Somme Esponenziali
e
Enumerazione di Polinomi Permutazione

Francesco Pappalardi

Secondo Convegno Italiano di TEORIA DEI NUMERI

UNIVERSITA DEGLI STUDI DI PARMA
Dipartimento di Matematica

13-15 Novembre, 2003

Notazioni

Notazioni

☞ $\mathbb{F}_q$ Campo finito, $q = p^n$

Notazioni

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

Notazioni

- $\mathbb{F}_q$ Campo finito, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permuta } \mathbb{F}_q\}$
- Se $\sigma \in \mathcal{S}(\mathbb{F}_q)$

Notazioni

- ☞ $\mathbb{F}_q$ Campo finito, $q = p^n$
- ☞ $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permuta } \mathbb{F}_q\}$
- ☞ Se $\sigma \in \mathcal{S}(\mathbb{F}_q)$

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

Notazioni

- $\mathbb{F}_q$ Campo finito, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permuta } \mathbb{F}_q\}$
- Se $\sigma \in \mathcal{S}(\mathbb{F}_q)$

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

si chiama *polinomio permutazione di* σ

Notazioni

- $\mathbb{F}_q$ Campo finito, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permuta } \mathbb{F}_q\}$
- Se $\sigma \in \mathcal{S}(\mathbb{F}_q)$

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

si chiama *polinomio permutazione di* σ

- Nota:

Notazioni

☞ $\mathbb{F}_q$ Campo finito, $q = p^n$

☞ $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permuta } \mathbb{F}_q\}$

☞ Se $\sigma \in \mathcal{S}(\mathbb{F}_q)$

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

si chiama *polinomio permutazione di* σ

☞ Nota:

✍ $\partial f_\sigma \leq q - 2$ se $q > 2$

Notazioni

- $\mathbb{F}_q$ Campo finito, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma$ permuta $\mathbb{F}_q\}$
- Se $\sigma \in \mathcal{S}(\mathbb{F}_q)$

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

  si chiama *polinomio permutazione di* σ
- Nota:
  - $\partial f_\sigma \leq q-2$ se $q>2$
  - $f_\sigma(c) = \sigma(c) \qquad \forall c \in \mathbb{F}_q$

Notazioni

- ☞ $\mathbb{F}_q$ Campo finito, $q = p^n$
- ☞ $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permuta } \mathbb{F}_q\}$
- ☞ Se $\sigma \in \mathcal{S}(\mathbb{F}_q)$

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

si chiama *polinomio permutazione di* σ

- ☞ Nota:
  - ✍ $\partial f_\sigma \leq q - 2$ se $q > 2$
  - ✍ $f_\sigma(c) = \sigma(c) \qquad \forall c \in \mathbb{F}_q$
  - ✍ **Definizione.**

Notazioni

- $\mathbb{F}_q$ Campo finito, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma$ permuta $\mathbb{F}_q\}$
- Se $\sigma \in \mathcal{S}(\mathbb{F}_q)$

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

  si chiama *polinomio permutazione di* σ
- Nota:
  - $\partial f_\sigma \leq q - 2$ se $q > 2$
  - $f_\sigma(c) = \sigma(c) \qquad \forall c \in \mathbb{F}_q$
  - **Definizione.**

    $f \in \mathbb{F}_q[x]$ *si dice polinomio permutazione (PP) se* $\exists \sigma \in \mathcal{S}(\mathbb{F}_q)$ *tale che*

Notazioni

- $\mathbb{F}_q$ Campo finito, $q = p^n$
- $\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ permuta } \mathbb{F}_q\}$
- Se $\sigma \in \mathcal{S}(\mathbb{F}_q)$

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

si chiama *polinomio permutazione di* σ

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

    $f \in \mathbb{F}_q[x]$ *si dice polinomio permutazione (PP) se* $\exists \sigma \in \mathcal{S}(\mathbb{F}_q)$ *tale che*

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

Proprietà

Proprietà

☞ **Esempi di Polinomi Permutazione:**

Proprietà

☞ **Esempi di Polinomi Permutazione:**

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

Proprietà

- **Esempi di Polinomi Permutazione:**
  - $ax + b, \qquad a, b \in \mathbb{F}_q, a \neq 0$
  - $x^k, \qquad (k, q-1) = 1$

Proprietà

☞ **Esempi di Polinomi Permutazione:**

- ✎ $ax + b, \qquad a, b \in \mathbb{F}_q, a \neq 0$
- ✎ $x^k, \qquad (k, q-1) = 1$
- ✎ La composizione $f \circ g$ è un PP se f e g sono PP

Proprietà

- **Esempi di Polinomi Permutazione:**
  - $ax + b, \qquad a, b \in \mathbb{F}_q, a \neq 0$
  - $x^k, \qquad (k, q-1) = 1$
  - La composizione $f \circ g$ è un PP se f e g sono PP
  - $x^{(q+m-1)/m} + ax$ è un PP se $m | q-1$

Proprietà

- **Esempi di Polinomi Permutazione:**
  - $ax + b, \qquad a, b \in \mathbb{F}_q, a \neq 0$
  - $x^k, \qquad (k, q-1) = 1$
  - La composizione $f \circ g$ è un PP se f e g sono PP
  - $x^{(q+m-1)/m} + ax$ è un PP se $m | q - 1$
  - Polinomi di Dickson $a \in \mathbb{F}_q$, $k \in \mathbb{N}$

Proprietà

☞ Esempi di Polinomi Permutazione:

- ✎ $ax+b, \qquad a,b \in \mathbb{F}_q, a \neq 0$
- ✎ $x^k, \qquad (k,q-1)=1$
- ✎ La composizione $f \circ g$ è un PP se f e g sono PP
- ✎ $x^{(q+m-1)/m}+ax$ è un PP se $m|q-1$
- ✎ Polinomi di Dickson $a \in \mathbb{F}_q$, $k \in \mathbb{N}$

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

Proprietà

☞ **Esempi di Polinomi Permutazione:**

- ✎ $ax+b, \qquad a,b \in \mathbb{F}_q, a \neq 0$
- ✎ $x^k, \qquad (k,q-1)=1$
- ✎ La composizione $f \circ g$ è un PP se f e g sono PP
- ✎ $x^{(q+m-1)/m}+ax$ è un PP se $m|q-1$
- ✎ Polinomi di Dickson $a \in \mathbb{F}_q$, $k \in \mathbb{N}$

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

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

Proprietà

☞ **Esempi di Polinomi Permutazione:**

- ✎ $ax+b, \qquad a,b \in \mathbb{F}_q, a \neq 0$
- ✎ $x^k, \qquad (k, q-1) = 1$
- ✎ La composizione $f \circ g$ è un PP se f e g sono PP
- ✎ $x^{(q+m-1)/m} + ax$ è un PP se $m|q-1$
- ✎ Polinomi di Dickson $a \in \mathbb{F}_q$, $k \in \mathbb{N}$

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

  - ➽ Se $a \neq 0$, $D_k(x,a)$ è un PP $\Leftrightarrow$ $(k, q^2-1) = 1$
- ✎ Polinomi Linearizzati $q = p^m$, $\alpha_1, \ldots, \alpha_s \in \mathbb{F}_{p^m}$

Proprietà

☞ **Esempi di Polinomi Permutazione:**

- $ax + b, \qquad a, b \in \mathbb{F}_q, a \neq 0$
- $x^k, \qquad (k, q-1) = 1$
- La composizione $f \circ g$ è un PP se f e g sono PP
- $x^{(q+m-1)/m} + ax$ è un PP se $m | q-1$
- Polinomi di Dickson $a \in \mathbb{F}_q$, $k \in \mathbb{N}$

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

  - Se $a \neq 0$, $D_k(x,a)$ è un PP $\Leftrightarrow$ $(k, q^2-1) = 1$
- Polinomi Linearizzati $q = p^m$, $\alpha_1, \ldots, \alpha_s \in \mathbb{F}_{p^m}$

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

Scambio Chiavi Dickson-Diffie-Hellmann

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

② **Alberto** sceglie $a \in [0, q^2 - 1]$

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

② **Alberto** sceglie $a \in [0, q^2 - 1]$ segreto

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

② **Alberto** sceglie $a \in [0, q^2 - 1]$ segreto

RoBerto sceglie $b \in [0, q^2 - 1]$

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

② **Alberto** sceglie $a \in [0, q^2 - 1]$ segreto

RoBerto sceglie $b \in [0, q^2 - 1]$ segreto

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

② **Alberto** sceglie $a \in [0, q^2 - 1]$ segreto

RoBerto sceglie $b \in [0, q^2 - 1]$ segreto

③ **Alberto** calcola e pubblica $\alpha := D_a(\gamma, \pm 1)$

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

② **Alberto** sceglie $a \in [0, q^2 - 1]$ segreto

RoBerto sceglie $b \in [0, q^2 - 1]$ segreto

③ **Alberto** calcola e pubblica $\alpha := D_a(\gamma, \pm 1)$

RoBerto calcola e pubblica $\beta := D_b(\gamma, \pm 1)$

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

② **Alberto** sceglie $a \in [0, q^2 - 1]$ segreto

RoBerto sceglie $b \in [0, q^2 - 1]$ segreto

③ **Alberto** calcola e pubblica $\alpha := D_a(\gamma, \pm 1)$

RoBerto calcola e pubblica $\beta := D_b(\gamma, \pm 1)$

④ La chiave comune segreta è

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

② **Alberto** sceglie $a \in [0, q^2 - 1]$ segreto

RoBerto sceglie $b \in [0, q^2 - 1]$ segreto

③ **Alberto** calcola e pubblica $\alpha := D_a(\gamma, \pm 1)$

RoBerto calcola e pubblica $\beta := D_b(\gamma, \pm 1)$

④ La chiave comune segreta è

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

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

② **Alberto** sceglie $a \in [0, q^2 - 1]$ segreto

RoBerto sceglie $b \in [0, q^2 - 1]$ segreto

③ **Alberto** calcola e pubblica $\alpha := D_a(\gamma, \pm 1)$

RoBerto calcola e pubblica $\beta := D_b(\gamma, \pm 1)$

④ La chiave comune segreta è

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

⑤ Per trovare la chiave segreta **Carlo** deve risolvere

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

② **Alberto** sceglie $a \in [0, q^2 - 1]$ segreto

RoBerto sceglie $b \in [0, q^2 - 1]$ segreto

③ **Alberto** calcola e pubblica $\alpha := D_a(\gamma, \pm 1)$

RoBerto calcola e pubblica $\beta := D_b(\gamma, \pm 1)$

④ La chiave comune segreta è

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

⑤ Per trovare la chiave segreta **Carlo** deve risolvere

$$\boxed{D_a(\gamma, \pm 1) = \alpha}$$ Logaritmo Discreto di Dickson

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

② **Alberto** sceglie $a \in [0, q^2 - 1]$ segreto

RoBerto sceglie $b \in [0, q^2 - 1]$ segreto

③ **Alberto** calcola e pubblica $\alpha := D_a(\gamma, \pm 1)$

RoBerto calcola e pubblica $\beta := D_b(\gamma, \pm 1)$

④ La chiave comune segreta è

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

⑤ Per trovare la chiave segreta **Carlo** deve risolvere

$$\boxed{D_a(\gamma, \pm 1) = \alpha}$$ Logaritmo Discreto di Dickson

NOTA Esiste algoritmo veloce per calcolare $D_a(\gamma, c) \in \mathbb{F}_q$

Scambio Chiavi Dickson-Diffie-Hellmann

① **Alberto** e **RoBerto** scelgono $\mathbb{F}_q$ e $\gamma \in \mathbb{F}_q$ suo generatore

② **Alberto** sceglie $a \in [0, q^2 - 1]$ segreto

RoBerto sceglie $b \in [0, q^2 - 1]$ segreto

③ **Alberto** calcola e pubblica $\alpha := D_a(\gamma, \pm 1)$

RoBerto calcola e pubblica $\beta := D_b(\gamma, \pm 1)$

④ La chiave comune segreta è

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

⑤ Per trovare la chiave segreta **Carlo** deve risolvere

$\boxed{D_a(\gamma, \pm 1) = \alpha}$ Logaritmo Discreto di Dickson

NOTA Esiste algoritmo veloce per calcolare $D_a(\gamma, c) \in \mathbb{F}_q$

Problema Trovare nuove classi di PP

Enumerazione dei PP di grado fissato

Enumerazione dei PP di grado fissato

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

Enumerazione dei PP di grado fissato

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

Problema: Calcolare $N_d(q)$

Enumerazione dei PP di grado fissato

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

Problema: Calcolare $N_d(q)$

☞ $\displaystyle\sum_{d \leq q-2} N_d(q) = q!$

Enumerazione dei PP di grado fissato

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

Problema: Calcolare $N_d(q)$

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

Enumerazione dei PP di grado fissato

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

Problema: Calcolare $N_d(q)$

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

☞ $N_1(q) = q(q-1)$

Enumerazione dei PP di grado fissato

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

Problema: Calcolare $N_d(q)$

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

Enumerazione dei PP di grado fissato

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

Problema: Calcolare $N_d(q)$

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

Enumerazione dei PP di grado fissato

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

Problema: Calcolare $N_d(q)$

- ☞ $\displaystyle\sum_{d \leq q-2} N_d(q) = q!$ (se $q > 2$, $\partial f_\sigma \leq q-2$)
- ☞ $N_1(q) = q(q-1)$ (PP lineari)
- ☞ $N_d(q) = 0$ se $d | q-1$ (criterio di Hermite)

Enumerazione dei PP di grado fissato

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

Problema: Calcolare $N_d(q)$

- ☞ $\displaystyle\sum_{d \leq q-2} N_d(q) = q!$ (se $q > 2$, $\partial f_\sigma \leq q-2$)
- ☞ $N_1(q) = q(q-1)$ (PP lineari)
- ☞ $N_d(q) = 0$ se $d|q-1$ (criterio di Hermite)
- ☞ $N_d(q)$ è noto per $d < 6$

Enumerazione dei PP di grado fissato

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

Problema: Calcolare $N_d(q)$

- ☞ $\displaystyle\sum_{d \leq q-2} N_d(q) = q!$ (se $q > 2$, $\partial f_\sigma \leq q-2$)
- ☞ $N_1(q) = q(q-1)$ (PP lineari)
- ☞ $N_d(q) = 0$ se $d|q-1$ (criterio di Hermite)
- ☞ $N_d(q)$ è noto per $d < 6$
- ☞ Quasi tutti i PP hanno grado $q-2$

Enumerazione dei PP di grado fissato

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

Problema: Calcolare $N_d(q)$

- $\displaystyle\sum_{d \leq q-2} N_d(q) = q!$ (se $q > 2$, $\partial f_\sigma \leq q-2$)
- $N_1(q) = q(q-1)$ (PP lineari)
- $N_d(q) = 0$ se $d|q-1$ (criterio di Hermite)
- $N_d(q)$ è noto per $d < 6$
- Quasi tutti i PP hanno grado $q-2$

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

Enumerazione dei PP di grado fissato

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

Problema: Calcolare $N_d(q)$

- $\displaystyle\sum_{d \leq q-2} N_d(q) = q!$ (se $q > 2$, $\partial f_\sigma \leq q-2$)
- $N_1(q) = q(q-1)$ (PP lineari)
- $N_d(q) = 0$ se $d | q-1$ (criterio di Hermite)
- $N_d(q)$ è noto per $d < 6$
- Quasi tutti i PP hanno grado $q-2$

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

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

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

Altro modo di contare

Altro modo di contare

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

Altro modo di contare

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

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

Altro modo di contare

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

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

☞ $c_{\sigma_1} = c_{\sigma_2}$ se σ_1 e σ_2 sono coniugate (i.e. $c_\sigma = c_{\mathcal{C}(\sigma)}$)

Altro modo di contare

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

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

- ☞ $c_{\sigma_1} = c_{\sigma_2}$ se σ_1 e σ_2 sono coniugate (i.e. $c_\sigma = c_{\mathcal{C}(\sigma)}$)
- ☞ $\mathcal{C} \subset \mathcal{S}(\mathbb{F}_q)$ classe di coniugazione

Altro modo di contare

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

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

- $c_{\sigma_1} = c_{\sigma_2}$ se σ_1 e σ_2 sono coniugate (i.e. $c_\sigma = c_{\mathcal{C}(\sigma)}$)
- $\mathcal{C} \subset \mathcal{S}(\mathbb{F}_q)$ classe di coniugazione
- Funzioni naturali:

Altro modo di contare

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

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

- $c_{\sigma_1} = c_{\sigma_2}$ se σ_1 e σ_2 sono coniugate (i.e. $c_\sigma = c_{\mathcal{C}(\sigma)}$)
- $\mathcal{C} \subset \mathcal{S}(\mathbb{F}_q)$ classe di coniugazione
- Funzioni naturali:
  - ✗ $m_{\mathcal{C}}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma = q - c_{\mathcal{C}}\}$ (grado minimale)

Altro modo di contare

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

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

- $c_{\sigma_1} = c_{\sigma_2}$ se σ_1 e σ_2 sono coniugate (i.e. $c_\sigma = c_{\mathcal{C}(\sigma)}$)
- $\mathcal{C} \subset \mathcal{S}(\mathbb{F}_q)$ classe di coniugazione
- Funzioni naturali:
  - ✗ $m_{\mathcal{C}}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma = q - c_{\mathcal{C}}\}$ (grado minimale)
  - ✗ $M_{\mathcal{C}}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma < q - 2\}$ (grado non-massimale)

Altro modo di contare

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

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

- $c_{\sigma_1} = c_{\sigma_2}$ se σ_1 e σ_2 sono coniugate (i.e. $c_\sigma = c_{\mathcal{C}(\sigma)}$)
- $\mathcal{C} \subset \mathcal{S}(\mathbb{F}_q)$ classe di coniugazione
- Funzioni naturali:
  - ✗ $m_{\mathcal{C}}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma = q - c_{\mathcal{C}}\}$ (grado minimale)
  - ✗ $M_{\mathcal{C}}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma < q - 2\}$ (grado non-massimale)

Teorema *C. Malvenuto, FP* (2002)

✎ Se $\mathcal{C} \neq [2], [3], [2\ 2]$, allora

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

✎ Formule esplicite per $M_{\mathcal{C}}(q)$ se $c_{\mathcal{C}} \leq 6$

Formule per PP con grado non massimale

Formule per PP con grado non massimale

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

char$(\mathbb{F}_q) > 3$ e η è il carattere quadratico

Formule per PP con grado non massimale

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

$\mathrm{char}(\mathbb{F}_q) > 3$ e η è il carattere quadratico

PP con grado minimale

Formule per PP con grado non massimale

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

char$(\mathbb{F}_q) > 3$ e η è il carattere quadratico

PP con grado minimale

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

Formule per PP con grado non massimale

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

char$(\mathbb{F}_q) > 3$ e η è il carattere quadratico

PP con grado minimale

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

Teorema *C. Malvenuto, FP* (in stampa)

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

Risultato di Oggi

Risultato di Oggi

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

Risultato di Oggi

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

Teorema *S. Konyagin, FP*

Sia $\alpha = (e-2)/3e = 0.08808\cdots$ *e* $d < \alpha q$. *Allora*

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

Se segue che

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

se $d \leq \alpha q$ *e* $\alpha < 0.03983$

Risultato di Oggi

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

Teorema *S. Konyagin, FP*

Sia $\alpha = (e-2)/3e = 0.08808\cdots$ *e* $d < \alpha q$. *Allora*

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

Se segue che

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

se $d \le \alpha q$ *e* $\alpha < 0.03983$

Nota: Il massimo possibile valore per α nel teorema è $0,5$. Infatti $\partial f_\sigma \ne (q-1)/2$ se q è dispari. Quindi

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

Prototipo di dimostrazione

Prototipo di dimostrazione

Il coefficiente di x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ è 0 se e solo se

Prototipo di dimostrazione

Il coefficiente di x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ è 0 se e solo se

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

Prototipo di dimostrazione

Il coefficiente di x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ è 0 se e solo se

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

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

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

Prototipo di dimostrazione

Il coefficiente di x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ è 0 se e solo se

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

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

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

"Inclusione-Esclusione" implica

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

Prototipo di dimostrazione

Il coefficiente di x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ è 0 se e solo se

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

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

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

"Inclusione-Esclusione" implica

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

Prototipo di dimostrazione

Il coefficiente di x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ è 0 se e solo se

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

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

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

"Inclusione-Esclusione" implica

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

Prototipo di dimostrazione

Il coefficiente di x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ è 0 se e solo se

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

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

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

"Inclusione-Esclusione" implica

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

Prototipo di dimostrazione

Il coefficiente di x^j in $f_\sigma(x) := \sum_{c\in\mathbb{F}_q} \sigma(c)\left(1-(x-c)^{q-1}\right)$ è 0 se e solo se

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

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

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

"Inclusione-Esclusione" implica

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

Bisogna valutare n_S. Sia $e_p(u) = e^{\frac{2\pi i u}{p}}$ e $\mathrm{Tr}(\alpha) \in \mathbb{F}_p$ la traccia di $\alpha \in \mathbb{F}_q$.

Allora

Allora

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

Allora

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

Allora

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

Allora

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

Allora

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

dove

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

Inoltre, siccome la media geometrica è sempre inferiore alla media aritmetica, si ha

Inoltre, siccome la media geometrica è sempre inferiore alla media aritmetica, si ha

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

Inoltre, siccome la media geometrica è sempre inferiore alla media aritmetica, si ha

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

Inoltre, siccome la media geometrica è sempre inferiore alla media aritmetica, si ha

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

Inoltre, siccome la media geometrica è sempre inferiore alla media aritmetica, si ha

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

Inoltre, siccome la media geometrica è sempre inferiore alla media aritmetica, si ha

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

Sostituiamo la stima per $|R_S|$ in (2) e poi in (1). Quindi

Sostituiamo la stima per $|R_S|$ in (2) e poi in (1). Quindi

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

Sostituiamo la stima per $|R_S|$ in (2) e poi in (1). Quindi

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

Sostituiamo la stima per $|R_S|$ in (2) e poi in (1). Quindi

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

Sostituiamo la stima per $|R_S|$ in (2) e poi in (1). Quindi

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

Sostituiamo la stima per $|R_S|$ in (2) e poi in (1). Quindi

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

Sostituiamo la stima per $|R_S|$ in (2) e poi in (1). Quindi

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

Questo dimostra che

Sostituiamo la stima per $|R_S|$ in (2) e poi in (1). Quindi

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

Questo dimostra che $\boxed{\mathcal{N}_d \sim \frac{q!}{q^d}}$

Sostituiamo la stima per $|R_S|$ in (2) e poi in (1). Quindi

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

Questo dimostra che $\boxed{\mathcal{N}_d \sim \frac{q!}{q^d}}$ se $\boxed{d < \frac{q}{\log q}\left(\frac{1}{2}\log\log q - \log\log\log q\right)}$

Sostituiamo la stima per $|R_S|$ in (2) e poi in (1). Quindi

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

Questo dimostra che $\boxed{\mathcal{N}_d \sim \frac{q!}{q^d}}$ se $\boxed{d < \frac{q}{\log q}\left(\frac{1}{2}\log\log q - \log\log\log q\right)}$

La vera dimostrazione è un'evoluzione di questo metodo. $\square$

Sostituiamo la stima per $|R_S|$ in (2) e poi in (1). Quindi

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

Questo dimostra che $\boxed{\mathcal{N}_d \sim \frac{q!}{q^d}}$ se $\boxed{d < \frac{q}{\log q}\left(\frac{1}{2}\log\log q - \log\log\log q\right)}$

La vera dimostrazione è un'evoluzione di questo metodo. □

– FINE –