ENTROPY

IN

ALGEBRAIC INDEPENDENCE TESTING

JR-FEST, ICTS-TIFR

May 09, 2025.

PRERONA CHATTERJEE

(IIT MADRAS)

Algebraic Independence

Vector Space: $\mathbb{R}^3$ over $\mathbb{R}$.

$$v_1 = (1,0,1) \qquad v_2 = (0,1,0) \qquad v_3 = (1,2,1).$$

are linearly dependent since $v_1 + 2v_2 - v_3 = \overline{0}$

Algebraic Independence

Vector Space: $\mathbb{R}^3$ over $\mathbb{R}$.

$$v_1 = (1,0,1) \qquad v_2 = (0,1,0) \qquad v_3 = (1,2,1).$$

are linearly dependent since $v_1 + 2v_2 - v_3 = \overline{0}$

Space of bi-variate polynomials over $\mathbb{C}$.

$$f_1 = x^2 \qquad f_2 = y^2 \qquad f_3 = xy$$

are algebraically dependent since $f_1 f_2 - f_3^2 = 0$.

Algebraic Independence

$f_1, f_2, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$ are said to be algebraically dependent if there exists an $A \in \mathbb{F}[y_1, \ldots, y_k]$ such that $A(y_1, \ldots, y_k) \neq 0$ but $A(f_1, \ldots, f_k) = 0$.

Algebraic Independence

$f_1, f_2, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$ are said to be **algebraically dependent** if there exists an $A \in \mathbb{F}[y_1, \ldots, y_k]$ such that $A(y_1, \ldots, y_k) \neq 0$ but $A(f_1, \ldots, f_k) = 0$.

Note: Underlying field is important.

For a prime p, $x^p + y^p$, $x + y$ are

Algebraic Independence

$f_1, f_2, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$ are said to be algebraically dependent if there exists an $A \in \mathbb{F}[y_1, \ldots, y_k]$ such that $A(y_1, \ldots, y_k) \neq 0$ but $A(f_1, \ldots, f_k) = 0$.

Note: Underlying field is important.

For a prime p, $x^p + y^p$, $x + y$ are

- algebraically independent over $\mathbb{C}$;

Algebraic Independence

$f_1, f_2, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$ are said to be algebraically dependent if there exists an $A \in \mathbb{F}[y_1, \ldots, y_k]$ such that $A(y_1, \ldots, y_k) \neq 0$ but $A(f_1, \ldots, f_k) = 0$.

Note: Underlying field is important.

For a prime p, $x^p + y^p$, $x + y$ are

- algebraically independent over $\mathbb{C}$;
- algebraically dependent over $\mathbb{F}_p$.

Testing Algebraic Independence

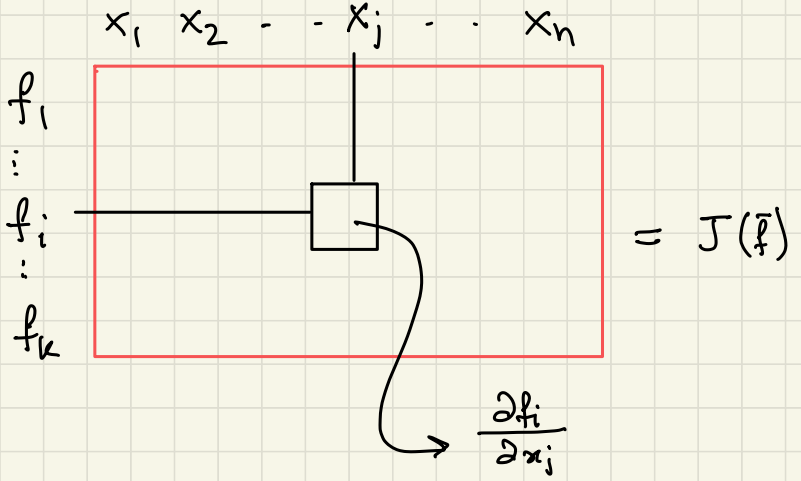
Given a set of polynomials $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$. how efficiently can one test whether they are algebraically independent?

Testing Algebraic Independence

Given a set of polynomials $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$, how efficiently can one test whether they are algebraically independent?

Over fields of characteristic zero.

Jacobian Criterion:



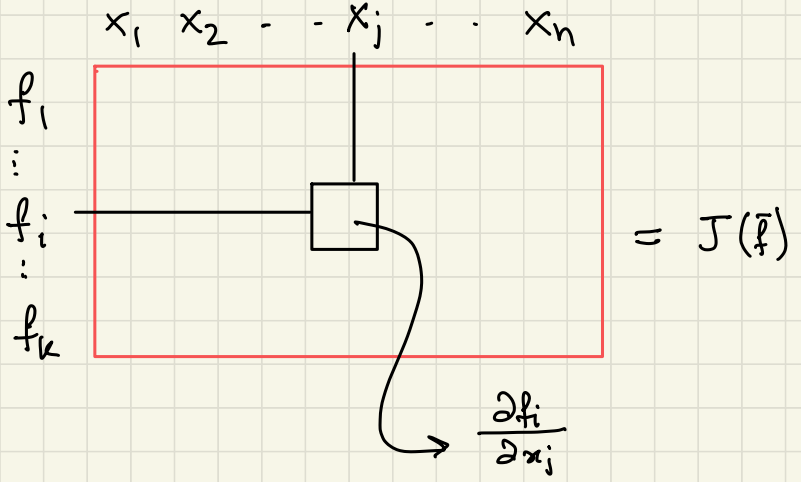
Testing Algebraic Independence

Given a set of polynomials $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$, how efficiently can one test whether they are algebraically independent?

Over fields of characteristic zero.

Jacobian Criterion:

$f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$ are algebraically independent iff $J(\bar{f})$ has full rank.



Testing Algebraic Independence

Over characteristic zero fields, $\mathrm{AD}(\mathbb{F}) \in \mathrm{coRP}$ due to Jacobian Criterion.

Testing Algebraic Independence

Over characteristic zero fields, $\mathrm{AD}(\mathbb{F}) \in \mathrm{coRP}$ due to Jacobian Criterion.

What about fields of positive characteristic?

Testing Algebraic Independence

Over characteristic zero fields, $AD(\mathbb{F}) \in coRP$ due to Jacobian Criterion.

What about fields of positive characteristic?

- Perron's Bound on the degree of the annihilators of $f_1, \ldots, f_k \Rightarrow AD(\mathbb{F}_q) \in PSPACE$

Testing Algebraic Independence

Over characteristic zero fields, $AD(\mathbb{F}) \in coRP$ due to Jacobian Criterion.

What about fields of positive characteristic?

- Perron's Bound on the degree of the annihilators of $f_1, \ldots, f_k \Rightarrow AD(\mathbb{F}_q) \in PSPACE$
- Mittmann, Saxena, Scheiblechner (2014) showed that $AD(\mathbb{F}_q) \in NP^{\#P}$.

Testing Algebraic Independence

Over characteristic zero fields, $AD(\mathbb{F}) \in coRP$ due to Jacobian Criterion.

What about fields of positive characteristic?

- Perron's Bound on the degree of the annihilators of $f_1, \ldots, f_k \Rightarrow AD(\mathbb{F}_q) \in PSPACE$
- Mittmann, Saxena, Scheiblechner (2014) showed that $AD(\mathbb{F}_q) \in NP^{\#P}$.
- Guo, Saxena, Sinhababu (2019) showed that $AD(\mathbb{F}_q) \in AM \cap co\text{-}AM$.

Testing Algebraic Independence in AM ∩ co-AM.

Core Observation: Let $f_1, \ldots, f_k \in \mathbb{F}_q[x_1, \ldots, x_n]$.

For any $(b_1, \ldots, b_k) \in \mathbb{F}_q$, let N_b be the number of solutions to the system of equations $\{f_i = b_i\}$.

Testing Algebraic Independence in AM ∩ co-AM.

Core Observation: Let $f_1, \ldots, f_k \in \mathbb{F}_q[x_1, \ldots, x_n]$.

For any $(b_1, \ldots, b_k) \in \mathbb{F}_q$, let N_b be the number of solutions to the system of equations $\{f_i = b_i\}$.

(1) For a random point $\bar{a} \in \mathbb{F}_q^n$

- if $f_1, \ldots, f_k$ are independent, then $N_{f(a)}$ is small.
- if $f_1, \ldots, f_k$ are dependent, then $N_{f(a)}$ is large.

Testing Algebraic Independence in AM ∩ co-AM.

Core Observation: Let $f_1, \ldots, f_k \in \mathbb{F}_q[x_1, \ldots, x_n]$.

For any $(b_1, \ldots, b_k) \in \mathbb{F}_q$, let N_b be the number of solutions to the system of equations $\{f_i = b_i\}$.

(1) For a random point $\bar{a} \in \mathbb{F}_q^n$
- if $f_1, \ldots, f_k$ are independent, then $N_{f(a)}$ is small.
- if $f_1, \ldots, f_k$ are dependent, then $N_{f(a)}$ is large.

(2) For a random point $\bar{b} \in \mathbb{F}_q^k$
- if $f_1, \ldots, f_k$ are independent, then $N_b = 0$ for most b.
- if $f_1, \ldots, f_k$ are dependent, then $N_b \geq 1$ for many b.

Restating the Observation in terms of Entropy.

(1)
- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

Restating the Observation in terms of Entropy.

(1)
- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

For any distribution Y with min-entropy $\ge n \log\left(\frac{|\mathbb{F}|}{d}\right)$,

Restating the Observation in terms of Entropy.

(1)
- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

For any distribution Y with min-entropy $\ge n \log\left(\frac{|\mathbb{F}|}{d}\right)$,

No element is picked with probability $> \left(\frac{d}{|\mathbb{F}|}\right)^n$

Restating the Observation in terms of Entropy.

(1)
- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \le d \quad \forall i$
- $X = f(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

For any distribution Y with min-entropy $\ge n \log\left(\frac{|\mathbb{F}|}{d}\right)$,

$$|X - Y|_{TV} \ge c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}.$$

No element is picked with probability $> \left(\frac{d}{|\mathbb{F}|}\right)^n$

Restating the Observation in terms of Entropy.

(2)

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically independent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

Restating the Observation in terms of Entropy.

(2)

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically independent
- $\deg(f_i) \le d \quad \forall i$
- $X = \overline{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

There is a distribution Y with

$$\text{min-entropy} \ge n \log\left(\frac{|\mathbb{F}|}{d}\right) - \log\left(\frac{2cd^n}{2cd^n - 1}\right)$$

Restating the Observation in terms of Entropy.

(2)

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically independent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

There is a distribution Y with

$$\text{min-entropy} \ge n \log\left(\frac{|\mathbb{F}|}{d}\right) - \log\left(\frac{2cd^n}{2cd^n - 1}\right)$$

such that $|X - Y|_{TV} \le n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\ n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

For any distribution Y with min-entropy $\ge n \log\left(\frac{|\mathbb{F}|}{d}\right)$,

$$|X - Y|_{TV} \ge c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}.$$

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\ n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically independent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

There is a distribution Y with

$$\text{min-entropy} \ge n \log\left(\frac{|\mathbb{F}|}{d}\right) - \log\left(\frac{2cd^n}{2cd^n - 1}\right)$$

such that $|X - Y|_{TV} \le n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

Proof of (1)

A : Annihilator of $f_1, \dots, f_n$

Perron's bound $\Rightarrow$

$$\deg(A) \leq d^n.$$

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \dots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \leq d \quad \forall i$
- $X = f(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

For any distribution Y with min-entropy $\geq n \log\left(\frac{|\mathbb{F}|}{d}\right)$,

$$|X - Y|_{TV} \geqslant c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}.$$

Proof of ①

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \dots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

For any distribution Y with min-entropy $\ge n \log\left(\frac{|\mathbb{F}|}{d}\right)$,

$$|X - Y|_{TV} \ge c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}.$$

A : Annihilator of $f_1, \dots, f_n$

Perron's bound $\Rightarrow$

$$\deg(A) \le d^n.$$

For any $\bar{b} \in \mathrm{Im}(\bar{f})$,

$$A(\bar{b}) = A(f(\bar{a})) \text{ for some } \bar{a} \Rightarrow A(\bar{b}) = 0.$$

Proof of ①

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \dots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

For any distribution Y with min-entropy $\ge n \log\left(\frac{|\mathbb{F}|}{d}\right)$,

$$|X - Y|_{TV} \ge c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}.$$

A : Annihilator of $f_1, \dots, f_n$

Perron's bound $\Rightarrow$

$$\deg(A) \le d^n.$$

For any $\bar{b} \in \mathrm{Im}(\bar{f})$,

$$A(\bar{b}) = A(f(\bar{a})) \text{ for some } \bar{a} \Rightarrow A(\bar{b}) = 0.$$

Thus $|\mathrm{Supp}(X)| = |\mathrm{Im}(\bar{f})| \le \frac{d^n}{|\mathbb{F}|} \cdot |\mathbb{F}|^n = d^n \cdot |\mathbb{F}|^{n-1}$

Proof of ①

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \dots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

For any distribution Y with min-entropy $\ge n \log\left(\frac{|\mathbb{F}|}{d}\right)$,

$$|X - Y|_{TV} \ge c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}.$$

A : Annihilator of $f_1, \dots, f_n$

Perron's bound $\Rightarrow$

$$\deg(A) \le d^n.$$

For any $\bar{b} \in \mathrm{Im}(\bar{f})$,

$$A(\bar{b}) = A(f(\bar{a})) \text{ for some } \bar{a} \Rightarrow A(\bar{b}) = 0.$$

Thus $|\mathrm{Supp}(X)| = |\mathrm{Im}(\bar{f})| \le \frac{d^n}{|\mathbb{F}|} \cdot |\mathbb{F}|^n = d^n \cdot |\mathbb{F}|^{n-1}$

Choose $S = \mathrm{Supp}(Y) \setminus \mathrm{Supp}(X)$.

Proof of ①

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \dots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

For any distribution Y with min-entropy $\ge n \log\left(\frac{|\mathbb{F}|}{d}\right)$,

$$|X - Y|_{TV} \ge c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}.$$

A : Annihilator of $f_1, \dots, f_n$

Perron's bound $\Rightarrow$

$$\deg(A) \le d^n.$$

For any $\bar{b} \in \mathrm{Im}(\bar{f})$,

$$A(\bar{b}) = A(f(\bar{a})) \text{ for some } \bar{a} \Rightarrow A(\bar{b}) = 0.$$

Thus $|\mathrm{Supp}(X)| = |\mathrm{Im}(\bar{f})| \le \frac{d^n}{|\mathbb{F}|} \cdot |\mathbb{F}|^n = d^n \cdot |\mathbb{F}|^{n-1}$

Choose $S = \mathrm{Supp}(Y) \setminus \mathrm{Supp}(X)$. $\Rightarrow \Pr_X(S) = 0$.

To Show: $|X - Y|_{TV} \geq c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

$\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$

Y has min-entropy $\geq n \log\left(\frac{|\mathbb{F}|}{d}\right)$

$|\mathrm{Supp}(X)| \leq d^n \cdot |\mathbb{F}|^{n-1}$

$S = \mathrm{Supp}(Y) \setminus \mathrm{Supp}(X)$.

To Show: $|X-Y|_{TV} \geq c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

$$|X-Y| \geq \left| P^{X}_{\gamma}(S) - P^{Y}_{\gamma}(S) \right|$$

$$= P^{Y}_{\gamma}(S)$$

$\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$

Y has min-entropy $\geq n \log\left(\frac{|\mathbb{F}|}{d}\right)$

$|\mathrm{Supp}(X)| \leq d^n \cdot |\mathbb{F}|^{n-1}$

$S = \mathrm{Supp}(Y) \setminus \mathrm{Supp}(X)$.

To Show: $|X-Y|_{TV} \geq c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

$\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$

Y has min-entropy $\geq n \log\left(\frac{|\mathbb{F}|}{d}\right)$

$|\mathrm{Supp}(X)| \leq d^n \cdot |\mathbb{F}|^{n-1}$

$S = \mathrm{Supp}(Y) \setminus \mathrm{Supp}(X)$.

$$|X-Y| \geq \left| \Pr_X(S) - \Pr_Y(S) \right|$$

$$= \Pr_Y(S) = 1 - \Pr_Y(\overline{S})$$

where $\overline{S} = \mathrm{Supp}(Y) \cap \mathrm{Supp}(X)$.

To Show: $|X-Y|_{TV} \geq c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

$\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$

Y has min-entropy $\geq n \log\left(\frac{|\mathbb{F}|}{d}\right)$

$|\mathrm{Supp}(X)| \leq d^n \cdot |\mathbb{F}|^{n-1}$

$S = \mathrm{Supp}(Y) \setminus \mathrm{Supp}(X)$.

$$|X-Y| \geq \left| P^{\gamma}_{X}(S) - P^{\gamma}_{Y}(S) \right|$$

$$= P^{\gamma}_{Y}(S) = 1 - P^{\gamma}_{Y}(\bar{S})$$

where $\bar{S} = \mathrm{Supp}(Y) \cap \mathrm{Supp}(X)$.

$$P^{\gamma}_{Y}(\bar{S}) \leq |\bar{S}| \cdot \left(\frac{d}{|\mathbb{F}|}\right)^n$$ due to the min-entropy condition.

To Show: $|X-Y|_{TV} \geq c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

$\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$

Y has min-entropy $\geq n \log\left(\frac{|\mathbb{F}|}{d}\right)$

$|\mathrm{Supp}(X)| \leq d^n \cdot |\mathbb{F}|^{n-1}$

$S = \mathrm{Supp}(Y) \setminus \mathrm{Supp}(X)$.

$$|X-Y| \geq \left| P^{\gamma}_{X}(S) - P^{\gamma}_{Y}(S) \right|$$

$$= P^{\gamma}_{Y}(S) = 1 - P^{\gamma}_{Y}(\bar{S})$$

where $\bar{S} = \mathrm{Supp}(Y) \cap \mathrm{Supp}(X)$.

$$P^{\gamma}_{Y}(\bar{S}) \leq |\bar{S}| \cdot \left(\frac{d}{|\mathbb{F}|}\right)^n$$ due to the min-entropy condition.

$$\leq d^n \cdot |\mathbb{F}|^{n-1} \left(\frac{d}{|\mathbb{F}|}\right)^n$$

To Show: $|X-Y|_{TV} \geq c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

$\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$

Y has min-entropy $\geq n \log\left(\frac{|\mathbb{F}|}{d}\right)$

$|\mathrm{Supp}(X)| \leq d^n \cdot |\mathbb{F}|^{n-1}$

$S = \mathrm{Supp}(Y) \setminus \mathrm{Supp}(X)$.

$$|X-Y| \geq \left| P^X_\gamma(S) - P^Y_\gamma(S) \right|$$

$$= P^Y_\gamma(S) = 1 - P^Y_\gamma(\bar{S})$$

where $\bar{S} = \mathrm{Supp}(Y) \cap \mathrm{Supp}(X)$.

$P^Y_\gamma(\bar{S}) \leq |\bar{S}| \cdot \left(\frac{d}{|\mathbb{F}|}\right)^n$ due to the min-entropy condition.

$$\leq d^n \cdot |\mathbb{F}|^{n-1} \left(\frac{d}{|\mathbb{F}|}\right)^n \Rightarrow |X-Y| \geq c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$$

using the assumption on $|\mathbb{F}|$.

Proof of (2)

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically independent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

There is a distribution Y with

$$\text{min-entropy} \ge n \log\left(\frac{|\mathbb{F}|}{d}\right) - \log\left(\frac{2cd^n}{2cd^n - 1}\right)$$

such that $|X - Y|_{tv} \le n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

Proof of (2)

For $i \in [n]$, define

$A_i \in \mathbb{F}[z, y_1, \ldots, y_n] \equiv$

Annihilator of

$\{x_i, f_1, \ldots, f_n\}$

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically independent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

There is a distribution Y with

$$\text{min-entropy} \ge n \log\left(\frac{|\mathbb{F}|}{d}\right) - \log\left(\frac{2cd^n}{2cd^n - 1}\right)$$

such that $|X - Y|_{tv} \le n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

Proof of (2)

For $i \in [n]$, define

$A_i \in \mathbb{F}[z, y_1, \ldots, y_n] \equiv$

Annihilator of

$\{x_i, f_1, \ldots, f_n\}$

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically independent
- $\deg(f_i) \le d \quad \forall i$
- $X = f(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

There is a distribution Y with

$$\text{min-entropy} \ge n \log\left(\frac{|\mathbb{F}|}{d}\right) - \log\left(\frac{2cd^n}{2cd^n - 1}\right)$$

such that $|X - Y|_{tv} \le n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

$$S = \left\{ \bar{a} \in \mathbb{F}^n : A_i(z, f(\bar{a})) \neq 0 \quad \forall i \in [n] \right\}. \qquad Y = f(U_S).$$

Proof of (2)

For $i \in [n]$, define

$A_i \in \mathbb{F}[z, y_1, \ldots, y_n] \equiv$

Annihilator of

$\{x_i, f_1, \ldots, f_n\}$

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\, n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically independent
- $\deg(f_i) \le d \quad \forall i$
- $X = f(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

There is a distribution Y with

$$\text{min-entropy} \ge n \log\left(\frac{|\mathbb{F}|}{d}\right) - \log\left(\frac{2cd^n}{2cd^n - 1}\right)$$

such that $|X - Y|_{TV} \le n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

$$S = \left\{\bar{a} \in \mathbb{F}^n : A_i(z, f(\bar{a})) \neq 0 \quad \forall i \in [n]\right\}. \qquad Y = f(U_S).$$

Claim:
- min-entropy of $Y \ge n \log\left(\frac{|\mathbb{F}|}{d}\right) - \log\left(\frac{2cd^n}{2cd^n - 1}\right)$
- $|X - Y|_{TV} \le n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$

Estimating $|S|$:

Let $A_i = \sum_{j=0}^{d_i} A_{ij}(\bar{y}) \cdot z^j$

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, f(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

Estimating $|S|$:

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, f(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

Let $A_i = \sum_{j=0}^{d_i} A_{ij}(\bar{y}) \cdot z^j$

Then $A_{id_i}(\bar{f}(\bar{x})) \neq 0$ since $f_1 \ldots f_n$ are alg. independent.

Estimating $|S|$:

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, f(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

Let $A_i = \sum_{j=0}^{d_i} A_{ij}(\bar{y}) \cdot z^j$

Then $A_{id_i}(\bar{f}(\bar{x})) \neq 0$ since $f_1 \ldots f_n$ are alg. independent.

Note: $\deg_{\bar{x}}\left(A_{id_i}(\bar{f}(\bar{x}))\right) \leq \prod_{i=1}^{n} \deg(f_i) \times \max_{i \in [n]} \deg_{\bar{x}}(f_i)$

Estimating $|S|$:

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, f(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

Let $A_i = \sum_{j=0}^{d_i} A_{ij}(\bar{y}) \cdot z^j$

Then $A_{id_i}(\bar{f}(\bar{x})) \neq 0$ since $f_1 \ldots f_n$ are alg. independent.

Note: $\deg_{\bar{x}}\left(A_{id_i}(\bar{f}(\bar{x}))\right) \leq \prod_{i=1}^{n} \deg(f_i) \times \max_{i \in [n]} \deg_{\bar{x}}(f_i)$

$\leq d^{n+1}$

Estimating $|S|$:

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, f(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

Let $A_i = \sum_{j=0}^{d_i} A_{ij}(\bar{y}) \cdot z^j$

Then $A_{id_i}(\bar{f}(\bar{x})) \neq 0$ since $f_1 \ldots f_n$ are alg. independent.

Note: $\deg_{\bar{x}}\left(A_{id_i}(\bar{f}(\bar{x}))\right) \leq \prod_{i=1}^{n} \deg(f_i) \times \max_{i \in [n]} \deg_{\bar{x}}(f_i)$

$\leq d^{n+1}$

Thus $\Pr_{\bar{a} \in_{u.a.r} \mathbb{F}^n}\left[A_{id_i}(\bar{f}(\bar{a}))\right] \leq \frac{d^{n+1}}{|\mathbb{F}|}$.

Estimating $|S|$:

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, f(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

Let $A_i = \sum_{j=0}^{d_i} A_{ij}(\bar{y}) \cdot z^j$

Then $A_{id_i}(\bar{f}(\bar{x})) \neq 0$ since $f_1 \ldots f_n$ are alg. independent.

Note: $\deg_{\bar{x}}\left(A_{id_i}(\bar{f}(\bar{x}))\right) \leq \prod_{i=1}^{n} \deg(f_i) \times \max_{i \in [n]} \deg_{\bar{x}}(f_i)$

$\leq d^{n+1}$

Thus $\Pr_{\bar{a} \in_{u.a.r} \mathbb{F}^n}\left[A_{id_i}(\bar{f}(\bar{a}))\right] \leq \frac{d^{n+1}}{|\mathbb{F}|}$.

$\Rightarrow \Pr_{\bar{a} \in_{u.a.r} \mathbb{F}^n}\left[\exists i \; A_{id_i}(\bar{f}(\bar{a}))\right] \leq \frac{n \cdot d^{n+1}}{|\mathbb{F}|}$

Estimating $|S|$:

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, f(\bar{a})) \neq 0 \ \ \forall i \in [n]\}$.

Let $A_i = \sum_{j=0}^{d_i} A_{ij}(\bar{y}) \cdot z^j$

Then $A_{id_i}(\bar{f}(\bar{x})) \neq 0$ since $f_1 \ldots f_n$ are alg. independent.

Note: $\deg_{\bar{x}}\left(A_{id_i}(\bar{f}(\bar{x}))\right) \leq \prod_{i=1}^{n} \deg(f_i) \times \max_{i \in [n]} \deg_{\bar{x}}(f_i)$

$\leq d^{n+1}$

Thus $\Pr_{\bar{a} \in_{u.a.r} \mathbb{F}^n}\left[A_{id_i}(\bar{f}(\bar{a}))\right] \leq \frac{d^{n+1}}{|\mathbb{F}|}$.

$\Rightarrow \Pr_{\bar{a} \in_{u.a.r} \mathbb{F}^n}\left[\exists i \ A_{id_i}(\bar{f}(\bar{a}))\right] \leq \frac{n \cdot d^{n+1}}{|\mathbb{F}|}$

$\Rightarrow |S| \geq (1-\delta) \cdot |\mathbb{F}|^n$ where $\delta = \frac{1}{2cd^n}$

Computing min-entropy of Y.

Let $\bar{b} \in f(S)$.

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, \bar{f}(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

$Y = f(U_S)$.

Computing min-entropy of Y.

Let $\bar{b} \in f(S)$.

$$N_{\bar{b}} = \{\bar{a} \in \mathbb{F}^n : f_i(\bar{a}) = b_i \ \forall i\}$$
$$= \{\bar{a} \in S : f_i(\bar{a}) = b_i \ \forall i\}$$

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, \bar{f}(\bar{a})) \neq 0 \ \forall i \in [n]\}$.

$Y = f(U_S)$.

Computing min-entropy of Y.

Let $\bar{b} \in f(S)$.

$$N_{\bar{b}} = \{\bar{a} \in \mathbb{F}^n : f_i(\bar{a}) = b_i \ \forall i\}$$
$$= \{\bar{a} \in S : f_i(\bar{a}) = b_i \ \forall i\}$$

Thus, $P_\sigma(Y = \bar{b}) = \begin{cases} \frac{|N_{\bar{b}}|}{|S|} & \text{if } \bar{b} \in f(S) \\ 0 & \text{otherwise} \end{cases}$

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, \bar{f}(\bar{a})) \neq 0 \ \forall i \in [n]\}$.

$Y = f(U_S)$.

Computing min-entropy of Y.

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, \bar{f}(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

$Y = f(U_S)$.

Let $\bar{b} \in f(S)$.

$$N_{\bar{b}} = \{\bar{a} \in \mathbb{F}^n : f_i(\bar{a}) = b_i \ \forall i\}$$
$$= \{\bar{a} \in S : f_i(\bar{a}) = b_i \ \forall i\}$$

Thus, $$P_r(Y = \bar{b}) = \begin{cases} \frac{|N_{\bar{b}}|}{|S|} & \text{if } \bar{b} \in f(S) \\ 0 & \text{otherwise} \end{cases}$$

Let $\tilde{N}_{\bar{b}} = \{\bar{a} \in \overline{\mathbb{F}}^n : f_i(\bar{a}) = \bar{b} \ \forall i\}$. and $A_i'(z) = A_i(z, \bar{b})$.

Computing min-entropy of Y.

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, \bar{f}(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

$Y = f(U_S)$.

Let $\bar{b} \in f(S)$.

$$N_{\bar{b}} = \{\bar{a} \in \mathbb{F}^n : f_i(\bar{a}) = b_i \ \forall i\}$$
$$= \{\bar{a} \in S : f_i(\bar{a}) = b_i \ \forall i\}$$

Thus, $$P_r(Y = \bar{b}) = \begin{cases} \frac{|N_{\bar{b}}|}{|S|} & \text{if } \bar{b} \in f(S) \\ 0 & \text{otherwise} \end{cases}$$

Let $\tilde{N}_{\bar{b}} = \{\bar{a} \in \overline{\mathbb{F}}^n : f_i(\bar{a}) = \bar{b} \ \forall i\}$. and $A_i'(z) = A_i(z, \bar{b})$.

Then $\tilde{N}_{\bar{b}} \subseteq$ Roots of $\{A_i'(z)\}_{i \in [n]}$

Computing min-entropy of Y.

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, \bar{f}(\bar{a})) \neq 0 \ \forall i \in [n]\}$.

$Y = f(U_S)$.

Let $\bar{b} \in f(S)$.

$$N_{\bar{b}} = \{\bar{a} \in \mathbb{F}^n : f_i(\bar{a}) = b_i \ \forall i\}$$
$$= \{\bar{a} \in S : f_i(\bar{a}) = b_i \ \forall i\}$$

Thus, $$P_r(Y = \bar{b}) = \begin{cases} \frac{|N_{\bar{b}}|}{|S|} & \text{if } \bar{b} \in f(S) \\ 0 & \text{otherwise} \end{cases}$$

Let $\tilde{N}_{\bar{b}} = \{\bar{a} \in \overline{\mathbb{F}}^n : f_i(\bar{a}) = \bar{b} \ \forall i\}$. and $A_i'(z) = A_i(z, \bar{b})$.

Then $\tilde{N}_{\bar{b}} \subseteq$ Roots of $\{A_i'(z)\}_{i \in [n]} \Rightarrow |\tilde{N}_{\bar{b}}| \leq \prod_{i=1}^{n} \deg_z(A_i') < 2^n$.

Computing min-entropy of Y.

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, \bar{f}(\bar{a})) \neq 0 \ \forall i \in [n]\}$.

$Y = f(U_S)$.

Let $\bar{b} \in f(S)$.

$$N_{\bar{b}} = \{\bar{a} \in \mathbb{F}^n : f_i(\bar{a}) = b_i \ \forall i\}$$
$$= \{\bar{a} \in S : f_i(\bar{a}) = b_i \ \forall i\}$$

Thus, $$\Pr(Y = \bar{b}) = \begin{cases} \frac{|N_{\bar{b}}|}{|S|} & \text{if } \bar{b} \in f(S) \\ 0 & \text{otherwise} \end{cases}$$

Let $\tilde{N}_{\bar{b}} = \{\bar{a} \in \overline{\mathbb{F}}^n : f_i(\bar{a}) = \bar{b} \ \forall i\}$. and $A_i'(z) = A_i(z, \bar{b})$.

Then $\tilde{N}_{\bar{b}} \subseteq$ Roots of $\{A_i'(z)\}_{i \in [n]} \Rightarrow |\tilde{N}_{\bar{b}}| \leq \prod_{i=1}^{n} \deg_z(A_i') < \infty$.

Bezout $\Rightarrow |\tilde{N}_{\bar{b}}| \leq \prod_{i=1}^{n} \deg(g_i)$ where $g_i = f_i(x) - b_i$

Computing min-entropy of Y.

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, \bar{f}(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

$Y = f(U_S)$.

let $\bar{b} \in f(S)$.

Then $P_r(Y = \bar{b})$

$$= \begin{cases} \frac{|N_{\bar{b}}|}{|S|} & \text{if } \bar{b} \in f(S) \\ 0 & \text{otherwise} \end{cases}$$

Computing min-entropy of Y.

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, \bar{f}(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

$Y = f(U_S)$.

let $\bar{b} \in f(S)$.

Then $P_D(Y = \bar{b})$

$$= \begin{cases} \frac{|N_{\bar{b}}|}{|S|} & \text{if } \bar{b} \in f(S) \\ 0 & \text{otherwise} \end{cases}$$

where $|S| \geq \left(1 - \frac{1}{2cd^n}\right) \cdot |\mathbb{F}|^n$

Computing min-entropy of Y.

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, \bar{f}(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

$Y = f(U_S)$.

let $\bar{b} \in f(S)$.

Then $P_D(Y = \bar{b})$

$$= \begin{cases} \frac{|N_{\bar{b}}|}{|S|} & \text{if } \bar{b} \in f(S) \\ 0 & \text{otherwise} \end{cases}$$

where $|S| \geq \left(1 - \frac{1}{2cd^n}\right) \cdot |\mathbb{F}|^n$

and $|N_{\bar{b}}| \leq |\hat{N}_{\bar{b}}| \leq d^n$

Computing min-entropy of Y.

$A_i \equiv$ Annihilator of $\{x_i, f_1, \ldots, f_n\}$

$S = \{\bar{a} \in \mathbb{F}^n : A_i(z, \bar{f}(\bar{a})) \neq 0 \quad \forall i \in [n]\}$.

$Y = f(U_S)$.

let $\bar{b} \in f(S)$.

Then $P_Y(Y = \bar{b})$

$$= \begin{cases} \frac{|N_{\bar{b}}|}{|S|} & \text{if } \bar{b} \in f(S) \\ 0 & \text{otherwise} \end{cases}$$

where $|S| \geq \left(1 - \frac{1}{2cd^n}\right) \cdot |\mathbb{F}|^n$

and $|N_{\bar{b}}| \leq |\hat{N}_{\bar{b}}| \leq d^n$

$\Rightarrow$ min-entropy of $Y \geq n \log\left(\frac{|\mathbb{F}|}{d}\right) - \log\left(\frac{2cd^n}{2cd^n - 1}\right)$

Computing $|X - Y|$

For any $b \in \mathbb{F}^n$, $\Pr[X = b] = \frac{|N_b|}{|\mathbb{F}|^n}$

Computing $|X - Y|$

For any $b \in \mathbb{F}^n$, $\Pr[X = b] = \frac{|N_b|}{|\mathbb{F}|^n}$

$$\Leftrightarrow |X - Y| = \frac{1}{2} \sum_{b \in \mathbb{F}^n} \left| \Pr[X = b] - \Pr[Y = b] \right|$$

Computing $|X - Y|$

For any $b \in \mathbb{F}^n$, $\Pr[X = b] = \frac{|N_b|}{|\mathbb{F}|^n}$

$$\Rightarrow |X - Y| = \frac{1}{2} \sum_{b \in \mathbb{F}^n} \left| \Pr[X = b] - \Pr[Y = b] \right|$$

$$\hookrightarrow \begin{cases} |N_b| \cdot \left(\frac{1}{|S|} - \frac{1}{|\mathbb{F}|^n} \right) & \text{if } b \in f(S) \\ \frac{|N_b|}{|\mathbb{F}|^n} & \text{otherwise.} \end{cases}$$

Computing $|X - Y|$

For any $b \in \mathbb{F}^n$, $\Pr[X = b] = \frac{|N_b|}{|\mathbb{F}|^n}$

$$\Rightarrow |X - Y| = \frac{1}{2} \sum_{b \in \mathbb{F}^n} \left| \Pr[X = b] - \Pr[Y = b] \right|$$

$\hookrightarrow$ $\begin{cases} |N_b| \cdot \left(\frac{1}{|S|} - \frac{1}{|\mathbb{F}|^n} \right) & \text{if } b \in f(S) \\ \frac{|N_b|}{|\mathbb{F}|^n} & \text{otherwise.} \end{cases}$

$$\leq n \frac{d^{2n+1}}{|\mathbb{F}|}.$$

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\ n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

For any distribution Y with min-entropy $\ge n \log\left(\frac{|\mathbb{F}|}{d}\right)$,

$$|X - Y|_{TV} \ge c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}.$$

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\ n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically independent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

There is a distribution Y with

$$\text{min-entropy} \ge n \log\left(\frac{|\mathbb{F}|}{d}\right) - \log\left(\frac{2cd^n}{2cd^n - 1}\right)$$

such that $|X - Y|_{TV} \le n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\ n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

For any distribution Y with min-entropy $\ge n \log\left(\frac{|\mathbb{F}|}{d}\right)$,

$$|X - Y|_{TV} \ge c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}.$$

Is $AD(\mathbb{F}_q) \in coRP$?

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\ n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically independent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

There is a distribution Y with

$$\text{min-entropy} \ge n \log\left(\frac{|\mathbb{F}|}{d}\right) - \log\left(\frac{2cd^n}{2cd^n - 1}\right)$$

such that $|X - Y|_{TV} \le n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\ n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically dependent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

For any distribution Y with min-entropy $\ge n \log\left(\frac{|\mathbb{F}|}{d}\right)$,

$$|X - Y|_{TV} \ge c \cdot n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}.$$

Is $AD(\mathbb{F}_q) \in coRP$?

Thank You !!

- $\mathbb{F}$ is a field with $|\mathbb{F}| > 2c\ n d^{2n+1}$
- $f_1, \ldots, f_n \in \mathbb{F}^n \to \mathbb{F}^n$ are algebraically independent
- $\deg(f_i) \le d \quad \forall i$
- $X = \bar{f}(U_n)$ where U_n : Uniform distribution over $\mathbb{F}^n$

There is a distribution Y with

$$\text{min-entropy} \ge n \log\left(\frac{|\mathbb{F}|}{d}\right) - \log\left(\frac{2cd^n}{2cd^n - 1}\right)$$

such that $|X - Y|_{TV} \le n \cdot \frac{d^{2n+1}}{|\mathbb{F}|}$.