Exponential Sums and Enumeration of Permutation Polynomials

Francesco Pappalardi

Conference on Zeta Functions in honor of Prof. K. Ramachandra on his 70th birthday

National Institute of Advanced Studies
NIAS

Bangalore December 13 - 15, 2003

Notations

Notations

- ☞ $\mathbb{F}_q$ Finite field, $q = p^n$

Notations

- ☞ $\mathbb{F}_q$ Finite field, $q = p^n$
- ☞ $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permutes } \mathbb{F}_q\}$

Notations

- ☞ $\mathbb{F}_q$ Finite field, $q = p^n$
- ☞ $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permutes } \mathbb{F}_q\}$
- ☞ If $\sigma \in \mathcal{S}(\mathbb{F}_q)$

Notations

- $\mathbb{F}_q$ Finite field, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma$ permutes $\mathbb{F}_q\}$
- If $\sigma \in \mathcal{S}(\mathbb{F}_q)$

$$\boxed{f_\sigma(x) := \sum_{c \in \mathbb{F}_q} \sigma(c) \left(1 - (x-c)^{q-1}\right) \in \mathbb{F}_q[x]}$$

Notations

- $\mathbb{F}_q$ Finite field, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permutes } \mathbb{F}_q\}$
- If $\sigma \in \mathcal{S}(\mathbb{F}_q)$

$$\boxed{f_\sigma(x) := \sum_{c \in \mathbb{F}_q} \sigma(c) \left(1 - (x-c)^{q-1}\right) \in \mathbb{F}_q[x]}$$

is called *permutation polynomial of* σ

Notations

- $\mathbb{F}_q$ Finite field, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permutes } \mathbb{F}_q\}$
- If $\sigma \in \mathcal{S}(\mathbb{F}_q)$

$$\boxed{f_\sigma(x) := \sum_{c \in \mathbb{F}_q} \sigma(c)\left(1 - (x-c)^{q-1}\right) \in \mathbb{F}_q[x]}$$

  is called *permutation polynomial of* σ

- Note:

Notations

- $\mathbb{F}_q$ Finite field, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permutes } \mathbb{F}_q\}$
- If $\sigma \in \mathcal{S}(\mathbb{F}_q)$

$$\boxed{f_\sigma(x) := \sum_{c \in \mathbb{F}_q} \sigma(c)\left(1 - (x-c)^{q-1}\right) \in \mathbb{F}_q[x]}$$

  is called *permutation polynomial of* σ

- Note:
  - $\partial f_\sigma \leq q - 2$ if $q > 2$

Notations

- $\mathbb{F}_q$ Finite field, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permutes } \mathbb{F}_q\}$
- If $\sigma \in \mathcal{S}(\mathbb{F}_q)$

$$\boxed{f_\sigma(x) := \sum_{c \in \mathbb{F}_q} \sigma(c)\left(1 - (x-c)^{q-1}\right) \in \mathbb{F}_q[x]}$$

  is called *permutation polynomial of* σ
- Note:
  - $\partial f_\sigma \leq q - 2$ if $q > 2$
  - $f_\sigma(c) = \sigma(c) \qquad \forall c \in \mathbb{F}_q$

Notations

- $\mathbb{F}_q$ Finite field, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma$ permutes $\mathbb{F}_q\}$
- If $\sigma \in \mathcal{S}(\mathbb{F}_q)$

$$\boxed{f_\sigma(x) := \sum_{c \in \mathbb{F}_q} \sigma(c) \left(1 - (x-c)^{q-1}\right) \in \mathbb{F}_q[x]}$$

  is called *permutation polynomial of* σ

- Note:
  - $\partial f_\sigma \leq q - 2$ if $q > 2$
  - $f_\sigma(c) = \sigma(c) \qquad \forall c \in \mathbb{F}_q$
  - **Definition.**

Notations

- $\mathbb{F}_q$ Finite field, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permutes } \mathbb{F}_q\}$
- If $\sigma \in \mathcal{S}(\mathbb{F}_q)$

$$\boxed{f_\sigma(x) := \sum_{c \in \mathbb{F}_q} \sigma(c) \left(1 - (x-c)^{q-1}\right) \in \mathbb{F}_q[x]}$$

  is called *permutation polynomial of* σ

- Note:
  - $\partial f_\sigma \leq q - 2$ if $q > 2$
  - $f_\sigma(c) = \sigma(c) \qquad \forall c \in \mathbb{F}_q$
  - **Definition.**

    $f \in \mathbb{F}_q[x]$ *is a permutation polynomial (PP) if* $\exists \sigma \in \mathcal{S}(\mathbb{F}_q)$ *such that*

Notations

- $\mathbb{F}_q$ Finite field, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permutes } \mathbb{F}_q\}$
- If $\sigma \in \mathcal{S}(\mathbb{F}_q)$

$$\boxed{f_\sigma(x) := \sum_{c \in \mathbb{F}_q} \sigma(c)\left(1 - (x-c)^{q-1}\right) \in \mathbb{F}_q[x]}$$

  is called *permutation polynomial of* σ

- Note:
  - $\partial f_\sigma \leq q - 2$ if $q > 2$
  - $f_\sigma(c) = \sigma(c) \qquad \forall c \in \mathbb{F}_q$
  - **Definition.**

    $f \in \mathbb{F}_q[x]$ *is a permutation polynomial (PP) if* $\exists \sigma \in \mathcal{S}(\mathbb{F}_q)$ *such that*

$$\boxed{f \equiv f_\sigma \bmod x^q - x}$$

Properties

Properties

☞ **Examples of Permutation Polynomial:**

Properties

☞ **Examples of Permutation Polynomial:**

✎ $ax + b, \qquad a, b \in \mathbb{F}_q, a \neq 0$

Properties

- **Examples of Permutation Polynomial:**
  - $ax+b, \qquad a, b \in \mathbb{F}_q, a \neq 0$
  - $x^k, \qquad (k, q-1) = 1$

Properties

- **Examples of Permutation Polynomial:**
  - $ax + b, \qquad a, b \in \mathbb{F}_q, a \neq 0$
  - $x^k, \qquad (k, q-1) = 1$
  - COMPOSITION $f \circ g$ is a PP if f and g are PP

Properties

- **Examples of Permutation Polynomial:**
  - $ax + b, \qquad a, b \in \mathbb{F}_q, a \neq 0$
  - $x^k, \qquad (k, q-1) = 1$
  - COMPOSITION $f \circ g$ is a PP if f and g are PP
  - $x^{(q+m-1)/m} + ax$ is a PP if $m|q-1$

Properties

☞ **Examples of Permutation Polynomial:**

- ✎ $ax + b, \qquad a, b \in \mathbb{F}_q, a \neq 0$
- ✎ $x^k, \qquad (k, q-1) = 1$
- ✎ COMPOSITION $f \circ g$ is a PP if f and g are PP
- ✎ $x^{(q+m-1)/m} + ax$ is a PP if $m | q-1$
- ✎ DICKSON POLYNOMIALS $a \in \mathbb{F}_q$, $k \in \mathbb{N}$

Properties

☞ **Examples of Permutation Polynomial:**

- ✎ $ax + b, \qquad a, b \in \mathbb{F}_q, a \neq 0$
- ✎ $x^k, \qquad (k, q-1) = 1$
- ✎ COMPOSITION $f \circ g$ is a PP if f and g are PP
- ✎ $x^{(q+m-1)/m} + ax$ is a PP if $m|q-1$
- ✎ DICKSON POLYNOMIALS $a \in \mathbb{F}_q$, $k \in \mathbb{N}$

$$\boxed{D_k(x,a) = \sum_{j=0}^{[k/2]} \frac{k}{k-j}\binom{k-j}{j}(-a)^j x^{k-2j}}$$

Properties

☞ **Examples of Permutation Polynomial:**

✎ $ax+b, \qquad a,b \in \mathbb{F}_q, a \neq 0$

✎ $x^k, \qquad (k, q-1) = 1$

✎ COMPOSITION $f \circ g$ is a PP if f and g are PP

✎ $x^{(q+m-1)/m} + ax$ is a PP if $m | q-1$

✎ DICKSON POLYNOMIALS $a \in \mathbb{F}_q$, $k \in \mathbb{N}$

$$\boxed{D_k(x,a) = \sum_{j=0}^{[k/2]} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}}$$

➳ If $a \neq 0$, $D_k(x,a)$ is a PP $\Leftrightarrow$ $(k, q^2-1) = 1$

Properties

- **Examples of Permutation Polynomial:**
  - $ax+b, \qquad a,b \in \mathbb{F}_q, a \neq 0$
  - $x^k, \qquad (k, q-1) = 1$
  - COMPOSITION $f \circ g$ is a PP if f and g are PP
  - $x^{(q+m-1)/m} + ax$ is a PP if $m|q-1$
  - DICKSON POLYNOMIALS $a \in \mathbb{F}_q$, $k \in \mathbb{N}$

$$\boxed{D_k(x,a) = \sum_{j=0}^{[k/2]} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}}$$

    - If $a \neq 0$, $D_k(x,a)$ is a PP $\Leftrightarrow$ $(k, q^2-1) = 1$
  - LINEARIZED POLYNOMIALS $q = p^m$, $\alpha_1, \ldots, \alpha_s \in \mathbb{F}_{p^m}$

Properties

☞ **Examples of Permutation Polynomial:**

- $ax + b, \qquad a, b \in \mathbb{F}_q, a \neq 0$
- $x^k, \qquad (k, q-1) = 1$
- COMPOSITION $f \circ g$ is a PP if f and g are PP
- $x^{(q+m-1)/m} + ax$ is a PP if $m | q-1$
- DICKSON POLYNOMIALS $a \in \mathbb{F}_q$, $k \in \mathbb{N}$

$$\boxed{D_k(x, a) = \sum_{j=0}^{[k/2]} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}}$$

  - If $a \neq 0$, $D_k(x, a)$ is a PP $\Leftrightarrow$ $(k, q^2 - 1) = 1$

- LINEARIZED POLYNOMIALS $q = p^m$, $\alpha_1, \ldots, \alpha_s \in \mathbb{F}_{p^m}$

$$\boxed{L(x) = \sum_{s=0}^{r-1} \alpha_s x^{q^s} \text{ is a PP} \Leftrightarrow \det(\alpha_{i-j}^{q^j}) \neq 0}$$

Dickson-Diffie-Hellmann Key Exchange

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** `and` **Balu** `choose` $\mathbb{F}_q$ `and` $\gamma \in \mathbb{F}_q$ `generator`

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** and **Balu** choose $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q$ generator

② **Adhikari** chooses $a \in [0, q^2 - 1]$

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** and **Balu** choose $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q$ generator

② **Adhikari** chooses $a \in [0, q^2 - 1]$ secret

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** `and` **Balu** `choose` $\mathbb{F}_q$ `and` $\gamma \in \mathbb{F}_q$ `generator`

② **Adhikari** `chooses` $a \in [0, q^2 - 1]$ `secret`

Balu `chooses` $b \in [0, q^2 - 1]$

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** and **Balu** choose $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q$ generator

② **Adhikari** chooses $a \in [0, q^2 - 1]$ secret

Balu chooses $b \in [0, q^2 - 1]$ secret

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** `and` **Balu** `choose` $\mathbb{F}_q$ `and` $\gamma \in \mathbb{F}_q$ `generator`

② **Adhikari** `chooses` $a \in [0, q^2 - 1]$ `secret`

Balu `chooses` $b \in [0, q^2 - 1]$ `secret`

③ **Adhikari** `computes and publish` $\alpha := D_a(\gamma, \pm 1)$

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** and **Balu** choose $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q$ generator

② **Adhikari** chooses $a \in [0, q^2 - 1]$ secret

Balu chooses $b \in [0, q^2 - 1]$ secret

③ **Adhikari** computes and publish $\alpha := D_a(\gamma, \pm 1)$

Balu computes and publish $\beta := D_b(\gamma, \pm 1)$

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** and **Balu** choose $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q$ generator

② **Adhikari** chooses $a \in [0, q^2 - 1]$ secret

Balu chooses $b \in [0, q^2 - 1]$ secret

③ **Adhikari** computes and publish $\alpha := D_a(\gamma, \pm 1)$

Balu computes and publish $\beta := D_b(\gamma, \pm 1)$

④ The common secret key is

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** and **Balu** choose $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q$ generator

② **Adhikari** chooses $a \in [0, q^2 - 1]$ secret

Balu chooses $b \in [0, q^2 - 1]$ secret

③ **Adhikari** computes and publish $\alpha := D_a(\gamma, \pm 1)$

Balu computes and publish $\beta := D_b(\gamma, \pm 1)$

④ The common secret key is

$$\boxed{D_{ab}(\gamma, \pm 1) = D_a(D_b(\gamma, \pm 1), \pm 1) = D_b(D_a(\gamma, \pm 1), \pm 1))}$$

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** and **Balu** choose $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q$ generator

② **Adhikari** chooses $a \in [0, q^2 - 1]$ secret

Balu chooses $b \in [0, q^2 - 1]$ secret

③ **Adhikari** computes and publish $\alpha := D_a(\gamma, \pm 1)$

Balu computes and publish $\beta := D_b(\gamma, \pm 1)$

④ The common secret key is

$$\boxed{D_{ab}(\gamma, \pm 1) = D_a(D_b(\gamma, \pm 1), \pm 1) = D_b(D_a(\gamma, \pm 1), \pm 1))}$$

⑤ To find the secret key **Ramki** has to solve

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** and **Balu** choose $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q$ generator

② **Adhikari** chooses $a \in [0, q^2 - 1]$ secret

Balu chooses $b \in [0, q^2 - 1]$ secret

③ **Adhikari** computes and publish $\alpha := D_a(\gamma, \pm 1)$

Balu computes and publish $\beta := D_b(\gamma, \pm 1)$

④ The common secret key is

$$\boxed{D_{ab}(\gamma, \pm 1) = D_a(D_b(\gamma, \pm 1), \pm 1) = D_b(D_a(\gamma, \pm 1), \pm 1))}$$

⑤ To find the secret key **Ramki** has to solve

$$\boxed{D_a(\gamma, \pm 1) = \alpha}$$ Dickson Discrete Logarithm

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** and **Balu** choose $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q$ generator

② **Adhikari** chooses $a \in [0, q^2 - 1]$ secret

Balu chooses $b \in [0, q^2 - 1]$ secret

③ **Adhikari** computes and publish $\alpha := D_a(\gamma, \pm 1)$

Balu computes and publish $\beta := D_b(\gamma, \pm 1)$

④ The common secret key is

$$\boxed{D_{ab}(\gamma, \pm 1) = D_a(D_b(\gamma, \pm 1), \pm 1) = D_b(D_a(\gamma, \pm 1), \pm 1))}$$

⑤ To find the secret key **Ramki** has to solve

$$\boxed{D_a(\gamma, \pm 1) = \alpha}$$ Dickson Discrete Logarithm

NOTE There exists a fast algorithm to compute $D_a(\gamma, c) \in \mathbb{F}_q$

Dickson-Diffie-Hellmann Key Exchange

① **Adhikari** and **Balu** choose $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q$ generator

② **Adhikari** chooses $a \in [0, q^2 - 1]$ secret

Balu chooses $b \in [0, q^2 - 1]$ secret

③ **Adhikari** computes and publish $\alpha := D_a(\gamma, \pm 1)$

Balu computes and publish $\beta := D_b(\gamma, \pm 1)$

④ The common secret key is

$$\boxed{D_{ab}(\gamma, \pm 1) = D_a(D_b(\gamma, \pm 1), \pm 1) = D_b(D_a(\gamma, \pm 1), \pm 1))}$$

⑤ To find the secret key **Ramki** has to solve

$$\boxed{D_a(\gamma, \pm 1) = \alpha}$$ Dickson Discrete Logarithm

NOTE There exists a fast algorithm to compute $D_a(\gamma, c) \in \mathbb{F}_q$

Problem Find new classes of PP

Enumeration of PP with given degree

Enumeration of PP with given degree

$$\boxed{N_d(q) = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Enumeration of PP with given degree

$$\boxed{N_d(q) = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Problem: Compute $N_d(q)$

Enumeration of PP with given degree

$$\boxed{N_d(q) = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Problem: Compute $N_d(q)$

☞ $$\sum_{d \leq q-2} N_d(q) = q!$$

Enumeration of PP with given degree

$$\boxed{N_d(q) = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Problem: Compute $N_d(q)$

☞ $\displaystyle\sum_{d \le q-2} N_d(q) = q!$ (if $q > 2$, $\partial f_\sigma \le q-2$)

Enumeration of PP with given degree

$$\boxed{N_d(q) = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Problem: Compute $N_d(q)$

- ☞ $\displaystyle\sum_{d \leq q-2} N_d(q) = q!$ (if $q > 2$, $\partial f_\sigma \leq q-2$)
- ☞ $N_1(q) = q(q-1)$

Enumeration of PP with given degree

$$\boxed{N_d(q) = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Problem: Compute $N_d(q)$

- ☞ $\displaystyle\sum_{d \leq q-2} N_d(q) = q!$ (if $q > 2$, $\partial f_\sigma \leq q-2$)
- ☞ $N_1(q) = q(q-1)$ (linear PP)

Enumeration of PP with given degree

$$\boxed{N_d(q) = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Problem: Compute $N_d(q)$

- ☞ $\displaystyle\sum_{d \le q-2} N_d(q) = q!$ (if $q > 2$, $\partial f_\sigma \le q-2$)
- ☞ $N_1(q) = q(q-1)$ (linear PP)
- ☞ $N_d(q) = 0$ if $d | q-1$

Enumeration of PP with given degree

$$\boxed{N_d(q) = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Problem: Compute $N_d(q)$

- $\displaystyle\sum_{d \leq q-2} N_d(q) = q!$ (if $q > 2$, $\partial f_\sigma \leq q-2$)
- $N_1(q) = q(q-1)$ (linear PP)
- $N_d(q) = 0$ if $d | q-1$ (Hermite's criterion)

Enumeration of PP with given degree

$$\boxed{N_d(q) = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Problem: Compute $N_d(q)$

- $\displaystyle\sum_{d \leq q-2} N_d(q) = q!$ (if $q > 2$, $\partial f_\sigma \leq q-2$)
- $N_1(q) = q(q-1)$ (linear PP)
- $N_d(q) = 0$ if $d|q-1$ (Hermite's criterion)
- $N_d(q)$ is known for $d < 6$

Enumeration of PP with given degree

$$\boxed{N_d(q) = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Problem: Compute $N_d(q)$

- ☞ $\displaystyle\sum_{d \le q-2} N_d(q) = q!$ (if $q > 2$, $\partial f_\sigma \le q-2$)
- ☞ $N_1(q) = q(q-1)$ (linear PP)
- ☞ $N_d(q) = 0$ if $d | q-1$ (Hermite's criterion)
- ☞ $N_d(q)$ is known for $d < 6$
- ☞ Almost all PP have degree $q-2$

Enumeration of PP with given degree

$$\boxed{N_d(q) = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Problem: Compute $N_d(q)$

- $\displaystyle\sum_{d \leq q-2} N_d(q) = q!$ (if $q > 2$, $\partial f_\sigma \leq q-2$)
- $N_1(q) = q(q-1)$ (linear PP)
- $N_d(q) = 0$ if $d | q-1$ (Hermite's criterion)
- $N_d(q)$ is known for $d < 6$
- Almost all PP have degree $q-2$

$$M_q = \{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial f_\sigma < q-2\}$$

Enumeration of PP with given degree

$$\boxed{N_d(q) = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Problem: Compute $N_d(q)$

- $\displaystyle\sum_{d \le q-2} N_d(q) = q!$ (if $q > 2$, $\partial f_\sigma \le q-2$)
- $N_1(q) = q(q-1)$ (linear PP)
- $N_d(q) = 0$ if $d | q-1$ (Hermite's criterion)
- $N_d(q)$ is known for $d < 6$
- Almost all PP have degree $q-2$

$$M_q = \{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial f_\sigma < q-2\}$$

S. Konyagin, FP (2002), *P. Das* (2002)

$$\boxed{|\#M_q - (q-1)!| \le \sqrt{2e/\pi}\, q^{q/2}}$$

Another way to count

Another way to count

$$\boxed{q - c_\sigma \leq \partial f_\sigma \leq q-2 \qquad \Leftarrow \qquad \sigma \in \mathcal{S}(\mathbb{F}_q) \setminus \{id\} \quad \text{and } q > 2}$$

Another way to count

$$\boxed{q - c_\sigma \leq \partial f_\sigma \leq q-2 \qquad \Leftarrow \qquad \sigma \in \mathcal{S}(\mathbb{F}_q) \setminus \{id\} \quad \text{and } q > 2}$$

where $c_\sigma = \#\{a \in \mathbb{F}_q \mid \sigma(a) \neq a\}$

Another way to count

$$\boxed{q - c_\sigma \leq \partial f_\sigma \leq q-2 \qquad \Leftarrow \qquad \sigma \in \mathcal{S}(\mathbb{F}_q) \setminus \{id\} \quad \text{and } q > 2}$$

where $c_\sigma = \#\{a \in \mathbb{F}_q \mid \sigma(a) \neq a\}$

☞ $c_{\sigma_1} = c_{\sigma_2}$ if σ_1 and σ_2 are conjugate (i.e. $c_\sigma = c_{\mathcal{C}(\sigma)}$)

Another way to count

$$\boxed{q - c_\sigma \leq \partial f_\sigma \leq q - 2 \qquad \Leftarrow \qquad \sigma \in \mathcal{S}(\mathbb{F}_q) \setminus \{id\} \quad \text{and } q > 2}$$

where $c_\sigma = \#\{a \in \mathbb{F}_q \mid \sigma(a) \neq a\}$

- ☞ $c_{\sigma_1} = c_{\sigma_2}$ if σ_1 and σ_2 are conjugate (i.e. $c_\sigma = c_{\mathcal{C}(\sigma)}$)
- ☞ $\mathcal{C} \subset \mathcal{S}(\mathbb{F}_q)$ conjugation class

Another way to count

$$\boxed{q - c_\sigma \leq \partial f_\sigma \leq q-2 \qquad \Leftarrow \qquad \sigma \in \mathcal{S}(\mathbb{F}_q) \setminus \{id\} \quad \text{and } q > 2}$$

where $c_\sigma = \#\{a \in \mathbb{F}_q \mid \sigma(a) \neq a\}$

- ☞ $c_{\sigma_1} = c_{\sigma_2}$ if σ_1 and σ_2 are conjugate (i.e. $c_\sigma = c_{\mathcal{C}(\sigma)}$)
- ☞ $\mathcal{C} \subset \mathcal{S}(\mathbb{F}_q)$ conjugation class
- ☞ Natural functions:

Another way to count

$$\boxed{q - c_\sigma \le \partial f_\sigma \le q-2 \qquad \Leftarrow \qquad \sigma \in \mathcal{S}(\mathbb{F}_q) \setminus \{id\} \quad \text{and } q > 2}$$

where $c_\sigma = \#\{a \in \mathbb{F}_q \mid \sigma(a) \ne a\}$

- $c_{\sigma_1} = c_{\sigma_2}$ if σ_1 and σ_2 are conjugate (i.e. $c_\sigma = c_{\mathcal{C}(\sigma)}$)
- $\mathcal{C} \subset \mathcal{S}(\mathbb{F}_q)$ conjugation class
- Natural functions:
  - ✗ $m_{\mathcal{C}}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma = q - c_{\mathcal{C}}\}$ (minimal degree)

Another way to count

$$\boxed{q - c_\sigma \le \partial f_\sigma \le q-2 \qquad \Leftarrow \qquad \sigma \in \mathcal{S}(\mathbb{F}_q) \setminus \{id\} \quad \text{and } q > 2}$$

where $c_\sigma = \#\{a \in \mathbb{F}_q \mid \sigma(a) \neq a\}$

- $c_{\sigma_1} = c_{\sigma_2}$ if σ_1 and σ_2 are conjugate (i.e. $c_\sigma = c_{\mathcal{C}(\sigma)}$)
- $\mathcal{C} \subset \mathcal{S}(\mathbb{F}_q)$ conjugation class
- Natural functions:
  - ✗ $m_\mathcal{C}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma = q - c_\mathcal{C}\}$ (minimal degree)
  - ✗ $M_\mathcal{C}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma < q - 2\}$ (non–maximal degree)

Another way to count

$$\boxed{q - c_\sigma \leq \partial f_\sigma \leq q-2 \qquad \Leftarrow \qquad \sigma \in \mathcal{S}(\mathbb{F}_q) \setminus \{id\} \quad \text{and } q > 2}$$

where $c_\sigma = \#\{a \in \mathbb{F}_q \mid \sigma(a) \neq a\}$

- ☞ $c_{\sigma_1} = c_{\sigma_2}$ if σ_1 and σ_2 are conjugate (i.e. $c_\sigma = c_{\mathcal{C}(\sigma)}$)
- ☞ $\mathcal{C} \subset \mathcal{S}(\mathbb{F}_q)$ conjugation class
- ☞ Natural functions:
  - ✗ $m_\mathcal{C}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma = q - c_\mathcal{C}\}$ (minimal degree)
  - ✗ $M_\mathcal{C}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma < q - 2\}$ (non–maximal degree)

Theorem *C. Malvenuto, FP* (2002)

- If $\mathcal{C} \neq [2], [3], [2\ 2]$, then

$$M_{\mathcal{C}}(q) = \frac{\#\mathcal{C}}{q} + O_{\mathcal{C}}\left(\frac{1}{q^2}\right) \quad \text{if} \quad \operatorname{char} \mathbb{F}_q \to \infty$$

- Explicit Formulas for $M_{\mathcal{C}}(q)$ if $c_{\mathcal{C}} \leq 6$

Formulas for non–maximal degree PP

Formulas for non–maximal degree PP

$$
\begin{aligned}
M_{[4]}(q) &= \tfrac{1}{4}\, q(q-1)\,(q-5-2\eta(-1)-4\eta(-3))\\
M_{[2\ 2]}(q) &= \tfrac{1}{8}\, q(q-1)(q-4)\,\{1+\eta(-1)\}\\
M_{[5]}(q) &= \tfrac{1}{5}\, q(q-1)\quad q^2-(9-\eta(5)-5\eta(-1)+5\eta(-9))\,q++26+5\eta(-7)+15\eta(-3)+15\eta(-1)\\
M_{[2\ 3]}(q) &= \tfrac{1}{6}\, q(q-1)\quad q^2-(9+\eta(-3)+3\eta(-1))q+(24+6\eta(-3)+18\eta(-1)+6\eta(-7))\\
M_{[6]}(q) &= \frac{q(q-1)}{6}\{q^3-14\,q^2+[68-6\,\eta(5)-6\,\eta(50)]q-[154+66\,\eta(-3)+93\,\eta(-1)\\
&\quad +12\,\eta(-2)+54\,\eta(-7)]\}\\
M_{[4\ 2]}(q) &= \frac{q(q-1)}{8}(q^3-[14-\eta(2)]q^2+[71+12\,\eta(-1)+\eta(-2)+4\,\eta(-3)-8\,\eta(50)]q\\
&\quad -[148+100\,\eta(-1)+24\,\eta(-2)+44\,\eta(-3)+40\,\eta(-7)])\\
M_{[3\ 3]}(q) &= \frac{q(q-1)}{18}(q^3-13\,q^2+[62+9\,\eta(-1)+4\,\eta(-3)]q-[150+99\,\eta(-1)+42\,\eta(-3)+72\,\eta(-7)])\\
M_{[2\ 2\ 2]}(q) &= \frac{q(q-1)}{48}(q^3-[14+3\,\eta(-1)]q^2+[70+36\,\eta(-1)+6\,\eta(-2)]q-[136+120\,\eta(-1)\\
&\quad +48\,\eta(-2)+8\,\eta(-3)])
\end{aligned}
$$

char$(\mathbb{F}_q)>3$ and η is the quadratic character

Formulas for non–maximal degree PP

$$
\begin{aligned}
M_{[4]}(q) &= \tfrac{1}{4}\, q(q-1)\,(q-5-2\eta(-1)-4\eta(-3)) \\
M_{[2\ 2]}(q) &= \tfrac{1}{8}\, q(q-1)(q-4)\,\{1+\eta(-1)\} \\
M_{[5]}(q) &= \tfrac{1}{5}\, q(q-1)\ \ q^2-(9-\eta(5)-5\eta(-1)+5\eta(-9))\,q++26+5\eta(-7)+15\eta(-3)+15\eta(-1) \\
M_{[2\ 3]}(q) &= \tfrac{1}{6}\, q(q-1)\ \ q^2-(9+\eta(-3)+3\eta(-1))q+(24+6\eta(-3)+18\eta(-1)+6\eta(-7)) \\
M_{[6]}(q) &= \frac{q(q-1)}{6}\{q^3-14\,q^2+[68-6\,\eta(5)-6\,\eta(50)]q-[154+66\,\eta(-3)+93\,\eta(-1) \\
&\quad +12\,\eta(-2)+54\,\eta(-7)]\} \\
M_{[4\ 2]}(q) &= \frac{q(q-1)}{8}(q^3-[14-\eta(2)]q^2+[71+12\,\eta(-1)+\eta(-2)+4\,\eta(-3)-8\,\eta(50)]q \\
&\quad -[148+100\,\eta(-1)+24\,\eta(-2)+44\,\eta(-3)+40\,\eta(-7)]) \\
M_{[3\ 3]}(q) &= \frac{q(q-1)}{18}(q^3-13\,q^2+[62+9\,\eta(-1)+4\,\eta(-3)]q-[150+99\,\eta(-1)+42\,\eta(-3)+72\,\eta(-7)]) \\
M_{[2\ 2\ 2]}(q) &= \frac{q(q-1)}{48}(q^3-[14+3\,\eta(-1)]q^2+[70+36\,\eta(-1)+6\,\eta(-2)]q-[136+120\,\eta(-1) \\
&\quad +48\,\eta(-2)+8\,\eta(-3)])
\end{aligned}
$$

$\mathrm{char}(\mathbb{F}_q) > 3$ and η is the quadratic character

PP with minimal degree

Formulas for non–maximal degree PP

$$
\begin{array}{rcl}
M_{[4]}(q) & = & \frac{1}{4}\, q(q-1)\,(q-5-2\eta(-1)-4\eta(-3)) \\
M_{[2\ 2]}(q) & = & \frac{1}{8}\, q(q-1)(q-4)\,\{1+\eta(-1)\} \\
M_{[5]}(q) & = & \frac{1}{5}\, q(q-1)\quad q^2-(9-\eta(5)-5\eta(-1)+5\eta(-9))\,q+{}+26+5\eta(-7)+15\eta(-3)+15\eta(-1) \\
M_{[2\ 3]}(q) & = & \frac{1}{6}\, q(q-1)\quad q^2-(9+\eta(-3)+3\eta(-1))q+(24+6\eta(-3)+18\eta(-1)+6\eta(-7)) \\
M_{[6]}(q) & = & \frac{q(q-1)}{6}\{q^3-14\,q^2+[68-6\,\eta(5)-6\,\eta(50)]q-[154+66\,\eta(-3)+93\,\eta(-1) \\
 & & +12\,\eta(-2)+54\,\eta(-7)]\} \\
M_{[4\ 2]}(q) & = & \frac{q(q-1)}{8}(q^3-[14-\eta(2)]q^2+[71+12\,\eta(-1)+\eta(-2)+4\,\eta(-3)-8\,\eta(50)]q \\
 & & -[148+100\,\eta(-1)+24\,\eta(-2)+44\,\eta(-3)+40\,\eta(-7)]) \\
M_{[3\ 3]}(q) & = & \frac{q(q-1)}{18}(q^3-13\,q^2+[62+9\,\eta(-1)+4\,\eta(-3)]q-[150+99\,\eta(-1)+42\,\eta(-3)+72\,\eta(-7)]) \\
M_{[2\ 2\ 2]}(q) & = & \frac{q(q-1)}{48}(q^3-[14+3\,\eta(-1)]q^2+[70+36\,\eta(-1)+6\,\eta(-2)]q-[136+120\,\eta(-1) \\
 & & +48\,\eta(-2)+8\,\eta(-3)])
\end{array}
$$

$\mathrm{char}(\mathbb{F}_q) > 3$ and η is the quadratic character

PP with minimal degree

✗ $m_{\mathcal{C}}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma = q - c_{\mathcal{C}}\}$

Formulas for non–maximal degree PP

$$
\begin{array}{rcl}
M_{[4]}(q) & = & \frac{1}{4}q(q-1)\,(q-5-2\eta(-1)-4\eta(-3))\\
M_{[2\ 2]}(q) & = & \frac{1}{8}q(q-1)(q-4)\,\{1+\eta(-1)\}\\
M_{[5]}(q) & = & \frac{1}{5}q(q-1)\quad q^2-(9-\eta(5)-5\eta(-1)+5\eta(-9))\,q++26+5\eta(-7)+15\eta(-3)+15\eta(-1)\\
M_{[2\ 3]}(q) & = & \frac{1}{6}q(q-1)\quad q^2-(9+\eta(-3)+3\eta(-1))q+(24+6\eta(-3)+18\eta(-1)+6\eta(-7))\\
M_{[6]}(q) & = & \frac{q(q-1)}{6}\{q^3-14\,q^2+[68-6\,\eta(5)-6\,\eta(50)]q-[154+66\,\eta(-3)+93\,\eta(-1)\\
 & & +12\,\eta(-2)+54\,\eta(-7)]\}\\
M_{[4\ 2]}(q) & = & \frac{q(q-1)}{8}(q^3-[14-\eta(2)]q^2+[71+12\,\eta(-1)+\eta(-2)+4\,\eta(-3)-8\,\eta(50)]q\\
 & & -[148+100\,\eta(-1)+24\,\eta(-2)+44\,\eta(-3)+40\,\eta(-7)])\\
M_{[3\ 3]}(q) & = & \frac{q(q-1)}{18}(q^3-13\,q^2+[62+9\,\eta(-1)+4\,\eta(-3)]q-[150+99\,\eta(-1)+42\,\eta(-3)+72\,\eta(-7)])\\
M_{[2\ 2\ 2]}(q) & = & \frac{q(q-1)}{48}(q^3-[14+3\,\eta(-1)]q^2+[70+36\,\eta(-1)+6\,\eta(-2)]q-[136+120\,\eta(-1)\\
 & & +48\,\eta(-2)+8\,\eta(-3)])
\end{array}
$$

char$(\mathbb{F}_q) > 3$ and η is the quadratic character

PP with minimal degree

✗ $m_{\mathcal{C}}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma = q - c_{\mathcal{C}}\}$

Theorem *C. Malvenuto, FP* (to appear)

- If $q \equiv 1 \bmod k$ then $m_{[k]}(q) \geq \frac{\varphi(k)}{k} q(q-1)$
- If $\operatorname{char}(\mathbb{F}_q) \geq 2 \cdot 3^{[k/3]-1}$ then $m_{[k]}(q) \leq \frac{(k-1)!}{k} q(q-1)$

Today's Result

Today's Result

$$\boxed{\mathcal{N}_d = \#\left\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) < q-d-1\right\}}$$

Today's Result

$$\boxed{\mathcal{N}_d = \#\left\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) < q - d - 1\right\}}$$

Theorem *S. Konyagin, FP*

Let $\alpha = (e-2)/3e = 0.08808\cdots$ *and* $d < \alpha q$. *Then*

$$\left|\mathcal{N}_d - \frac{q!}{q^d}\right| \leq 2^d d q^{2+q-d} \binom{q}{d} \left(\frac{2d}{q-d}\right)^{(q-d)/2}.$$

It follows that

$$\mathcal{N}_d \sim \frac{q!}{q^d}$$

if $d \leq \alpha q$ *and* $\alpha < 0.03983$

Today's Result

$$\boxed{\mathcal{N}_d = \#\left\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) < q-d-1\right\}}$$

Theorem *S. Konyagin, FP*

Let $\alpha = (e-2)/3e = 0.08808\cdots$ *and* $d < \alpha q$. *Then*

$$\left|\mathcal{N}_d - \frac{q!}{q^d}\right| \leq 2^d d q^{2+q-d} \binom{q}{d} \left(\frac{2d}{q-d}\right)^{(q-d)/2}.$$

It follows that

$$\mathcal{N}_d \sim \frac{q!}{q^d}$$

if $d \leq \alpha q$ *and* $\alpha < 0.03983$

Note: The best possible value for α in the theorem is 0.5. In fact $\partial f_\sigma \neq (q-1)/2$ if q is odd. Therefore

$$\boxed{\mathcal{N}_{(q-1)/2} = 0}$$

Proof's Method

Proof's Method

The coefficient of x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ is 0 if and only if

Proof's Method

The coefficient of x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ is 0 if and only if

$$\boxed{\sum_{c\in\mathbb{F}_q} c^{q-j-1}\sigma(c) = 0.}$$

Proof's Method

The coefficient of x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ is 0 if and only if

$$\boxed{\sum_{c\in\mathbb{F}_q} c^{q-j-1}\sigma(c) = 0.}$$

$\forall S \subseteq \mathbb{F}_q$

$$\boxed{n_S := \#\left\{ f \;\middle|\; f:\mathbb{F}_q \longrightarrow S, \sum_{c\in\mathbb{F}_q} c^{q-i-1} f(c) = 0, \forall i = 1,\ldots,d \right\}.}$$

Proof's Method

The coefficient of x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ is 0 if and only if

$$\boxed{\sum_{c\in\mathbb{F}_q} c^{q-j-1}\sigma(c) = 0.}$$

$\forall S \subseteq \mathbb{F}_q$

$$\boxed{n_S := \#\left\{ f \;\middle|\; f : \mathbb{F}_q \longrightarrow S, \sum_{c\in\mathbb{F}_q} c^{q-i-1} f(c) = 0, \forall i = 1, \ldots, d \right\}.}$$

"Inclusion-Exclusion" implies

$$\mathcal{N}_d = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) < q-d-1\} = \sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|} n_S \qquad (1)$$

Proof's Method

The coefficient of x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ is 0 if and only if

$$\boxed{\sum_{c\in\mathbb{F}_q} c^{q-j-1}\sigma(c) = 0.}$$

$\forall S \subseteq \mathbb{F}_q$

$$\boxed{n_S := \#\left\{ f \;\middle|\; f : \mathbb{F}_q \longrightarrow S, \sum_{c\in\mathbb{F}_q} c^{q-i-1} f(c) = 0, \forall i = 1,\ldots,d \right\}.}$$

"Inclusion-Exclusion" implies

$$\mathcal{N}_d = \#\left\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) < q-d-1\right\} = \sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|} n_S \qquad (1)$$

Proof's Method

The coefficient of x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ is 0 if and only if

$$\boxed{\sum_{c\in\mathbb{F}_q} c^{q-j-1}\sigma(c) = 0.}$$

$\forall S \subseteq \mathbb{F}_q$

$$\boxed{n_S := \#\left\{ f \;\middle|\; f:\mathbb{F}_q \longrightarrow S, \sum_{c\in\mathbb{F}_q} c^{q-i-1} f(c) = 0, \forall i = 1,\ldots,d \right\}.}$$

"Inclusion-Exclusion" implies

$$\mathcal{N}_d = \#\left\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) < q-d-1\right\} = \sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|} n_S \tag{1}$$

Proof's Method

The coefficient of x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ is 0 if and only if

$$\boxed{\sum_{c\in\mathbb{F}_q} c^{q-j-1}\sigma(c) = 0.}$$

$\forall S \subseteq \mathbb{F}_q$

$$\boxed{n_S := \#\left\{ f \;\middle|\; f:\mathbb{F}_q \longrightarrow S, \sum_{c\in\mathbb{F}_q} c^{q-i-1} f(c) = 0, \forall i = 1,\ldots,d \right\}.}$$

"Inclusion-Exclusion" implies

$$\mathcal{N}_d = \#\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) < q-d-1\} = \sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|} n_S \qquad (1)$$

Proof's Method

The coefficient of x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ is 0 if and only if

$$\boxed{\sum_{c\in\mathbb{F}_q} c^{q-j-1}\sigma(c) = 0.}$$

$\forall S \subseteq \mathbb{F}_q$

$$\boxed{n_S := \#\left\{ f \;\middle|\; f : \mathbb{F}_q \longrightarrow S, \sum_{c\in\mathbb{F}_q} c^{q-i-1} f(c) = 0, \forall i = 1,\ldots,d \right\}.}$$

"Inclusion-Exclusion" implies

$$\mathcal{N}_d = \#\left\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) < q-d-1\right\} = \sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|} n_S \tag{1}$$

Need to evaluate n_S. Let $e_p(u) = e^{\frac{2\pi i u}{p}}$ and $\mathrm{Tr}(\alpha) \in \mathbb{F}_p$ be the trace of $\alpha \in \mathbb{F}_q$. 3

Then

Then

$$
\begin{aligned}
n_S &= \frac{1}{q^d} \sum_{(a_1,\dots,a_d)\in\mathbb{F}_q^d} \sum_{f:\mathbb{F}_q \longrightarrow S} e_p\left(\sum_{c\in\mathbb{F}_q} \mathrm{Tr}(f(c)\sum_{i=1}^{d} a_i c^{q-i-1})\right) \\
&= \frac{1}{q^d} \sum_{(a_1,\dots,a_d)\in\mathbb{F}_q^d} \prod_{c\in\mathbb{F}_q} \sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1})) \qquad (2) \\
&= \frac{|S|^q}{q^d} + R_S
\end{aligned}
$$

Then

$$\begin{aligned} n_S &= \frac{1}{q^d} \sum_{(a_1,\ldots,a_d)\in\mathbb{F}_q^d} \sum_{f:\mathbb{F}_q\longrightarrow S} e_p\left(\sum_{c\in\mathbb{F}_q} \mathrm{Tr}(f(c)\sum_{i=1}^{d} a_i c^{q-i-1})\right) \\ &= \frac{1}{q^d} \sum_{(a_1,\ldots,a_d)\in\mathbb{F}_q^d} \prod_{c\in\mathbb{F}_q} \sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1})) \qquad (2) \\ &= \frac{|S|^q}{q^d} + R_S \end{aligned}$$

Then

$$\begin{aligned} n_S &= \frac{1}{q^d} \sum_{(a_1,\dots,a_d)\in\mathbb{F}_q^d} \sum_{f:\mathbb{F}_q\longrightarrow S} e_p\left(\sum_{c\in\mathbb{F}_q} \mathrm{Tr}(f(c)\sum_{i=1}^{d} a_i c^{q-i-1})\right) \\ &= \frac{1}{q^d} \sum_{(a_1,\dots,a_d)\in\mathbb{F}_q^d} \prod_{c\in\mathbb{F}_q} \sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1})) \qquad (2) \\ &= \frac{|S|^q}{q^d} + R_S \end{aligned}$$

Then

$$
\begin{aligned}
n_S &= \frac{1}{q^d} \sum_{(a_1,\ldots,a_d)\in\mathbb{F}_q^d} \sum_{f:\mathbb{F}_q \longrightarrow S} e_p\left(\sum_{c\in\mathbb{F}_q} \mathrm{Tr}(f(c)\sum_{i=1}^{d} a_i c^{q-i-1})\right) \\
&= \frac{1}{q^d} \sum_{(a_1,\ldots,a_d)\in\mathbb{F}_q^d} \prod_{c\in\mathbb{F}_q} \sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1})) \qquad (2) \\
&= \frac{|S|^q}{q^d} + R_S
\end{aligned}
$$

Then

$$
\begin{aligned}
n_S &= \frac{1}{q^d} \sum_{(a_1,\dots,a_d)\in\mathbb{F}_q^d} \sum_{f:\mathbb{F}_q\longrightarrow S} e_p\left(\sum_{c\in\mathbb{F}_q} \mathrm{Tr}(f(c)\sum_{i=1}^{d} a_i c^{q-i-1})\right) \\
&= \frac{1}{q^d} \sum_{(a_1,\dots,a_d)\in\mathbb{F}_q^d} \prod_{c\in\mathbb{F}_q} \sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1})) \qquad (2) \\
&= \frac{|S|^q}{q^d} + R_S
\end{aligned}
$$

where

$$
\boxed{|R_S| \le \frac{q^d-1}{q^d} \max_{(a_1,\dots,a_d)\in\mathbb{F}_q^d\setminus\{\underline{0}\}} \prod_{c\in\mathbb{F}_q} \left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1}))\right|}
$$

3

Furthermore, since the geometric mean is bounded by the arithmetic mean, we have

Furthermore, since the geometric mean is bounded by the arithmetic mean, we have

$$
\begin{aligned}
|R_S| \leq \max_{(a_1,\ldots,a_d)} \prod_{c\in\mathbb{F}_q} \left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1}))\right| &\leq \\
\max_{(a_1,\ldots,a_d)} \left(\frac{1}{q}\sum_{c\in\mathbb{F}_q}\left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1}))\right|^2\right)^{q/2} &\leq \\
\left(\frac{1}{q}\sum_{f\in\mathbb{F}_q}(q-2)\left|\sum_{t\in S} e_p(\mathrm{Tr}(tf))\right|^2\right)^{q/2} &= ((q-2)|S|)^{q/2}. \quad (3)
\end{aligned}
$$

Furthermore, since the geometric mean is bounded by the arithmetic mean, we have

$$
\begin{aligned}
|R_S| \le \max_{(a_1,\ldots,a_d)} \prod_{c\in\mathbb{F}_q} \left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^d a_i c^{q-i-1}))\right| &\le \\
\max_{(a_1,\ldots,a_d)} \left(\frac{1}{q}\sum_{c\in\mathbb{F}_q}\left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^d a_i c^{q-i-1}))\right|^2\right)^{q/2} &\le \\
\left(\frac{1}{q}\sum_{f\in\mathbb{F}_q}(q-2)\left|\sum_{t\in S} e_p(\mathrm{Tr}(tf))\right|^2\right)^{q/2} &= ((q-2)|S|)^{q/2}. \quad (3)
\end{aligned}
$$

Furthermore, since the geometric mean is bounded by the arithmetic mean, we have

$$
\begin{aligned}
|R_S| \leq \max_{(a_1,\dots,a_d)} \prod_{c\in\mathbb{F}_q} \left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1}))\right| &\leq \\
\max_{(a_1,\dots,a_d)} \left(\frac{1}{q}\sum_{c\in\mathbb{F}_q}\left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1}))\right|^2\right)^{q/2} &\leq \\
\left(\frac{1}{q}\sum_{f\in\mathbb{F}_q}(q-2)\left|\sum_{t\in S} e_p(\mathrm{Tr}(tf))\right|^2\right)^{q/2} &= ((q-2)|S|)^{q/2}. \quad (3)
\end{aligned}
$$

Furthermore, since the geometric mean is bounded by the arithmetic mean, we have

$$|R_S| \leq \max_{(a_1,\dots,a_d)} \prod_{c\in\mathbb{F}_q} \left| \sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1})) \right| \leq$$

$$\max_{(a_1,\dots,a_d)} \left(\frac{1}{q} \sum_{c\in\mathbb{F}_q} \left| \sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1})) \right|^2 \right)^{q/2} \leq$$

$$\left(\frac{1}{q} \sum_{f\in\mathbb{F}_q} (q-2) \left| \sum_{t\in S} e_p(\mathrm{Tr}(tf)) \right|^2 \right)^{q/2} = ((q-2)|S|)^{q/2}. \quad (3)$$

Furthermore, since the geometric mean is bounded by the arithmetic mean, we have

$$
\begin{aligned}
|R_S| \le \max_{(a_1,\dots,a_d)} \prod_{c\in\mathbb{F}_q} \left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1}))\right| &\le \\
\max_{(a_1,\dots,a_d)} \left(\frac{1}{q}\sum_{c\in\mathbb{F}_q}\left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1}))\right|^2\right)^{q/2} &\le \\
\left(\frac{1}{q}\sum_{f\in\mathbb{F}_q}(q-2)\left|\sum_{t\in S} e_p(\mathrm{Tr}(tf))\right|^2\right)^{q/2} &= ((q-2)|S|)^{q/2}. \quad (3)
\end{aligned}
$$

Furthermore, since the geometric mean is bounded by the arithmetic mean, we have

$$
\begin{aligned}
|R_S| \leq \max_{(a_1,\ldots,a_d)} \prod_{c\in\mathbb{F}_q} \left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1}))\right| &\leq \\
\max_{(a_1,\ldots,a_d)} \left(\frac{1}{q}\sum_{c\in\mathbb{F}_q}\left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1}))\right|^2\right)^{q/2} &\leq \\
\left(\frac{1}{q}\sum_{f\in\mathbb{F}_q}(q-2)\left|\sum_{t\in S} e_p(\mathrm{Tr}(tf))\right|^2\right)^{q/2} &= ((q-2)|S|)^{q/2}. \quad (3)
\end{aligned}
$$

Replace the estimate for $|R_S|$ in (2) and then in (1) obtaining:

Furthermore, since the geometric mean is bounded by the arithmetic mean, we have

$$
\begin{aligned}
|R_S| \le \max_{(a_1,\ldots,a_d)} \prod_{c\in\mathbb{F}_q} \left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1}))\right| &\le \\
\max_{(a_1,\ldots,a_d)} \left(\frac{1}{q}\sum_{c\in\mathbb{F}_q}\left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^{d} a_i c^{q-i-1}))\right|^2\right)^{q/2} &\le \\
\left(\frac{1}{q}\sum_{f\in\mathbb{F}_q}(q-2)\left|\sum_{t\in S} e_p(\mathrm{Tr}(tf))\right|^2\right)^{q/2} &= ((q-2)|S|)^{q/2}. \quad (3)
\end{aligned}
$$

Replace the estimate for $|R_S|$ in (2) and then in (1) obtaining:

$$
\boxed{\left|n_S - \frac{|S|^q}{q^d}\right| \le ((q-2)|S|)^{q/2}}
$$

4

Therefore

Therefore

$$\begin{aligned}
\left|\mathcal{N}_d - \sum_{S\subseteq\mathbb{F}_q} \frac{(-1)^{q-|S|}}{q^d}|S|^q\right| &= \left|\mathcal{N}_d - \frac{q!}{q^d}\right| \\
&= \left|\sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}\left(n_S - \frac{|S|^q}{q^d}\right)\right| \\
&\leq \frac{q^d-1}{q^d}\sum_{S\subseteq\mathbb{F}_q}((q-2)|S|)^{q/2} \\
&\leq 2^q((q-2)q)^{q/2}
\end{aligned}$$

Therefore

$$
\begin{aligned}
\left|\mathcal{N}_d - \sum_{S\subseteq\mathbb{F}_q} \frac{(-1)^{q-|S|}}{q^d}|S|^q\right| &= \left|\mathcal{N}_d - \frac{q!}{q^d}\right| \\
&= \left|\sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}\left(n_S - \frac{|S|^q}{q^d}\right)\right| \\
&\leq \frac{q^d-1}{q^d}\sum_{S\subseteq\mathbb{F}_q}((q-2)|S|)^{q/2} \\
&\leq 2^q((q-2)q)^{q/2}
\end{aligned}
$$

Therefore

$$\begin{aligned}
\left|\mathcal{N}_d - \sum_{S\subseteq\mathbb{F}_q} \frac{(-1)^{q-|S|}}{q^d}|S|^q\right| &= \left|\mathcal{N}_d - \frac{q!}{q^d}\right| \\
&= \left|\sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}\left(n_S - \frac{|S|^q}{q^d}\right)\right| \\
&\leq \frac{q^d-1}{q^d}\sum_{S\subseteq\mathbb{F}_q}((q-2)|S|)^{q/2} \\
&\leq 2^q((q-2)q)^{q/2}
\end{aligned}$$

Therefore

$$
\begin{aligned}
\left|\mathcal{N}_d - \sum_{S\subseteq\mathbb{F}_q} \frac{(-1)^{q-|S|}}{q^d}|S|^q\right| &= \left|\mathcal{N}_d - \frac{q!}{q^d}\right| \\
&= \left|\sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|}\left(n_S - \frac{|S|^q}{q^d}\right)\right| \\
&\le \frac{q^d-1}{q^d}\sum_{S\subseteq\mathbb{F}_q} ((q-2)|S|)^{q/2} \\
&\le 2^q((q-2)q)^{q/2}
\end{aligned}
$$

Therefore

$$\begin{aligned}
\left|\mathcal{N}_d - \sum_{S\subseteq\mathbb{F}_q} \frac{(-1)^{q-|S|}}{q^d}|S|^q\right| &= \left|\mathcal{N}_d - \frac{q!}{q^d}\right| \\
&= \left|\sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|}\left(n_S - \frac{|S|^q}{q^d}\right)\right| \\
&\le \frac{q^d-1}{q^d}\sum_{S\subseteq\mathbb{F}_q}((q-2)|S|)^{q/2} \\
&\le 2^q((q-2)q)^{q/2}
\end{aligned}$$

Therefore

$$\begin{aligned}
\left|\mathcal{N}_d - \sum_{S\subseteq\mathbb{F}_q} \frac{(-1)^{q-|S|}}{q^d}|S|^q\right| &= \left|\mathcal{N}_d - \frac{q!}{q^d}\right| \\
&= \left|\sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|}\left(n_S - \frac{|S|^q}{q^d}\right)\right| \\
&\leq \frac{q^d-1}{q^d}\sum_{S\subseteq\mathbb{F}_q}((q-2)|S|)^{q/2} \\
&\leq 2^q((q-2)q)^{q/2}
\end{aligned}$$

Therefore

$$\begin{aligned}
\left|\mathcal{N}_d - \sum_{S\subseteq\mathbb{F}_q} \frac{(-1)^{q-|S|}}{q^d}|S|^q\right| &= \left|\mathcal{N}_d - \frac{q!}{q^d}\right| \\
&= \left|\sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|}\left(n_S - \frac{|S|^q}{q^d}\right)\right| \\
&\leq \frac{q^d-1}{q^d}\sum_{S\subseteq\mathbb{F}_q} ((q-2)|S|)^{q/2} \\
&\leq 2^q((q-2)q)^{q/2}
\end{aligned}$$

This shows that

Therefore

$$\begin{aligned}
\left|\mathcal{N}_d - \sum_{S\subseteq\mathbb{F}_q} \frac{(-1)^{q-|S|}}{q^d}|S|^q\right| &= \left|\mathcal{N}_d - \frac{q!}{q^d}\right| \\
&= \left|\sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|}\left(n_S - \frac{|S|^q}{q^d}\right)\right| \\
&\leq \frac{q^d-1}{q^d}\sum_{S\subseteq\mathbb{F}_q}((q-2)|S|)^{q/2} \\
&\leq 2^q((q-2)q)^{q/2}
\end{aligned}$$

This shows that $\boxed{\mathcal{N}_d \sim \frac{q!}{q^d}}$

Therefore

$$\begin{aligned}
\left|\mathcal{N}_d - \sum_{S\subseteq\mathbb{F}_q} \frac{(-1)^{q-|S|}}{q^d}|S|^q\right| &= \left|\mathcal{N}_d - \frac{q!}{q^d}\right| \\
&= \left|\sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|}\left(n_S - \frac{|S|^q}{q^d}\right)\right| \\
&\le \frac{q^d-1}{q^d}\sum_{S\subseteq\mathbb{F}_q}((q-2)|S|)^{q/2} \\
&\le 2^q((q-2)q)^{q/2}
\end{aligned}$$

This shows that $\boxed{\mathcal{N}_d \sim \frac{q!}{q^d}}$ if $\boxed{d < \frac{q}{\log q}\left(\frac{1}{2}\log\log q - \log\log\log q\right)}$

Therefore

$$
\begin{aligned}
\left|\mathcal{N}_d - \sum_{S\subseteq\mathbb{F}_q} \frac{(-1)^{q-|S|}}{q^d}|S|^q\right| &= \left|\mathcal{N}_d - \frac{q!}{q^d}\right| \\
&= \left|\sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|}\left(n_S - \frac{|S|^q}{q^d}\right)\right| \\
&\leq \frac{q^d-1}{q^d}\sum_{S\subseteq\mathbb{F}_q}((q-2)|S|)^{q/2} \\
&\leq 2^q((q-2)q)^{q/2}
\end{aligned}
$$

This shows that $\boxed{\mathcal{N}_d \sim \frac{q!}{q^d}}$ if $\boxed{d < \frac{q}{\log q}\left(\frac{1}{2}\log\log q - \log\log\log q\right)}$ $\square$

The proof of the Theorem is an evolution of this method.

Key Lemmas 1/2

Key Lemmas 1/2

If $P(x) \in \mathbb{F}_q[x]$, $\mu(P) := \min_{T \subset \mathbb{F}_q, |T|=d} |P(T)|$.

Key Lemmas 1/2

If $P(x) \in \mathbb{F}_q[x]$, $\mu(P) := \min_{T \subset \mathbb{F}_q, |T|=d} |P(T)|$.

Lemma 1. *If $\mu \in \mathbb{N}$. Then*

$$|\{P \in \mathbb{F}_q[x] \mid \partial P = d, \mu(P) = \mu\}| \leq q^{\mu} \frac{\mu^d}{\mu!} \binom{q}{d}.$$

Key Lemmas 1/2

If $P(x) \in \mathbb{F}_q[x]$, $\mu(P) := \min_{T \subset \mathbb{F}_q, |T|=d} |P(T)|$.

Lemma 1. *If* $\mu \in \mathbb{N}$. *Then*

$$|\{P \in \mathbb{F}_q[x] \mid \partial P = d, \mu(P) = \mu\}| \leq q^\mu \frac{\mu^d}{\mu!} \binom{q}{d}.$$

Lemma 1. is used in (3):

Key Lemmas 1/2

If $P(x) \in \mathbb{F}_q[x]$, $\mu(P) := \min_{T \subset \mathbb{F}_q, |T|=d} |P(T)|$.

Lemma 1. *If $\mu \in \mathbb{N}$. Then*

$$|\{P \in \mathbb{F}_q[x] \mid \partial P = d, \mu(P) = \mu\}| \leq q^\mu \frac{\mu^d}{\mu!}\binom{q}{d}.$$

Lemma 1. is used in (3):

$$\sum_{\substack{P \in \mathbb{F}_q[x], \\ P(0)=0, \partial(P)=d}} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(\mathrm{Tr}(tP(c))) = \sum_{\mu \leq d} \sum_{\substack{P \in \mathbb{F}_q[x] \\ \partial(P)=d, \mu(P)=\mu}} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(\mathrm{Tr}(tP(c))) \quad (4)$$

Key Lemmas 1/2

If $P(x) \in \mathbb{F}_q[x]$, $\mu(P) := \min_{T \subset \mathbb{F}_q, |T|=d} |P(T)|$.

Lemma 1. *If $\mu \in \mathbb{N}$. Then*

$$|\{P \in \mathbb{F}_q[x] \mid \partial P = d, \mu(P) = \mu\}| \leq q^{\mu} \frac{\mu^d}{\mu!} \binom{q}{d}.$$

Lemma 1. is used in (3):

$$\sum_{\substack{P \in \mathbb{F}_q[x], \\ P(0)=0, \partial(P)=d}} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(\mathrm{Tr}(tP(c))) = \sum_{\mu \leq d} \sum_{\substack{P \in \mathbb{F}_q[x] \\ \partial(P)=d, \mu(P)=\mu}} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(\mathrm{Tr}(tP(c))) \quad (4)$$

Key Lemmas 1/2

If $P(x) \in \mathbb{F}_q[x]$, $\mu(P) := \min_{T \subset \mathbb{F}_q, |T|=d} |P(T)|$.

Lemma 1. *If* $\mu \in \mathbb{N}$. *Then*

$$|\{P \in \mathbb{F}_q[x] \mid \partial P = d, \mu(P) = \mu\}| \leq q^\mu \frac{\mu^d}{\mu!} \binom{q}{d}.$$

Lemma 1. is used in (3):

$$\sum_{\substack{P \in \mathbb{F}_q[x], \\ P(0)=0, \partial(P)=d}} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(\mathrm{Tr}(tP(c))) = \sum_{\mu \leq d} \sum_{\substack{P \in \mathbb{F}_q[x] \\ \partial(P)=d, \mu(P)=\mu}} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(\mathrm{Tr}(tP(c))) \quad (4)$$

Lemma 2. *If* $d \leq q/3$, $P \in \mathbb{F}_q[x], \partial(P) = d$ *and* $\mu(P) \geq \mu \geq 2$, *then*

$$\prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(\mathrm{Tr}(tP(c))) \leq \left(\frac{q}{2}\right)^{(q+d)/2} \left(\frac{d}{\mu - 1} \frac{q}{q-d}\right)^{(q-d)/2}$$

Range of Uniformity

Range of Uniformity

The condition $d \leq \alpha q$ and $\alpha < 0.03983$ in Today's statement cames from

Range of Uniformity

The condition $d \leq \alpha q$ and $\alpha < 0.03983$ in Today's statement cames from

$$\boxed{-1 = \log\left(2^\alpha\right) - \log\left(\alpha^\alpha(1-\alpha)^{1-\alpha}\right) + \log\left(\left(\frac{2\alpha}{1-\alpha}\right)^{\frac{1-\alpha}{2}}\right)}$$

Range of Uniformity

The condition $d \leq \alpha q$ and $\alpha < 0.03983$ in Today's statement cames from

$$\boxed{-1 = \log\left(2^{\alpha}\right) - \log\left(\alpha^{\alpha}(1-\alpha)^{1-\alpha}\right) + \log\left(\left(\frac{2\alpha}{1-\alpha}\right)^{\frac{1-\alpha}{2}}\right)}$$

with root $\alpha \approx 0.039834785421713449799577559 01$

Corollaries

Corollaries

Fix $k_1, \ldots, k_d \in \mathbb{N}$, $k_1 < \cdots < k_d$,

Corollaries

Fix $k_1, \ldots, k_d \in \mathbb{N}$, $k_1 < \cdots < k_d$,

$$N_q(k_1, \ldots, k_d) = \#\left\{ \sigma \in \mathcal{S}(\mathbb{F}_q) \;\middle|\; \begin{array}{l} \forall i = 1, \ldots, d, \text{ the } k_i\text{–th} \\ \text{coefficient of } f_\sigma \text{ is } 0 \end{array} \right\}.$$

Corollaries

Fix $k_1, \ldots, k_d \in \mathbb{N}$, $k_1 < \cdots < k_d$,

$$\boxed{N_q(k_1, \ldots, k_d) = \#\left\{ \sigma \in \mathcal{S}(\mathbb{F}_q) \;\middle|\; \begin{array}{l} \forall i = 1, \ldots, d, \text{ the } k_i\text{–th} \\ \text{coefficient of } f_\sigma \text{ is } 0 \end{array} \right\}.}$$

Then

$$\boxed{\left| N_q(k_1, \ldots, k_d) - \frac{q!}{q^d} \right| \leq 2^q((q - k_1 - 1)q)^{q/2}}$$

Corollaries

Fix $k_1, \ldots, k_d \in \mathbb{N}$, $k_1 < \cdots < k_d$,

$$\boxed{N_q(k_1, \ldots, k_d) = \#\left\{ \sigma \in \mathcal{S}(\mathbb{F}_q) \;\middle|\; \begin{array}{l} \forall i = 1, \ldots, d, \text{ the } k_i\text{–th} \\ \text{coefficient of } f_\sigma \text{ is } 0 \end{array} \right\}.}$$

Then

$$\boxed{\left| N_q(k_1, \ldots, k_d) - \frac{q!}{q^d} \right| \leq 2^q ((q - k_1 - 1)q)^{q/2}}$$

Planning to adopt the method of for arbitrary $k_1, \ldots, k_d$ where d grows *slowly* as $q \to \infty$