An Improved Algorithm for Code Equivalence

Julian Nowakowski **Ruhr University Bochum, Germany**

Code Equivalence

Linear [n,k] code:

Monomial:

Code Equivalence

Linear [n,k] code: subspace $C \subseteq \mathbb{F}_q^n$ of dimension k.

☞ $C = \{\mathbf{x} \cdot \mathbf{G} \mid \mathbf{x} \in \mathbb{F}_q^k\}, \mathbf{G} \in \mathbb{F}_q^{k \times n}$.

Monomial:

Code Equivalence

Linear [n,k] code: subspace $C \subseteq \mathbb{F}_q^n$ of dimension k.

☞ $C = \{\mathbf{x} \cdot \mathbf{G} \mid \mathbf{x} \in \mathbb{F}_q^k\}, \mathbf{G} \in \mathbb{F}_q^{k \times n}$.

Monomial: linear map $\mathbf{Q} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ that preserves Hamming weight.

☞ $\mathbf{Q} \in \mathbb{F}_q^{n \times n}, \quad \mathrm{wt}(\mathbf{v} \cdot \mathbf{Q}) = \mathrm{wt}(\mathbf{v})$ for every $\mathbf{v} \in \mathbb{F}_q^n$.

Code Equivalence

Linear [n,k] code: subspace $C \subseteq \mathbb{F}_q^n$ of dimension k.

☞ $C = \{\mathbf{x} \cdot \mathbf{G} \mid \mathbf{x} \in \mathbb{F}_q^k\}, \mathbf{G} \in \mathbb{F}_q^{k \times n}$.

Monomial: linear map $\mathbf{Q} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ that preserves Hamming weight.

☞ $\mathbf{Q} \in \mathbb{F}_q^{n \times n}, \quad \mathrm{wt}(\mathbf{v} \cdot \mathbf{Q}) = \mathrm{wt}(\mathbf{v})$ for every $\mathbf{v} \in \mathbb{F}_q^n$.

Examples:

- permutations $\mathbf{P}$
- diagonal matrices $\mathbf{D}$ with non-zero diagonal

$$\mathbf{P} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad \mathbf{D} = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

Code Equivalence

Linear [n,k] code: subspace $C \subseteq \mathbb{F}_q^n$ of dimension k.

☞ $C = \{\mathbf{x} \cdot \mathbf{G} \mid \mathbf{x} \in \mathbb{F}_q^k\}, \mathbf{G} \in \mathbb{F}_q^{k \times n}$.

Monomial: linear map $\mathbf{Q} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ that preserves Hamming weight.

☞ $\mathbf{Q} \in \mathbb{F}_q^{n \times n}, \quad \mathrm{wt}(\mathbf{v} \cdot \mathbf{Q}) = \mathrm{wt}(\mathbf{v})$ for every $\mathbf{v} \in \mathbb{F}_q^n$.

Examples:

- permutations $\mathbf{P}$
- diagonal matrices $\mathbf{D}$ with non-zero diagonal

Fact:

Every monomial is of the form $\mathbf{Q} = \mathbf{P} \cdot \mathbf{D}$.

$$\mathbf{P} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad \mathbf{D} = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} \qquad \mathbf{Q} = \begin{bmatrix} 0 & 0 & 3 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

Code Equivalence

Linear [n,k] code: subspace $C \subseteq \mathbb{F}_q^n$ of dimension k.

☞ $C = \{\mathbf{x} \cdot \mathbf{G} \mid \mathbf{x} \in \mathbb{F}_q^k\}, \mathbf{G} \in \mathbb{F}_q^{k \times n}$.

Monomial: linear map $\mathbf{Q} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ that preserves Hamming weight.

$= \mathrm{wt}(\mathbf{v})$ for every $\mathbf{v} \in \mathbb{F}_q^n$.

Codes C_1, C_2 are linearly equivalent.

$$\Longleftrightarrow$$

$C_2 = C_1 \cdot \mathbf{Q}$, for some monomial $\mathbf{Q}$.

Examples:

- permutations $\mathbf{P}$
- diagonal matrices $\mathbf{D}$ with non-zero diagonal

is of the form $\mathbf{Q} = \mathbf{P} \cdot \mathbf{D}$.

$$\mathbf{P} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \mathbf{D} = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} \quad \mathbf{Q} = \begin{bmatrix} 0 & 0 & 3 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

Code Equivalence Problem

Given: generator matrices $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$ of equivalent codes C_1, C_2 .

Find: monomial $\mathbf{Q}$ with $C_2 = C_1 \cdot \mathbf{Q}$.

Code Equivalence Problem

Given: generator matrices $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$ of equivalent codes C_1, C_2 .

Find: monomial $\mathbf{Q}$ with $C_2 = C_1 \cdot \mathbf{Q}$.

⚠ not $\mathbf{G}_2 = \mathbf{G}_1 \cdot \mathbf{Q}$

Code Equivalence Problem

Given: generator matrices $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$ of equivalent codes C_1, C_2 .

Find: monomial $\mathbf{Q}$ with $C_2 = C_1 \cdot \mathbf{Q}$.

⚠ not $\mathbf{G}_2 = \mathbf{G}_1 \cdot \mathbf{Q}$, but $\mathbf{G}_2 = \mathbf{U} \cdot \mathbf{G}_1 \cdot \mathbf{Q}$, for some $\mathbf{U} \in \mathrm{GL}(\mathbb{F}_q^k)$.

Code Equivalence Problem

Given: generator matrices $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{F}_q^{k\times n}$ of equivalent codes C_1, C_2 .

Find: monomial $\mathbf{Q}$ with $C_2 = C_1 \cdot \mathbf{Q}$.

⚠ not $\mathbf{G}_2 = \mathbf{G}_1 \cdot \mathbf{Q}$, but $\mathbf{G}_2 = \mathbf{U} \cdot \mathbf{G}_1 \cdot \mathbf{Q}$, for some $\mathbf{U} \in \mathrm{GL}(\mathbb{F}_q^k)$.

LESS parameters:

- $n \in \{252,400,548\},\ k = n/2,\ q = 127$

Code Equivalence Problem

Given: generator matrices $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{F}_q^{k\times n}$ of equivalent codes C_1, C_2 .

Find: monomial $\mathbf{Q}$ with $C_2 = C_1 \cdot \mathbf{Q}$.

⚠ not $\mathbf{G}_2 = \mathbf{G}_1 \cdot \mathbf{Q}$, but $\mathbf{G}_2 = \mathbf{U} \cdot \mathbf{G}_1 \cdot \mathbf{Q}$, for some $\mathbf{U} \in \mathrm{GL}(\mathbb{F}_q^k)$.

LESS parameters:

- $n \in \{252{,}400{,}548\},\ k = n/2,\ q = 127$

Asymptotic analysis:

- k/n and q fixed, $n \to \infty$

Code Equivalence Problem

Given: generator matrices $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$ of equivalent codes C_1, C_2 .

Find: monomial $\mathbf{Q}$ with $C_2 = C_1 \cdot \mathbf{Q}$.

⚠ not $\mathbf{G}_2 = \mathbf{G}_1 \cdot \mathbf{Q}$, but $\mathbf{G}_2 = \mathbf{U} \cdot \mathbf{G}_1 \cdot \mathbf{Q}$, for some $\mathbf{U} \in \mathrm{GL}(\mathbb{F}_q^k)$.

LESS parameters:

- $n \in \{252,400,548\},\ k = n/2,\ q = 127$

Asymptotic analysis:

- k/n and q fixed, $n \to \infty$

☞ This talk: $k/n = 1/2$.

Code Equivalence Problem

Given: generator matrices $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$ of equivalent codes C_1, C_2.

Find: monomial $\mathbf{Q}$ with $C_2 = C_1 \cdot \mathbf{Q}$.

⚠ not $\mathbf{G}_2 = \mathbf{G}_1 \cdot \mathbf{Q}$, but $\mathbf{G}_2 = \mathbf{U} \cdot \mathbf{G}_1 \cdot \mathbf{Q}$, for some $\mathbf{U} \in \mathrm{GL}(\mathbb{F}_q^k)$.

LESS parameters:

- $n \in \{252, 400, 548\}, \ k = n/2, \ q = 127$

Asymptotic analysis:

- k/n and q fixed, $n \to \infty$

☞ This talk: $k/n = 1/2$.

Main result:
New algorithm for code equivalence with runtime

$$2^{n/2}$$

that works for all $q \geq 7$.

Code Equivalence Problem

Given: generator matrices $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{F}_q^{k\times n}$ of equivalent codes C_1, C_2.

Find: monomial $\mathbf{Q}$ with $C_2 = C_1 \cdot \mathbf{Q}$.

⚠ not $\mathbf{G}_2 = \mathbf{G}_1 \cdot \mathbf{Q}$, but $\mathbf{G}_2 = \mathbf{U} \cdot \mathbf{G}_1 \cdot \mathbf{Q}$, for some $\mathbf{U} \in \mathrm{GL}(\mathbb{F}_q^k)$.

LESS parameters:

- $n \in \{252, 400, 548\},\ k = n/2,\ q = 127$

Asymptotic analysis:

- k/n and q fixed, $n \to \infty$

☞ This talk: $k/n = 1/2$.

Main result:
New algorithm for code equivalence with runtime

$$2^{n/2}$$

that works for all $q \geq 7$.

Quantum algorithm with runtime $2^{n/3}$.

Comparison with State of the Art

Short codeword based:

- Leon, 1982
- Beullens, 2020
- Barenghi, Biasse, Persichetti, Santini, 2023

Canonical form based:

- Chou, Persichetti, Santini, 2025

Comparison with State of the Art

Short codeword based:

- Leon, 1982
- Beullens, 2020
- Barenghi, Biasse, Persichetti, Santini, 2023

Canonical form based:

- Chou, Persichetti, Santini, 2025

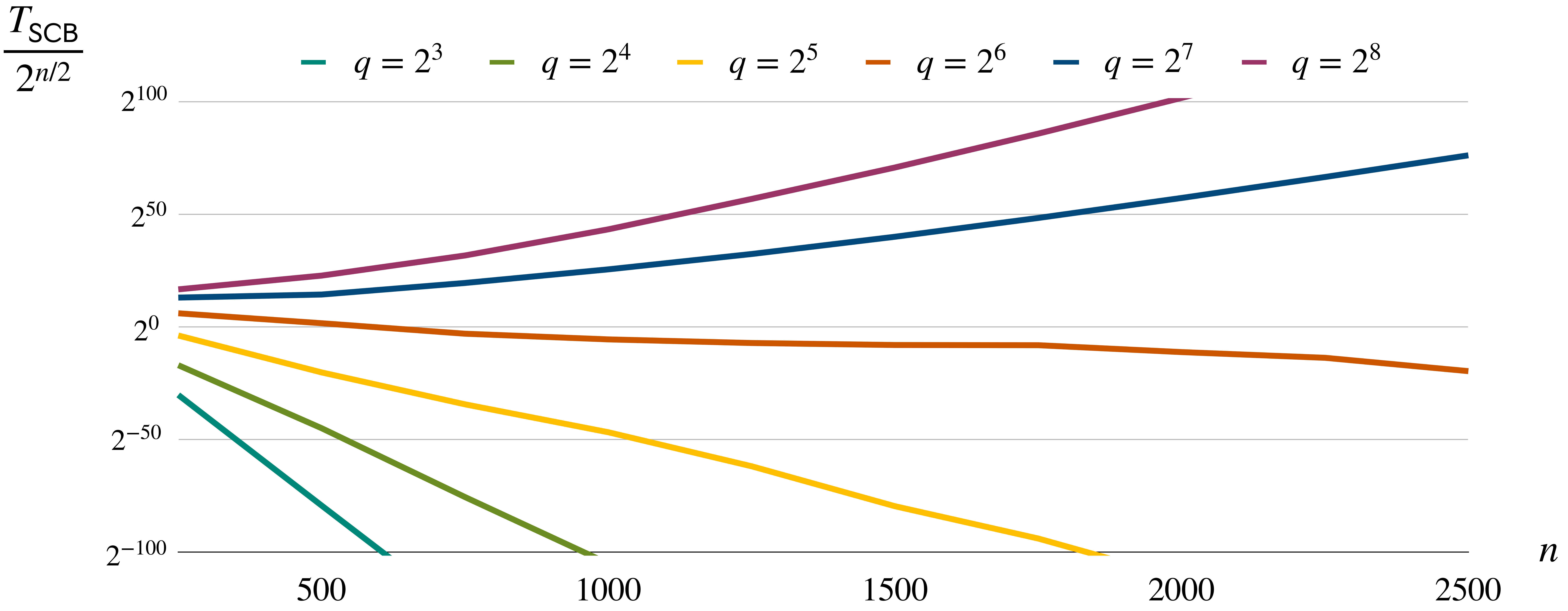
Comparison with State of the Art

Short codeword based:

- Leon, 1982
- Beullens, 2020
- Barenghi, Biasse, Persichetti, Santini, 2023

Canonical form based:

- Chou, Persichetti, Santini, 2025



Comparison with State of the Art

Short codeword based:

- Leon, 1982
- Beullens, 2020
- Barenghi, Biasse, Persichetti, Santini, 2023

Canonical form based:

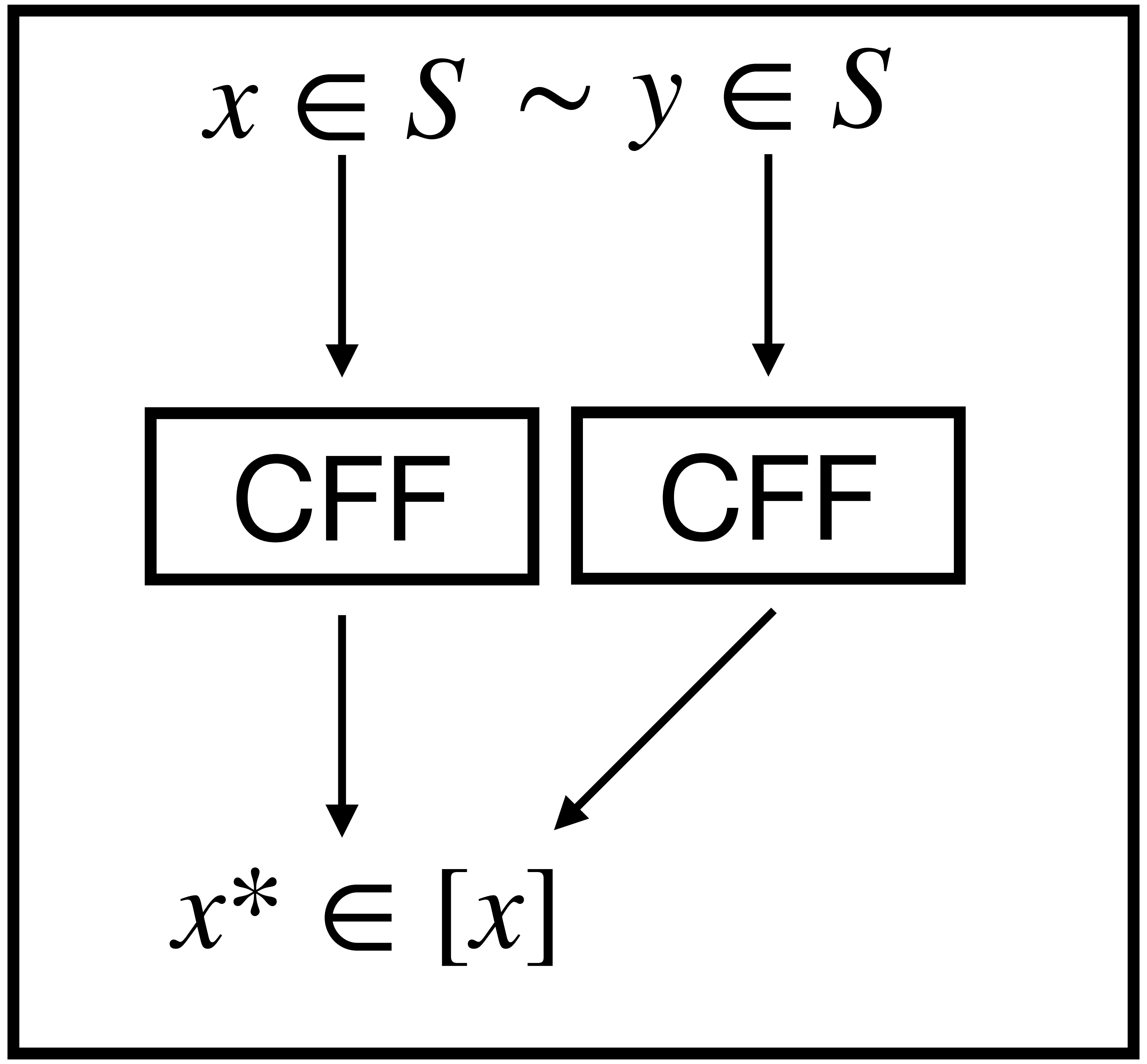
- Chou, Persichetti, Santini, 2025

Canonical Form Functions

- S: set
- $\sim$: equivalence relation on S
- $[x] := \{y \mid x \sim y\}$

Canonical Form Functions

- S: set
- $\sim$: equivalence relation on S
- $[x] := \{y \mid x \sim y\}$

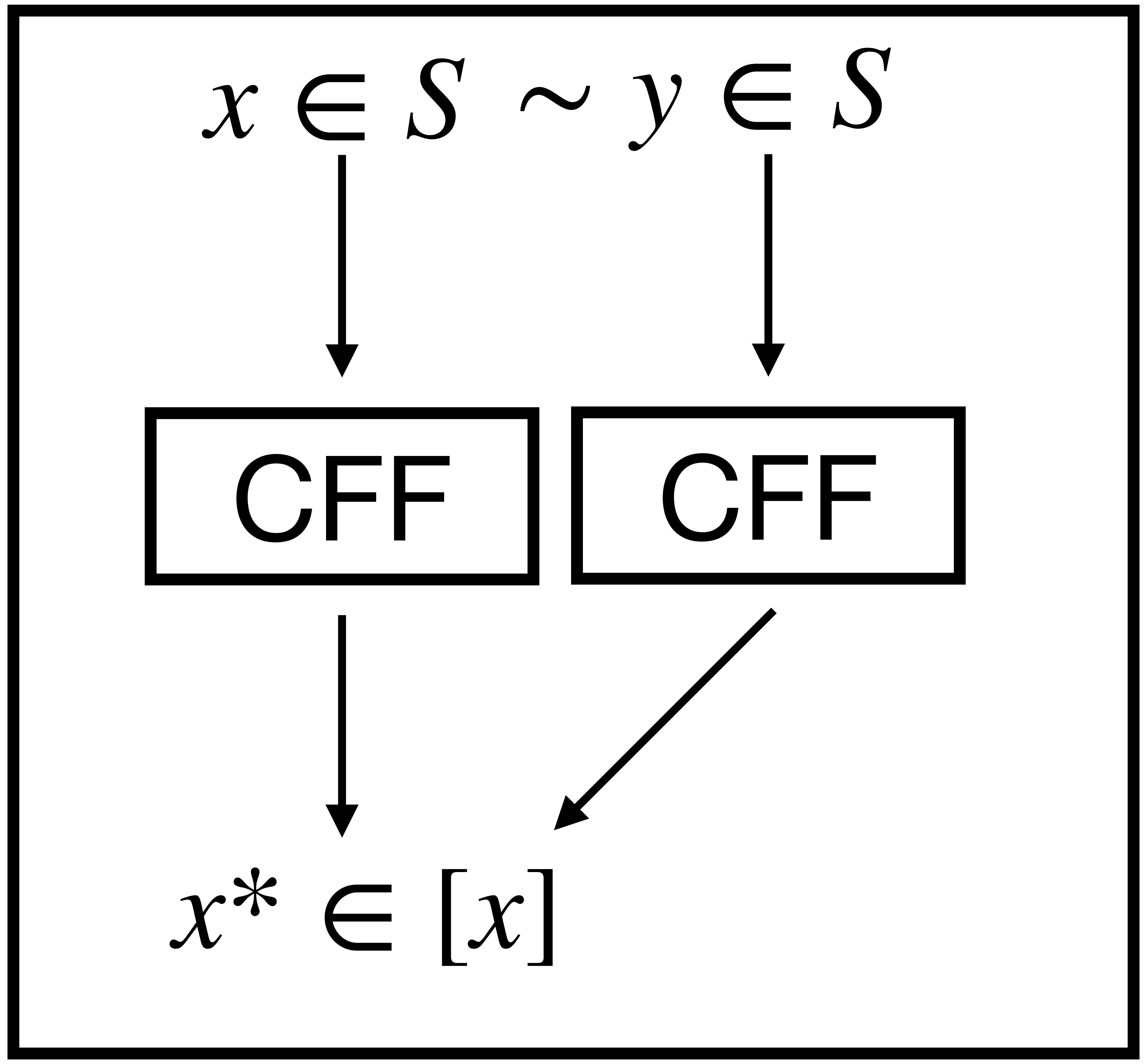


Canonical Form Functions

- S: set
- $\sim$: equivalence relation on S
- $[x] := \{y \mid x \sim y\}$

Example:

- $S = \mathbb{Z}$
- $x \sim y \iff x \equiv y \mod 3$
- CFF : $\mathbb{Z} \to \{0,1,2\}, \quad x \mapsto x \bmod 3$



Canonical Form Functions

- S: set
- $\sim$: equivalence relation on S
- $[x] := \{y \mid x \sim y\}$

Example:

- $S = \mathbb{Z}$
- $x \sim y \iff x \equiv y \mod 3$
- CFF : $\mathbb{Z} \to \{0,1,2\}, \quad x \mapsto x \bmod 3$

$$
\begin{tikzcd}
x \in S \arrow[d] & \sim & y \in S \arrow[d] \\
\boxed{\text{CFF}} \arrow[d] & & \boxed{\text{CFF}} \arrow[dll] \\
x^* \in [x] & &
\end{tikzcd}
$$

Chou, Persichetti, Santini (CPS), DCC 2025:

- $S := \mathbb{F}_q^{k\times(n-k)}$
- $\mathbf{A}_1 \sim \mathbf{A}_2 \iff \mathbf{A}_2 = \mathbf{Q}_r \cdot \mathbf{A}_1 \cdot \mathbf{Q}_c$

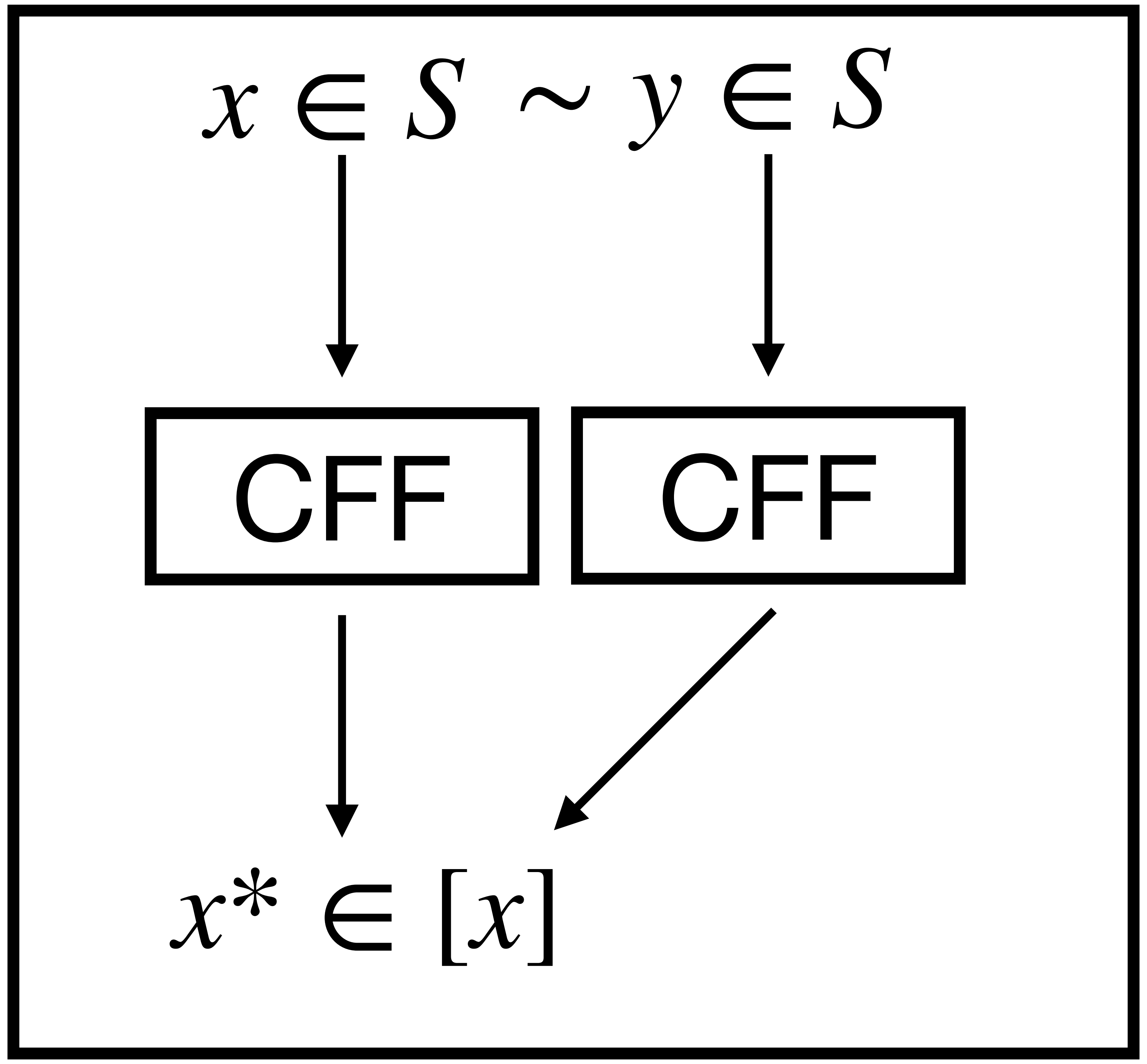
monomials

LRL equivalence

Canonical Form Functions

- S: set
- $\sim$: equivalence relation on S
- $[x] := \{y \mid x \sim y\}$

Example:
- $S = \mathbb{Z}$
- $x \sim y \iff x \equiv y \mod 3$
- CFF : $\mathbb{Z} \to \{0,1,2\}, \quad x \mapsto x \bmod 3$



Chou, Persichetti, Santini (CPS), DCC 2025:
- $S := \mathbb{F}_q^{k\times(n-k)}$
- $\mathbf{A}_1 \sim \mathbf{A}_2 \iff \mathbf{A}_2 = \mathbf{Q}_r \cdot \mathbf{A}_1 \cdot \mathbf{Q}_c$

monomials

LRL equivalence

- CFF should succeed with probability $\gamma = \Theta(1)$.

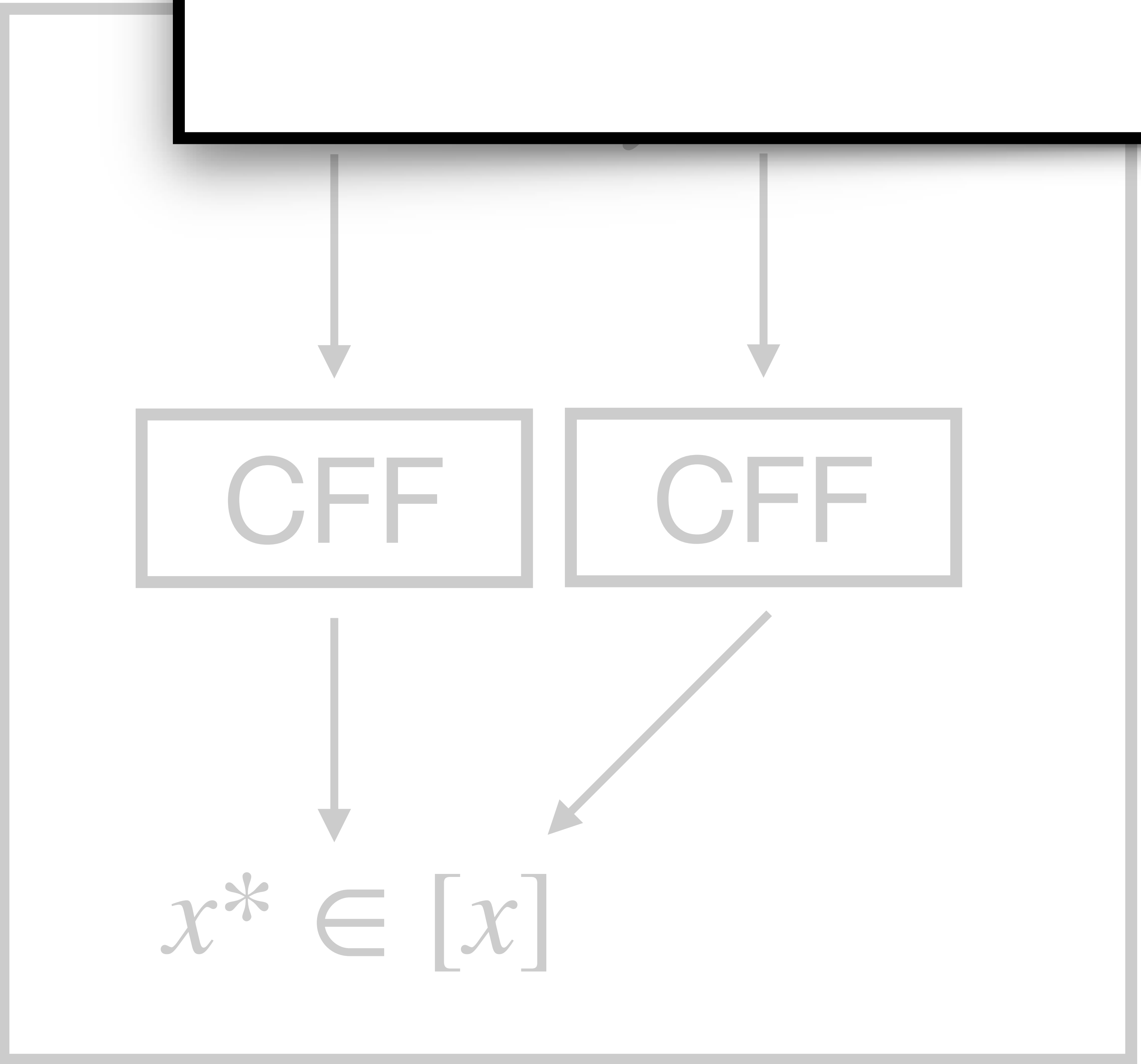
Canonical Form Functions

- S: set
- $\sim$:
- $[x]$

CPS 2025:

Suppose there exists an efficient CFF for LRL equivalence with success probability γ. Then we can solve the code equivalence problem in time

$$\gamma^{-1/2} \cdot 2^{n/2}.$$



Example

Chou, Persichetti, Santini (CPS), DCC 2025:

- $S := \mathbb{F}_q^{k\times(n-k)}$
- $\mathbf{A}_1 \sim \mathbf{A}_2 \iff \mathbf{A}_2 = \mathbf{Q}_r \cdot \mathbf{A}_1 \cdot \mathbf{Q}_c$

LRL equivalence

monomials

- CFF should succeed with probability $\gamma = \Theta(1)$.

Canonical Form Functions

CPS 2025:

Suppose there exists an efficient CFF for LRL equivalence with success probability γ.

Then we can solve the code equivalence problem in time

$$\gamma^{-1/2} \cdot 2^{n/2}.$$

Chou, Persichetti, Santini (CPS), DCC 2025:

CPS: CFF with $\gamma = \widetilde{\Theta}\left((1 - q^{-1})^{n-k}\right)$.

$\Rightarrow \mathbf{A}_2 = \mathbf{Q}_r \cdot \mathbf{A}_1 \cdot \mathbf{Q}_c$

monomials

succeed with probability $\gamma = \Theta(1)$.

Canonical Form Functions

CPS 2025:

Suppose there exists an efficient CFF for LRL equivalence with success probability γ.

Then we can solve the code equivalence problem in time

$$\gamma^{-1/2} \cdot 2^{n/2}.$$

Chou, Persichetti, Santini (CPS), DCC 2025:

CPS: CFF with $\gamma = \widetilde{\Theta}\left((1 - q^{-1})^{n-k}\right)$.

- $q = \Omega(n - k) \implies \gamma = \widetilde{\Theta}(1)$.

$\Rightarrow \mathbf{A}_2 = \mathbf{Q}_r \cdot \mathbf{A}_1 \cdot \mathbf{Q}_c$

monomials

succeed with probability $\gamma = \Theta(1)$.

Canonical Form Functions

CPS 2025:

Suppose there exists an efficient CFF for LRL equivalence with success probability γ.
Then we can solve the code equivalence problem in time

$$\gamma^{-1/2} \cdot 2^{n/2}.$$

Chou, Persichetti, Santini (CPS), DCC 2025:

CPS: CFF with $\gamma = \widetilde{\Theta}\left((1 - q^{-1})^{n-k}\right)$.

- $q = \Omega(n-k) \implies \gamma = \widetilde{\Theta}(1)$.

☞ LESS: $q = 127, n - k = 126$

$\Rightarrow \mathbf{A}_2 = \mathbf{Q}_r \cdot \mathbf{A}_1 \cdot \mathbf{Q}_c$

monomials

succeed with probability $\gamma = \Theta(1)$.

Canonical Form Functions

CPS 2025:

Suppose there exists an efficient CFF for LRL equivalence with success probability γ.
Then we can solve the code equivalence problem in time

$$\gamma^{-1/2} \cdot 2^{n/2}.$$

Chou, Persichetti, Santini (CPS), DCC 2025:

$\Rightarrow \mathbf{A}_2 = \mathbf{Q}_r \cdot \mathbf{A}_1 \cdot \mathbf{Q}_c$

monomials

CPS: CFF with $\gamma = \widetilde{\Theta}\left((1 - q^{-1})^{n-k}\right)$.

- $q = \Omega(n - k) \implies \gamma = \widetilde{\Theta}(1)$.

  ☞ LESS: $q = 127, n - k = 126$

- $q = O(1) \implies \gamma = 2^{-\Theta(n)}$.

succeed with probability $\gamma = \Theta(1)$.

Canonical Form Functions

CPS 2025:

Suppose there exists an efficient CFF for LRL equivalence with success probability γ.
Then we can solve the code equivalence problem in time

$$\gamma^{-1/2} \cdot 2^{n/2}.$$

Chou, Persichetti, Santini (CPS), DCC 2025:

CPS: CFF with $\gamma = \widetilde{\Theta}\left((1-q^{-1})^{n-k}\right)$.

- $q = \Omega(n-k) \implies \gamma = \widetilde{\Theta}(1)$.

  ☞ LESS: $q = 127, n-k = 126$

- $q = O(1) \implies \gamma = 2^{-\Theta(n)}$.

New result:
CFF with

$$\gamma = 1 - O(n^{-1})$$

for all $q \geq 7$.

succeed with probability $\gamma = \Theta(1)$.

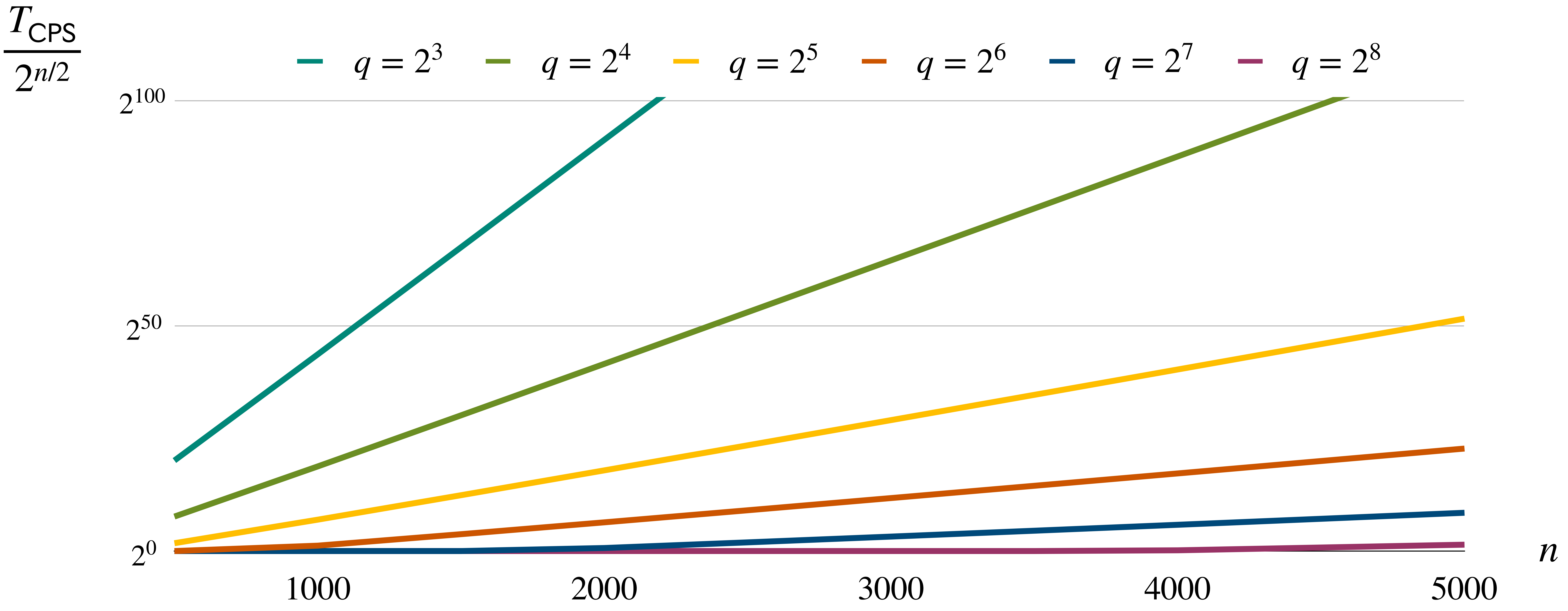
Comparison with CPS

Runtime using new CFF:

$$2^{n/2}$$

Runtime using CPS' CFF:

$$2^{n/2} \cdot 2^{\Theta(n)}$$



Why $q \geq 7$?

Theorem:
New CFF has success probability $\gamma = 1 - O(n^{-1})$ for all $q \geq 7$.

Why $q \geq 7$?

Theorem:
New CFF has success probability $\gamma = 1 - O(n^{-1})$ for all $q \geq 7$.

Proof sketch:

- $\mathbf{A} \leftarrow \mathbb{F}_q^{k \times (n-k)}$
- $P := \Pr[\text{two rows of } \mathbf{A} \text{ are identical up to permutation}]$

Why $q \geq 7$?

Theorem:
New CFF has success probability $\gamma = 1 - O(n^{-1})$ for all $q \geq 7$.

Proof sketch:

- $\mathbf{A} \leftarrow \mathbb{F}_q^{k\times(n-k)}$
- $P := \Pr[\text{two rows of } \mathbf{A} \text{ are identical up to permutation}]$
- For the new CFF, we have $\gamma \approx 1 - P$.

Why $q \geq 7$?

Theorem:
New CFF has success probability $\gamma = 1 - O(n^{-1})$ for all $q \geq 7$.

Proof sketch:

- $\mathbf{A} \leftarrow \mathbb{F}_q^{k \times (n-k)}$
- $P := \Pr[\text{two rows of } \mathbf{A} \text{ are identical up to permutation}]$
- For the new CFF, we have $\gamma \approx 1 - P$.

- Richmond, Shallit 2009: (Electronic Journal of Combinatorics)
  $\mathbf{v}, \mathbf{w} \leftarrow \mathbb{F}_q^{n-k}$ are identical up to permutation with probability $\approx (n-k)^{(1-q)/2}$.

Why $q \geq 7$?

Theorem:
New CFF has success probability $\gamma = 1 - O(n^{-1})$ for all $q \geq 7$.

Proof sketch:

- $\mathbf{A} \leftarrow \mathbb{F}_q^{k\times(n-k)}$
- $P := \Pr[\text{two rows of } \mathbf{A} \text{ are identical up to permutation}]$
- For the new CFF, we have $\gamma \approx 1 - P$.
- Richmond, Shallit 2009: (Electronic Journal of Combinatorics)
  $\mathbf{v}, \mathbf{w} \leftarrow \mathbb{F}_q^{n-k}$ are identical up to permutation with probability $\approx (n-k)^{(1-q)/2}$.
- $\implies P \leq k^2 \cdot (n-k)^{(q-1)/2}$

Union Bound

Why $q \geq 7$?

Theorem:
New CFF has success probability $\gamma = 1 - O(n^{-1})$ for all $q \geq 7$.

Proof sketch:

- $\mathbf{A} \leftarrow \mathbb{F}_q^{k \times (n-k)}$
- $P := \Pr[\text{two rows of } \mathbf{A} \text{ are identical up to permutation}]$
- For the new CFF, we have $\gamma \approx 1 - P$.
- Richmond, Shallit 2009: (Electronic Journal of Combinatorics)
  $\mathbf{v}, \mathbf{w} \leftarrow \mathbb{F}_q^{n-k}$ are identical up to permutation with probability $\approx (n-k)^{(1-q)/2}$.
- $\implies P \underset{\text{Union Bound}}{\leq} k^2 \cdot (n-k)^{(q-1)/2} \underset{k = n/2}{=} \Theta(n^{2+(1-q)/2}) = \Theta(n^{(5-q)/2})$

Why $q \geq 7$?

Theorem:
New CFF has success probability $\gamma = 1 - O(n^{-1})$ for all $q \geq 7$.

Proof sketch:

- $\mathbf{A} \leftarrow \mathbb{F}_q^{k \times (n-k)}$
- $P := \Pr[\text{two rows of } \mathbf{A} \text{ are identical up to permutation}]$
- For the new CFF, we have $\gamma \approx 1 - P$.
- Richmond, Shallit 2009: (Electronic Journal of Combinatorics)
  $\mathbf{v}, \mathbf{w} \leftarrow \mathbb{F}_q^{n-k}$ are identical up to permutation with probability $\approx (n-k)^{(1-q)/2}$.
- $$\implies P \underset{\text{Union Bound}}{\leq} k^2 \cdot (n-k)^{(q-1)/2} \underset{k = n/2}{=} \Theta(n^{2+(1-q)/2}) = \Theta(n^{(5-q)/2}) = \begin{cases} \Omega(1), & \text{for } q \leq 5 \\ O(n^{-1}), & \text{for } q \geq 7 \end{cases}$$

Success Probability in Practice

q \ n	50	60	70	80	90	100
2	0 %	0 %	0 %	0 %	0 %	0 %
3	0 %	0 %	0 %	0 %	0 %	0 %
4	52 %	32 %	30 %	20 %	10 %	0 %
≥ 5	100 %	100 %	100 %	100 %	100 %	100 %

Summary

- **New algorithm for code equivalence with runtime** $2^{n/2}$
  - Exponential improvement over short-codeword based for all $q \geq 2^7$
  - Exponential improvement over CPS for $q = O(1)$
  - LESS parameters not affected

https://ia.cr/2024/1272

Summary

- **New algorithm for code equivalence with runtime $2^{n/2}$**
  - Exponential improvement over short-codeword based for all $q \geq 2^7$
  - Exponential improvement over CPS for $q = O(1)$
  - LESS parameters not affected
- **Core ingredient is improved canonical form function (CFF)**
  - Previous CFF required $q = \Omega(n)$
  - Improved CFF requires $q \geq 7$

https://ia.cr/2024/1272

Summary

- **New algorithm for code equivalence with runtime $2^{n/2}$**
  - Exponential improvement over short-codeword based for all $q \geq 2^7$
  - Exponential improvement over CPS for $q = O(1)$
  - LESS parameters not affected
- **Core ingredient is improved canonical form function (CFF)**
  - Previous CFF required $q = \Omega(n)$
  - Improved CFF requires $q \geq 7$

- **Potential application**
  - Using improved CFF to construct more efficient code-based cryptosystems with smaller q

https://ia.cr/2024/1272