \neq 0 \), for each \( i = 1, \ldots, \ell; \)

(ii) \( g^\bar{a}(\alpha^i)^s \neq g^\bar{a}(\alpha^j)^s \), for \( 1 \leq i < j \leq \ell. \)

\[ N_{r, \bar{e}}^m(\ell, q) = \frac{1}{\ell^\ell} \sum_{\bar{a} \in (\mathbb{F}_q^*)^m} \sum_{\sigma \in S_\ell} P_\sigma \left( g^\bar{a}(\alpha^1)^s, \ldots, g^\bar{a}(\alpha^\ell)^s \right). \]

\( \bar{a} \) satisfies (i)
The Main Term

\[ N_m(r(\ell, q)) = 1 \sum_{\bar{a} \in (F^* q)^m} \bar{a} \text{ satisfies } (i) \sum_{\sigma \in S} \ell P(\sigma) \left( g \bar{a}(\alpha_1), ..., g \bar{a}(\alpha_\ell) \right). \]
The Main Term

\[ N_{r,\bar{a}}(\ell, q) = \frac{1}{\ell^\ell} \sum_{\bar{a} \in (\mathbb{F}^*_{q})^m} \sum_{\sigma \in S_\ell} P_\sigma \left( g^{\bar{a}}(\alpha^1)^s, \ldots, g^{\bar{a}}(\alpha^\ell)^s \right). \]
The Main Term

\[ N_{r, \vec{e}}^m(\ell, q) = \frac{1}{\ell^\ell} \sum_{\vec{a} \in (\mathbb{F}_q^*)^m} \sum_{\sigma \in S_\ell} P_\sigma \left( g^{\vec{a}(\alpha^1)^s}, \ldots, g^{\vec{a}(\alpha^\ell)^s} \right). \]

Main Term = \( \frac{\ell!}{\ell^\ell} q^m \).
The Error Term

\[ \text{Error Term} = \sum (a_1, \cdots, a_m) \in (F_q)^m \Psi(t \phi(a_1, a_2, \cdots, a_m)), \]

where \( t \in F_q \), \( \Psi(\alpha) = \psi(\alpha) \) is a multiplicative character of \( F_q \), and \( \phi(a_1, a_2, \cdots, a_m) \in F_q[a_1, \cdots, a_m] \).
The Error Term

\[
\text{Error Term} = \sum_{(a_1,\ldots,a_m) \in (\mathbb{F}_q)^m} \Psi(t \, \varphi(a_1, a_2, \cdots, a_m)),
\]

where \( t \in \mathbb{F}_q, \Psi(\alpha) = \psi(\alpha^s) \) is a multiplicative character of \( \mathbb{F}_q \), and \( \varphi(a_1, a_2, \cdots, a_m) \in \mathbb{F}_q[a_1, \cdots, a_m] \).
The Error Term

\[ \beta = \alpha \sum_{1}^{m} (a_1, \cdots, a_m) \in (F_q)^m \]

\[ \Psi(t) \ell \prod_{i=1}^{k} (\beta e^m i + a_{1} \beta e^{m-1} i + \cdots + a_{m-1} \beta e^1 i + a_m) \]
The Error Term

\[ \beta = \alpha^s \]
The Error Term

\[ \beta = \alpha^s \]

\[ \sum_{(a_1, \ldots, a_m) \in (\mathbb{F}_q)^m} \psi \left( t \prod_{i=1}^{\ell} (\beta_{e_i}^{a_i} + a_1 \beta_{e_i}^{a_{i-1}} + \cdots + a_{m-1} \beta_{e_i}^{a_1} + a_m)^{k_i} \right) \]
Estimations of Character Sums

It follows from Deligne's work on the Weil conjectures for algebraic varieties over finite field that if $\phi(a_1, \cdots, a_m)$ satisfies GOOD conditions

$$\sum_{(a_1, \cdots, a_m) \in (F_q)^m} \Psi(t^{\phi(a_1, a_2, \cdots, a_m)}) \ll q^m.$$
It follows from Deligne’s work on the Weil conjectures for algebraic varieties over finite field that if $\varphi(a_1, \cdots, a_m)$ satisfies GOOD conditions

$$\sum_{(a_1, \cdots, a_m) \in (\mathbb{F}_q)^m} \Psi \left( t \ \varphi(a_1, a_2, \cdots, a_m) \right) \ll q^{\frac{m}{2}}.$$
(Katz, 2002) Let $m \geq 1$ and let
\[ \varphi = \varphi(a_1, \cdots, a_m) \in \mathbb{F}_q[a_1, \cdots, a_m] \]
be a polynomial of degree $d$. We write $\varphi = \varphi_d + \varphi_{d-1} + \cdots + \varphi_0$, where each $\varphi_j$ is homogeneous of degree $j$. Then if $(d, q) = 1$ and if $\varphi_d = 0$ defines a smooth, degree $d$ hypersurface in $\mathbb{P}^{m-1}(\mathbb{F}_q)$, $\varphi = 0$ is a smooth hypersurface in $\mathbb{A}^m(\mathbb{F}_q)$, and if $\Psi^d$ is non-trivial then

\[
\sum_{(a_1, \cdots, a_m) \in (\mathbb{F}_q)^m} \Psi(\varphi(a_1, a_2, \cdots, a_m)) \leq (d - 1)q^\frac{m}{2}.
\]
Estimations of Character Sums
Estimations of Character Sums

\[ \sum_{(a_1, \ldots, a_m) \in (\mathbb{F}_q)^m} \psi \left( t \prod_{i=1}^{\ell} \left( \beta^{e_i} a_1 \beta^{e_{m-1}^i} + \cdots + a_{m-1} \beta^{e_1^i} + a_m \right)^{k_i} \right) \]
Estimations of Character Sums

(Weil, 1948) Let \( f(x) \in \mathbb{F}_q[x] \) be a monic polynomial of positive degree that is not an \( \ell \)-th power of a polynomial. Let \( d \) be the number of distinct roots of \( f(x) \) in its splitting field over \( \mathbb{F}_q \). Then for every \( t \in \mathbb{F}_q \) we have

\[
\left| \sum_{a \in \mathbb{F}_q} \Psi(t f(a)) \right| \leq (d - 1)q^{\frac{1}{2}}.
\]
Estimations of Character Sums
Estimations of Character Sums

\[
\sum_{a_m \in (\mathbb{F}_q)} \Psi \left( t \prod_{i=1}^{\ell} (\beta_{e_m}^i + a_1 \beta_{e_m-1}^i + \cdots + a_{m-1} \beta_{e_1}^i + a_m)^{k_i} \right).
\]
\[
\sum_{(a_1, \ldots, a_m) \in (F_q)^m} \psi \left( t \varphi(a_1, a_2, \cdots, a_m) \right)
\]

\[= \sum_{(a_1, \ldots, a_{m-1}) \in (F_q)^{m-1}} \sum_{a \in F_q} \psi \left( t \varphi(a_1, a_2, \cdots, a_{m-1}, a) \right) \]

\[= \sum_{\text{Good}} + \sum_{\text{Bad}} \ll q^{m-\frac{1}{2}}. \]
\[
\sum_{(a_1, \ldots, a_m) \in (\mathbb{F}_q)^m} \Psi \left( t \varphi(a_1, a_2, \ldots, a_m) \right)
\]

\[
= \sum_{(a_1, \ldots, a_{m-1}) \in (\mathbb{F}_q)^{m-1}} \sum_{a \in \mathbb{F}_q} \Psi \left( t \varphi(a_1, a_2, \ldots, a_{m-1}, a) \right)
\]

\[
= \sum_{\text{Good}} + \sum_{\text{Bad}} \ll q^{m-\frac{1}{2}}.
\]

\[
\left| N_{r, \ell}^m (\ell, q) - \frac{\ell!}{\ell^\ell} q^m \right| < \ell \cdot \ell! q^{m-\frac{1}{2}}.
\]