How To (Not) Decode In the Rank Metric

Hugo Sauerbier Couvée

Technical University of Munich (TUM)

Joint work with

Alberto Ravagnani (TU/e), Antonia Wachter-Zeh (TUM), Violetta Weger (TUM)

15 February 2024

Contents

- Generic decoding: **Rank Syndrome Decoding Problem (RSDP)**

Contents

- Generic decoding: **Rank Syndrome Decoding Problem (RSDP)**
- Focus on **combinatorial/geometric** attacks, might also help hybrid attacks

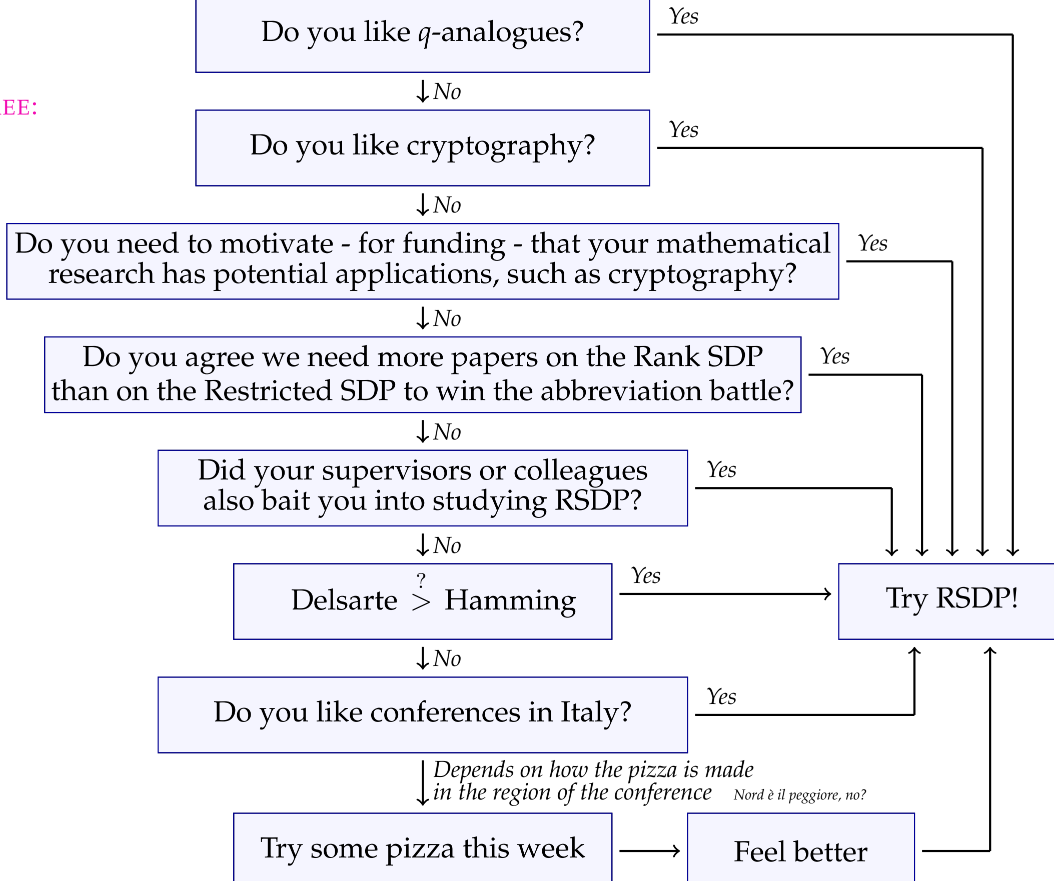
Contents

- Generic decoding: **Rank Syndrome Decoding Problem (RSDP)**
- Focus on **combinatorial/geometric** attacks, might also help hybrid attacks
- Two potential approaches leading to *open problems on rank-metric codes*™

Should you study/care about Rank Syndrome Decoding Problem (RSDP)?

Decision tree:

Decision tree:



Part

Problem introduction

Definition (SDP)

Given a parity-check matrix $\mathbf{H}$ *of a code* $\mathcal{C}$, *syndrome vector* $\mathbf{s}$, *target weight* t, *find an error vector* $\mathbf{e}$ *such that*

$$\mathbf{H}\mathbf{e}^T = \mathbf{s}^T \qquad \textit{and} \qquad wt(\mathbf{e}) \leq t.$$

Definition (SDP)

Given a parity-check matrix $\mathbf{H}$ *of a code* $\mathcal{C}$*, syndrome vector* $\mathbf{s}$*, target weight* t*, find an error vector* $\mathbf{e}$ *such that*

$$\mathbf{H}\mathbf{e}^T = \mathbf{s}^T \qquad \textit{and} \qquad wt(\mathbf{e}) \leq t.$$

- $\mathbb{F}_q$-lin. vector code, Hamming weight wt_H, error $\mathbf{e} \in \mathbb{F}_q^n$: HSDP

Definition (SDP)

Given a parity-check matrix $\mathbf{H}$ of a code $\mathcal{C}$, syndrome vector $\mathbf{s}$, target weight t, find an error vector $\mathbf{e}$ such that

$$\mathbf{H}\mathbf{e}^T = \mathbf{s}^T \qquad \text{and} \qquad wt(\mathbf{e}) \leq t.$$

- $\mathbb{F}_q$-lin. vector code, Hamming weight wt_H, error $\mathbf{e} \in \mathbb{F}_q^n$: HSDP
- $\mathbb{F}_q$-lin. matrix code, rank weight wt_R, error $\mathbf{e} \in \mathbb{F}_q^{m \times n}$: $\mathbb{F}_q$-linear RSDP

Definition (SDP)

Given a parity-check matrix $\mathbf{H}$ *of a code* $\mathcal{C}$, *syndrome vector* $\mathbf{s}$, *target weight* t, *find an error vector* $\mathbf{e}$ *such that*

$$\mathbf{H}\mathbf{e}^T = \mathbf{s}^T \qquad \textit{and} \qquad wt(\mathbf{e}) \leq t.$$

- $\mathbb{F}_q$-lin. vector code, Hamming weight wt_H, error $\mathbf{e} \in \mathbb{F}_q^n$: HSDP
- $\mathbb{F}_q$-lin. matrix code, rank weight wt_R, error $\mathbf{e} \in \mathbb{F}_q^{m \times n}$: $\mathbb{F}_q$-linear RSDP
- $\boxed{\mathbb{F}_{q^m}\text{-lin. vector code, rank weight } wt_R\text{, error } \mathbf{e} \in \mathbb{F}_{q^m}^n\text{: } \mathbb{F}_{q^m}\text{-linear RSDP}}$

Definition (SDP)

Given a parity-check matrix $\mathbf{H}$ *of a code* $\mathcal{C}$*, syndrome vector* $\mathbf{s}$*, target weight* t*, find an error vector* $\mathbf{e}$ *such that*

$$\mathbf{H}\mathbf{e}^T = \mathbf{s}^T \qquad \textit{and} \qquad wt(\mathbf{e}) \leq t.$$

- $\mathbb{F}_q$-lin. vector code, Hamming weight wt_H, error $\mathbf{e} \in \mathbb{F}_q^n$: HSDP
- $\mathbb{F}_q$-lin. matrix code, rank weight wt_R, error $\mathbf{e} \in \mathbb{F}_q^{m \times n}$: $\mathbb{F}_q$-linear RSDP
- $\boxed{\mathbb{F}_{q^m}\text{-lin. vector code, rank weight } wt_R\text{, error } \mathbf{e} \in \mathbb{F}_{q^m}^n\text{: } \mathbb{F}_{q^m}\text{-linear RSDP}}$

Slight abuse of notation: $\mathbf{e}$ for vector/matrix in $\mathbb{F}_{q^m}^n \cong \mathbb{F}_q^{m \times n} \cong \mathbb{F}_q^{mn}$

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn, \; k \sim Rn, \; t \sim Tn \quad$ for real $M, R, T > 0$

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn,\ k \sim Rn,\ t \sim Tn$ for real $M, R, T > 0$
- Often interested in GV-bound: $T = \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}}$ (merci Pierre!)

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn, \; k \sim Rn, \; t \sim Tn$ for real $M, R, T > 0$
- Often interested in GV-bound: $T = \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}}$ (merci Pierre!)

- **'Combinatorial´** attacks:

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn, \; k \sim Rn, \; t \sim Tn \quad$ for real $M, R, T > 0$
- Often interested in GV-bound: $T = \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}}$ (merci Pierre!)

- **'Combinatorial'** attacks:
  - Enumerate over a lot (coordinates, bases, spaces, etc.)

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn, \; k \sim Rn, \; t \sim Tn \quad$ for real $M, R, T > 0$
- Often interested in GV-bound: $T = \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}}$ (merci Pierre!)

- **'Combinatorial'** attacks:
  - Enumerate over a lot (coordinates, bases, spaces, etc.)
  - For every enumeration solve a system of linear equations.

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn, \; k \sim Rn, \; t \sim Tn$ for real $M, R, T > 0$
- Often interested in GV-bound: $T = \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}}$ (merci Pierre!)

- **'Combinatorial'** attacks:
  - Enumerate over a lot (coordinates, bases, spaces, etc.)
  - For every enumeration solve a system of linear equations.
  - Success if solution has weight $\leq t$.

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn,\ k \sim Rn,\ t \sim Tn \quad$ for real $M, R, T > 0$
- Often interested in GV-bound: $T = \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}}$ (merci Pierre!)
- **'Combinatorial'** attacks:
  - Enumerate over a lot (coordinates, bases, spaces, etc.)
  - For every enumeration solve a system of linear equations.
  - Success if solution has weight $\leq t$.
- Complexity (up to polyn. and rounding) of best combinatorial attacks:

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn,\ k \sim Rn,\ t \sim Tn \quad$ for real $M, R, T > 0$
- Often interested in GV-bound: $T = \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}}$ (merci Pierre!)
- **'Combinatorial'** attacks:
  - Enumerate over a lot (coordinates, bases, spaces, etc.)
  - For every enumeration solve a system of linear equations.
  - Success if solution has weight $\leq t$.
- Complexity (up to polyn. and rounding) of best combinatorial attacks:
  - Chabaud-Stern (1996): $q^{(m-t)(t-1)}$

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn,\ k \sim Rn,\ t \sim Tn$ for real $M, R, T > 0$
- Often interested in GV-bound: $T = \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}}$ (merci Pierre!)
- **'Combinatorial'** attacks:
  - Enumerate over a lot (coordinates, bases, spaces, etc.)
  - For every enumeration solve a system of linear equations.
  - Success if solution has weight $\leq t$.
- Complexity (up to polyn. and rounding) of best combinatorial attacks:
  - Chabaud-Stern (1996): $q^{(m-t)(t-1)}$
  - Ourivski-Johansson (2002): $q^{(k+1)(t-1)}$

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn,\ k \sim Rn,\ t \sim Tn$ for real $M, R, T > 0$
- Often interested in GV-bound: $T = \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}}$ (merci Pierre!)
- **'Combinatorial'** attacks:
  - Enumerate over a lot (coordinates, bases, spaces, etc.)
  - For every enumeration solve a system of linear equations.
  - Success if solution has weight $\leq t$.
- Complexity (up to polyn. and rounding) of best combinatorial attacks:
  - Chabaud-Stern (1996): $q^{(m-t)(t-1)}$
  - Ourivski-Johansson (2002): $q^{(k+1)(t-1)}$
  - Gaborit-Ruatta-Schrek (2016): $q^{kt},\ q^{Mkt}, q^{M(k+1)(t-1)},\ q^{(k+1)(t+1)-(n+1)}$

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn,\ k \sim Rn,\ t \sim Tn$ for real $M, R, T > 0$
- Often interested in GV-bound: $T = \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}}$ (merci Pierre!)
- **'Combinatorial'** attacks:
  - Enumerate over a lot (coordinates, bases, spaces, etc.)
  - For every enumeration solve a system of linear equations.
  - Success if solution has weight $\leq t$.
- Complexity (up to polyn. and rounding) of best combinatorial attacks:
  - Chabaud-Stern (1996): $q^{(m-t)(t-1)}$
  - Ourivski-Johansson (2002): $q^{(k+1)(t-1)}$
  - Gaborit-Ruatta-Schrek (2016): $q^{kt},\ q^{Mkt}, q^{M(k+1)(t-1)},\ q^{(k+1)(t+1)-(n+1)}$
  - Aragon-Gaborit-Hauteville-Tillich (2018): $q^{M(k+1)t-m}$

Problem introduction

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn,\ k \sim Rn,\ t \sim Tn$ for real $M, R, T > 0$
- Often interested in GV-bound: $T = \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}}$ (merci Pierre!)

- **'Combinatorial'** attacks:
  - Enumerate over a lot (coordinates, bases, spaces, etc.)
  - For every enumeration solve a system of linear equations.
  - Success if solution has weight $\leq t$.

- Complexity (up to polyn. and rounding) of best combinatorial attacks:
  - Chabaud-Stern (1996): $q^{(m-t)(t-1)}$
  - Ourivski-Johansson (2002): $q^{(k+1)(t-1)}$
  - Gaborit-Ruatta-Schrek (2016): q^{kt}, q^{Mkt}, $q^{M(k+1)(t-1)}$, $q^{(k+1)(t+1)-(n+1)}$
  - Aragon-Gaborit-Hauteville-Tillich (2018): $q^{M(k+1)t-m}$

- Almost all: $\boxed{q^{\min\{M,1\}RTn^2 + O(n)}}$

PROBLEM INTRODUCTION

- $\mathbb{F}_{q^m}$-lin. vector code $\mathcal{C}$ of length n and $\mathbb{F}_{q^m}$-dim k
- Regime: $m \sim Mn, \; k \sim Rn, \; t \sim Tn$ for real $M, R, T > 0$
- Often interested in GV-bound: $T = \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}}$ (merci Pierre!)
- **'Combinatorial'** attacks:
  - Enumerate over a lot (coordinates, bases, spaces, etc.)
  - For every enumeration solve a system of linear equations.
  - Success if solution has weight $\leq t$.
- Complexity (up to polyn. and rounding) of best combinatorial attacks:
  - Chabaud-Stern (1996): $q^{(m-t)(t-1)}$
  - Ourivski-Johansson (2002): $q^{(k+1)(t-1)}$
  - Gaborit-Ruatta-Schrek (2016): q^{kt}, q^{Mkt}, $q^{M(k+1)(t-1)}$, $q^{(k+1)(t+1)-(n+1)}$
  - Aragon-Gaborit-Hauteville-Tillich (2018): $q^{M(k+1)t-m}$

- Almost all:
$\boxed{q^{\min\{M,1\}RTn^2 + O(n)}}$

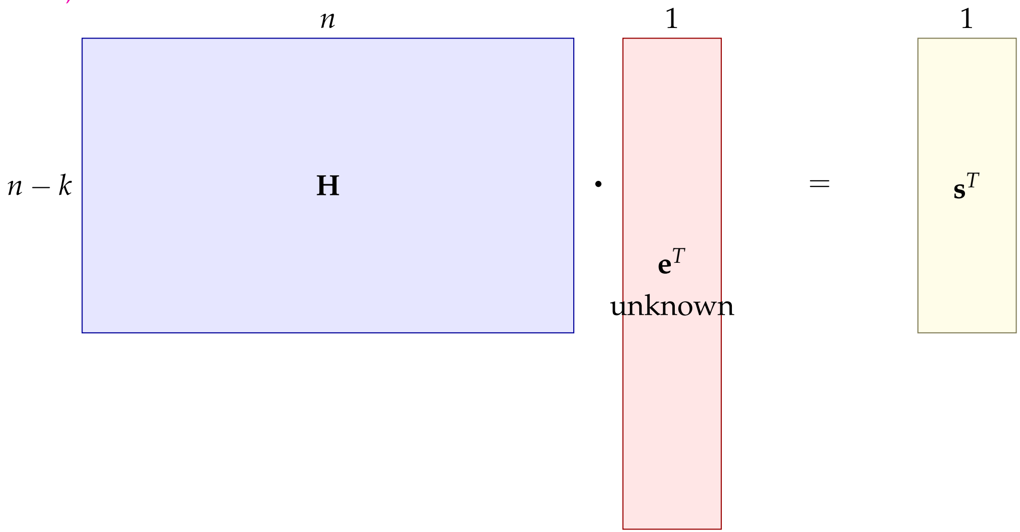
- $\boxed{\lim_{n\to\infty} \frac{1}{n^2} \log_q(complexity)}$ $\boxed{= \min\{M,1\}RT}$

Can we improve asymptotically?

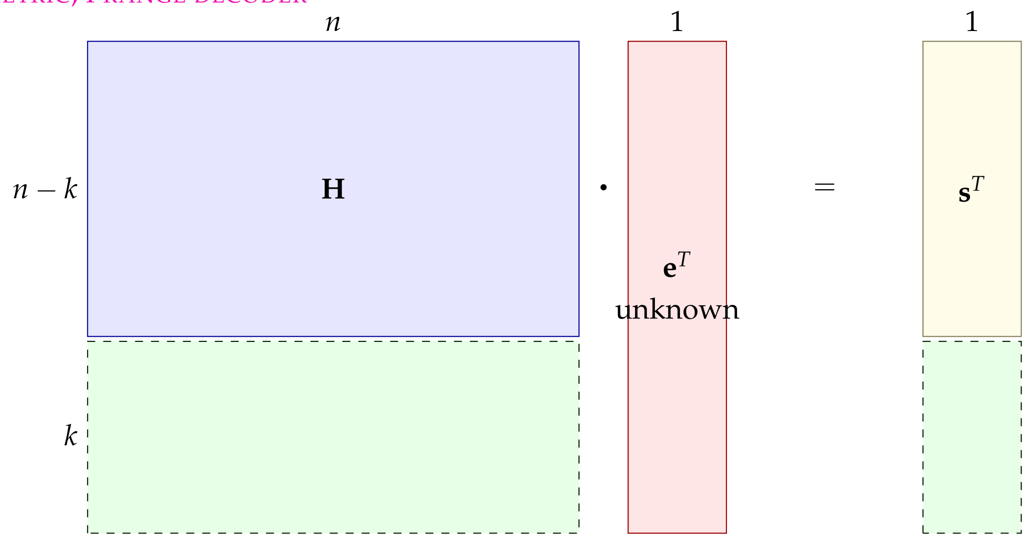
Part I

First approach

Hamming metric, Prange decoder

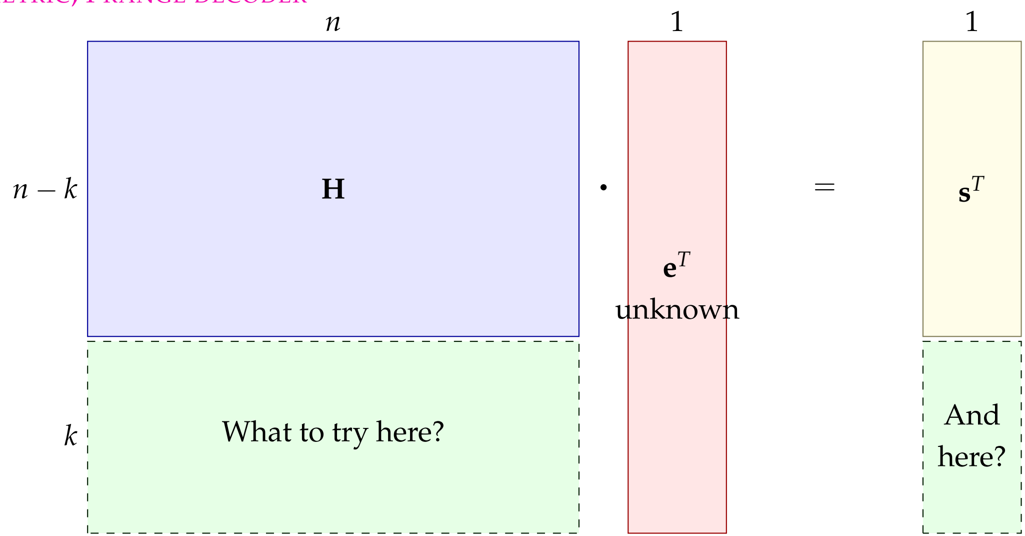


Hamming metric, Prange decoder



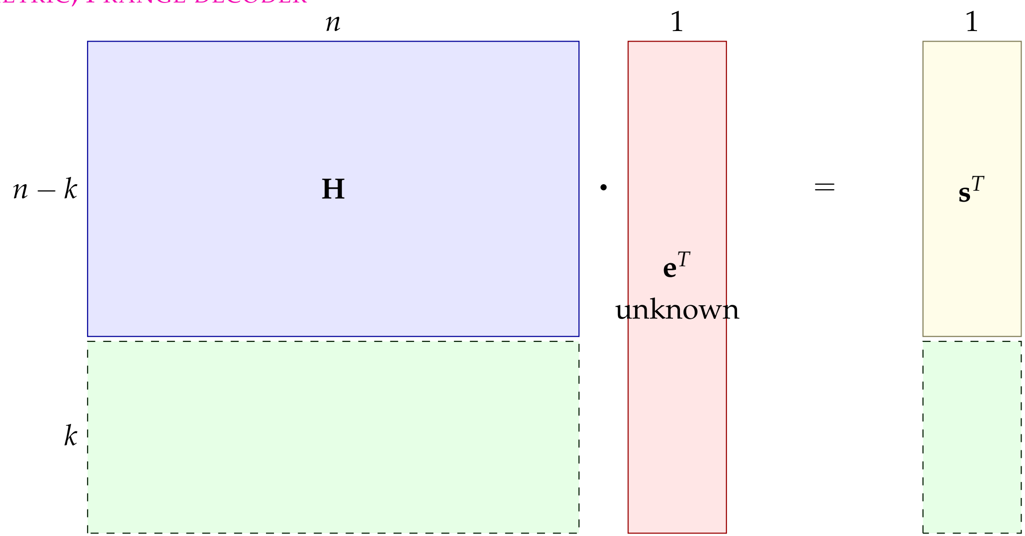
Idea: $\hat{\mathbf{e}}^T := \left(\frac{\mathbf{H}}{\textit{something}}\right)^{-1} \cdot \left(\frac{\mathbf{s}^T}{\textit{something else}}\right)$, try many times until $wt_H(\hat{\mathbf{e}}) \leq t \quad \rightarrow \quad \hat{\mathbf{e}} = \mathbf{e}$

Hamming metric, Prange decoder



Idea: $\hat{\mathbf{e}}^T := \left(\frac{\mathbf{H}}{\textit{something}}\right)^{-1} \cdot \left(\frac{\mathbf{s}^T}{\textit{something else}}\right)$, try many times until $wt_H(\hat{\mathbf{e}}) \leq t \quad \rightarrow \quad \hat{\mathbf{e}} = \mathbf{e}$

Hamming metric, Prange decoder



One answer: LEFT: rows that are orthogonal to many $\mathbf{e}$'s with $wt_H(\mathbf{e}) \leq t$, RIGHT: 0's.

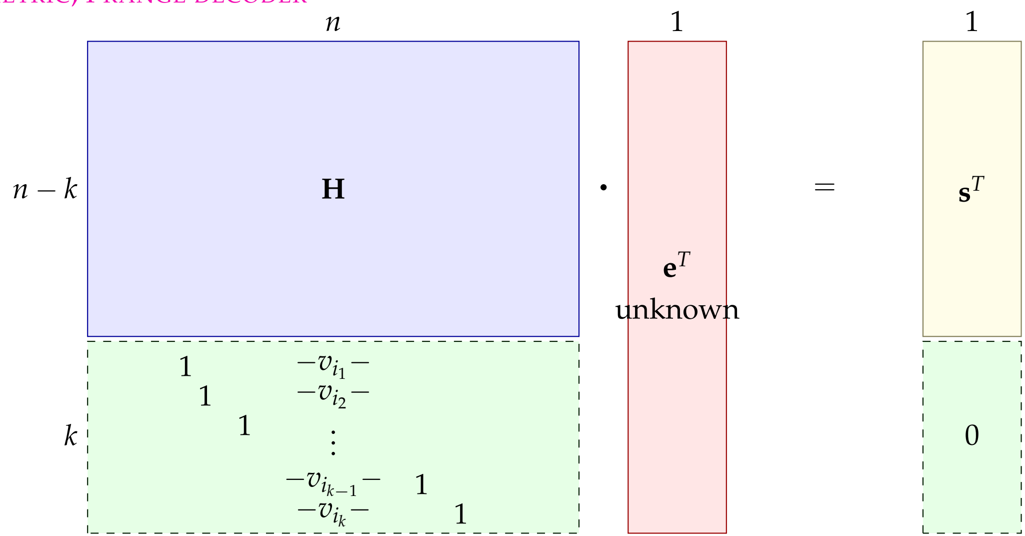
Hamming metric, Prange decoder

$$
\begin{array}{cc}
 & n \\
n-k & \mathbf{H} \\
k & \begin{matrix} 1 & & & -v_{i_1}- & & \\ & 1 & & -v_{i_2}- & & \\ & & 1 & & & \\ & & & \vdots & & \\ & & & -v_{i_{k-1}}- & 1 & \\ & & & -v_{i_k}- & & 1 \end{matrix}
\end{array}
\cdot
\begin{array}{c} 1 \\ \mathbf{e}^T \\ \text{unknown} \end{array}
=
\begin{array}{c} 1 \\ \mathbf{s}^T \\ 0 \end{array}
$$

LEFT: rows that are orthogonal to many $\mathbf{e}$'s with $wt_H(\mathbf{e}) \leq t$, RIGHT: 0's.

Try space spanned by k standard basis vectors v_i

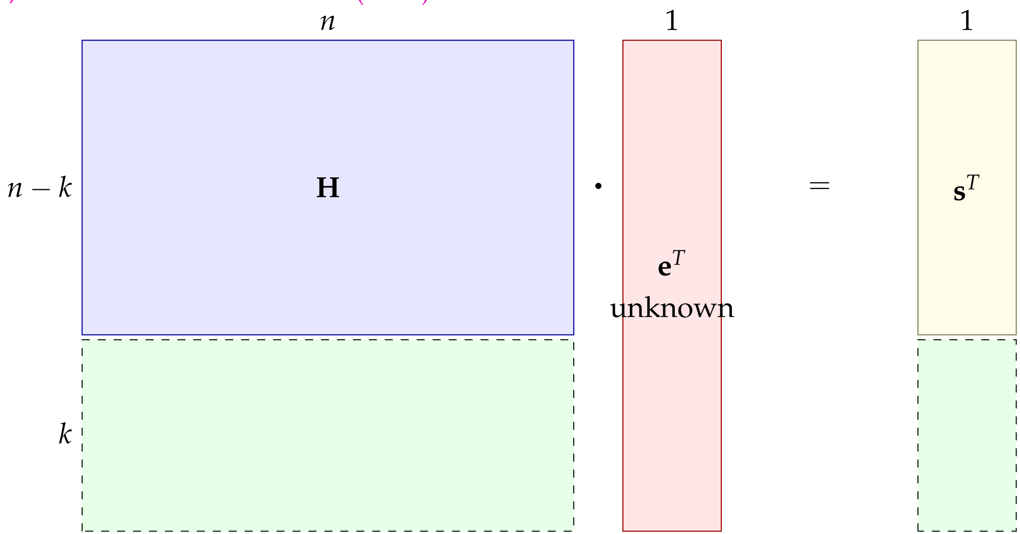
HAMMING METRIC, PRANGE DECODER



LEFT: rows that are orthogonal to many $\mathbf{e}$'s with $wt_H(\mathbf{e}) \leq t$, RIGHT: 0's.

Try space spanned by k standard basis vectors $v_i \rightarrow \binom{n}{k}$ choices, $\binom{n-t}{k}$ successful if all $i \in \mathrm{Support}(\mathbf{e})^c$

Rank metric, Gaborit-Ruatta-Schrek (GRS)



LEFT: rows that are orthogonal to many $\mathbf{e}$'s with $wt_R(\mathbf{e}) \leq t$, RIGHT: 0's.

Rank metric, Gaborit-Ruatta-Schrek (GRS)

$$\begin{array}{cc} & n \\ n-k & \mathbf{H} \\ k & \begin{matrix} -v_1- \\ -v_2- \\ \vdots \\ -v_{k-1}- \\ -v_k- \end{matrix} \end{array} \cdot \begin{array}{c} 1 \\ \mathbf{e}^T \\ \text{unknown} \end{array} = \begin{array}{c} 1 \\ \mathbf{s}^T \\ 0 \end{array}$$

LEFT: rows that are orthogonal to many $\mathbf{e}$'s with $wt_R(\mathbf{e}) \leq t$, RIGHT: 0's.

Try space spanned by k indep. vectors $v_i \in \mathbb{F}_q^n$

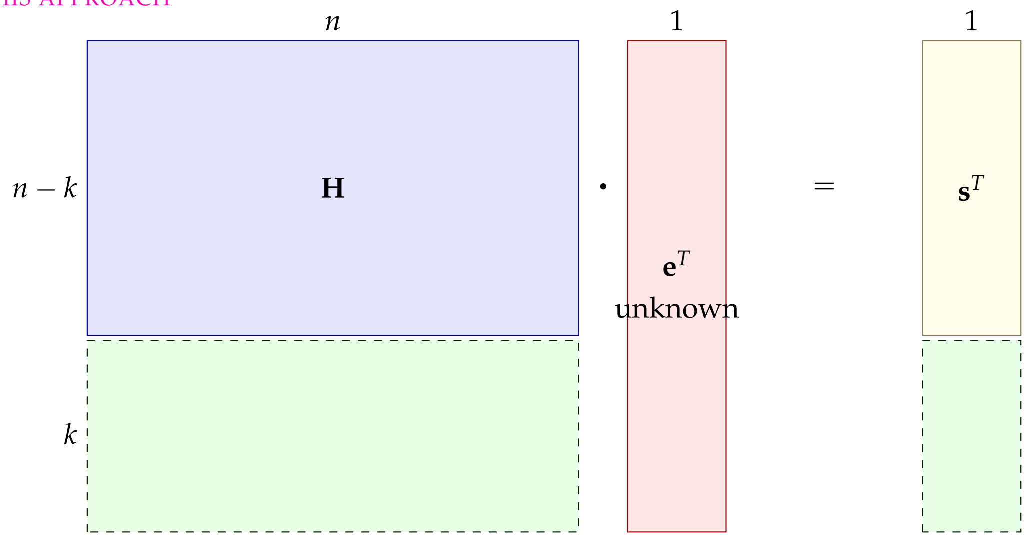
Rank metric, Gaborit-Ruatta-Schrek (GRS)

$$\begin{array}{r} \\ n-k \\ \\ k \end{array} \begin{array}{c} n \\ \left[\begin{array}{c} \mathbf{H} \\ \hline -v_1- \\ -v_2- \\ \vdots \\ -v_{k-1}- \\ -v_k- \end{array}\right] \end{array} \cdot \begin{array}{c} 1 \\ \left[\begin{array}{c} \mathbf{e}^T \\ \text{unknown} \end{array}\right] \end{array} = \begin{array}{c} 1 \\ \left[\begin{array}{c} \mathbf{s}^T \\ \hline 0 \end{array}\right] \end{array}$$

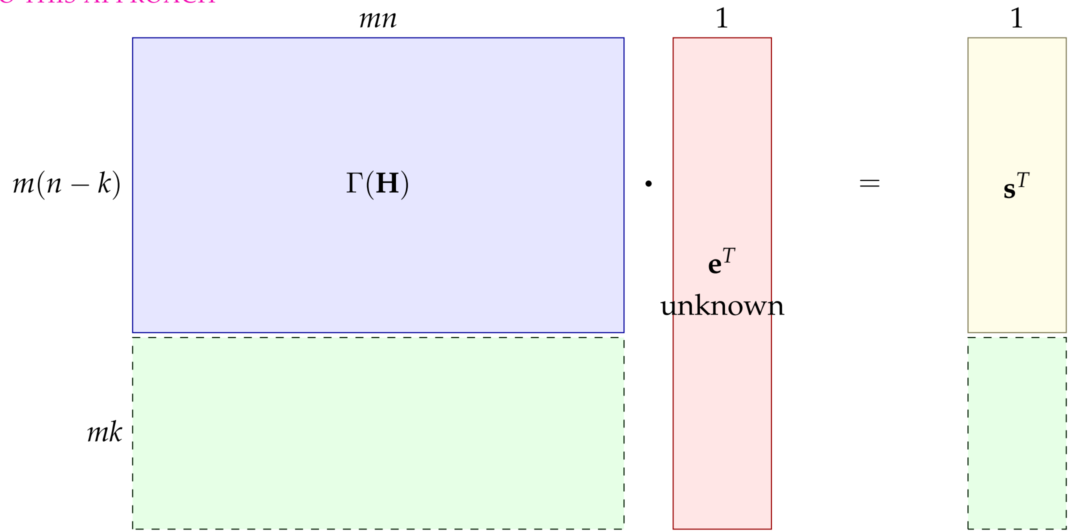
LEFT: rows that are orthogonal to many $\mathbf{e}$'s with $wt_R(\mathbf{e}) \leq t$, RIGHT: 0's.

Try space spanned by k indep. vectors $v_i \in \mathbb{F}_q^n \quad \rightarrow \quad \begin{bmatrix} n \\ k \end{bmatrix}_q$ choices, $\begin{bmatrix} n-t \\ k \end{bmatrix}_q$ successful if all $v_i \in \mathrm{RowSpan}_{\mathbb{F}_q}(\mathbf{e})^\perp$

Bounds to this approach

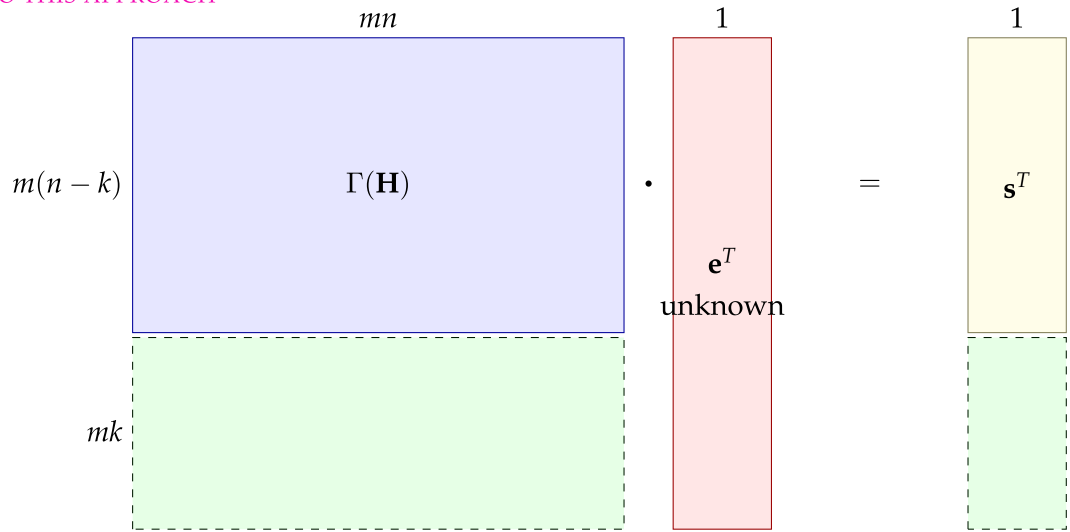


Bounds to this approach



For generality: transform into $\mathbb{F}_q$-linear problem using $\mathbb{F}_q$-basis Γ of $\mathbb{F}_{q^m}$

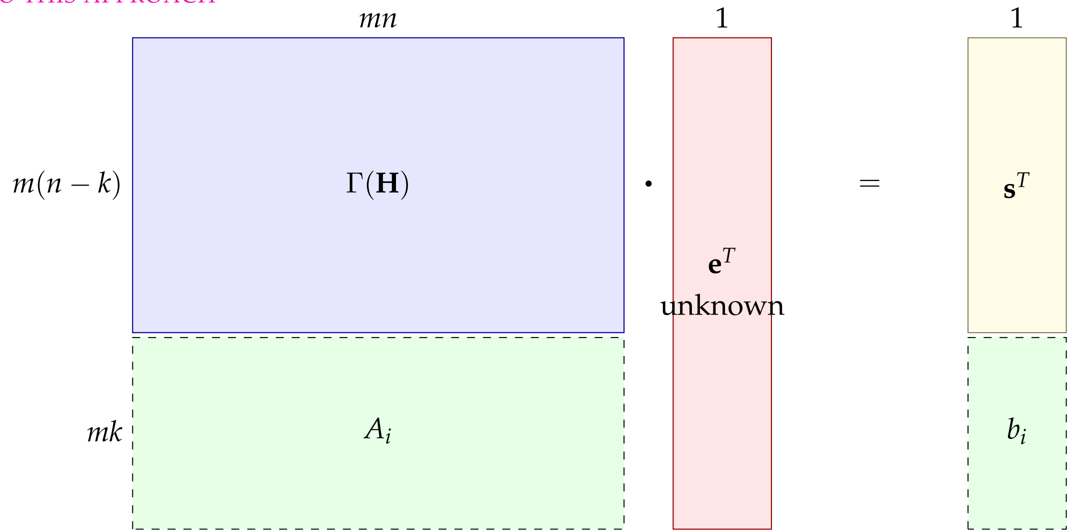
Bounds to this approach



For generality: transform into $\mathbb{F}_q$-linear problem using $\mathbb{F}_q$-basis Γ of $\mathbb{F}_{q^m}$

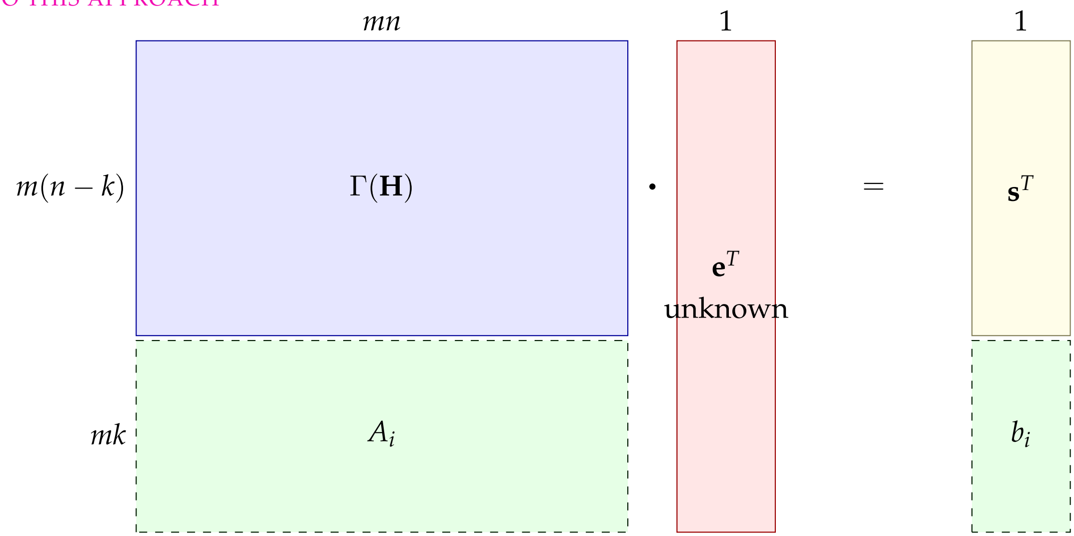
(Additional step: can use parity-check matrix of $\mathcal{C} + \langle \mathbf{e} \rangle$ instead of $\mathcal{C}$)

Bounds to this approach



Test set $\mathcal{T} = \{(A_i, b_i) \mid i \in \mathcal{I}\}$.

Bounds to this approach



Test set $\mathcal{T} = \{(A_i, b_i) \mid i \in \mathcal{I}\}$. Expected number of pairs to try is $N_{\mathcal{T}}(\mathbf{e}) := \dfrac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i \mathbf{e}^T = b_i\}|}$

Bounds to this approach

Test set $\mathcal{T} = \{(A_i, b_i) \mid i \in \mathcal{I}\}$. Expected number of pairs to try is $N_{\mathcal{T}}(\mathbf{e}) := \dfrac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i \mathbf{e}^T = b_i\}|}$

Bounds to this approach

Test set $\mathcal{T} = \{(A_i, b_i) \mid i \in \mathcal{I}\}$. Expected number of pairs to try is $N_{\mathcal{T}}(\mathbf{e}) := \dfrac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i\mathbf{e}^T = b_i\}|}$

Average of $N_{\mathcal{T}}(\mathbf{e})$ over all $\mathbf{e}$'s of weight t:

Bounds to this approach

Test set $\mathcal{T} = \{(A_i, b_i) \mid i \in \mathcal{I}\}$. Expected number of pairs to try is $N_{\mathcal{T}}(\mathbf{e}) := \dfrac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i \mathbf{e}^T = b_i\}|}$

Average of $N_{\mathcal{T}}(\mathbf{e})$ over all $\mathbf{e}$'s of weight t: $N_{\mathcal{T}}$ = expected run-time/complexity.

Bounds to this approach

Test set $\mathcal{T} = \{(A_i, b_i) \mid i \in \mathcal{I}\}$. Expected number of pairs to try is $N_{\mathcal{T}}(\mathbf{e}) := \dfrac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i\mathbf{e}^T = b_i\}|}$

Average of $N_{\mathcal{T}}(\mathbf{e})$ over all $\mathbf{e}$'s of weight t: $N_{\mathcal{T}}$ = expected run-time/complexity.

Lemma

$$\boxed{N_{\mathcal{T}} \geq \frac{|\{\mathbf{e} \mid wt(\mathbf{e}) = t\}|}{\max_{(A,b)\in\mathcal{T}} |\{\mathbf{e} \mid wt(\mathbf{e}) = t,\ A\mathbf{e}^T = b\}|}}$$

Test set $\mathcal{T} = \{(A_i, b_i) \mid i \in \mathcal{I}\}$. Expected number of pairs to try is $N_{\mathcal{T}}(\mathbf{e}) := \dfrac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i \mathbf{e}^T = b_i\}|}$
Average of $N_{\mathcal{T}}(\mathbf{e})$ over all $\mathbf{e}$'s of weight t: $N_{\mathcal{T}}$ = expected run-time/complexity.

Lemma

$$\boxed{N_{\mathcal{T}} \geq \frac{|\{\mathbf{e} \mid wt(\mathbf{e}) = t\}|}{\max_{(A,b)\in\mathcal{T}} |\{\mathbf{e} \mid wt(\mathbf{e}) = t,\ A\mathbf{e}^T = b\}|}}$$

Open Problem

v.1: Let $A \in \mathbb{F}_q^{mk \times mn}$, $b \in \mathbb{F}_q^{mk}$. Give an upper-bound on the maximum cardinality of

$$\{\mathbf{e} \mid wt_R(\mathbf{e}) = t,\ A\mathbf{e}^T = b\}.$$

Test set $\mathcal{T} = \{(A_i, b_i) \mid i \in \mathcal{I}\}$. Expected number of pairs to try is $N_{\mathcal{T}}(\mathbf{e}) := \dfrac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i\mathbf{e}^T = b_i\}|}$

Average of $N_{\mathcal{T}}(\mathbf{e})$ over all $\mathbf{e}$'s of weight t: $N_{\mathcal{T}}$ = expected run-time/complexity.

Lemma

$$\boxed{N_{\mathcal{T}} \geq \frac{|\{\mathbf{e} \mid wt(\mathbf{e}) = t\}|}{\max_{(A,b)\in\mathcal{T}} |\{\mathbf{e} \mid wt(\mathbf{e}) = t,\ A\mathbf{e}^T = b\}|}}$$

Open Problem

v.2: Let $\mathcal{S} = \{x \mid Ax = b\} \subset \mathbb{F}_q^{mn}$ *be a translated subspace/coset with* $|\mathcal{S}| = q^{m(n-k)}$*. Give an upper-bound on the maximum cardinality of*

$$\mathcal{S} \ \cap\ \{\mathbf{e} \mid wt_R(\mathbf{e}) = t\}.$$

BOUNDS TO THIS APPROACH

Test set $\mathcal{T} = \{(A_i, b_i) \mid i \in \mathcal{I}\}$. Expected number of pairs to try is $N_{\mathcal{T}}(\mathbf{e}) := \dfrac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i\mathbf{e}^T = b_i\}|}$
Average of $N_{\mathcal{T}}(\mathbf{e})$ over all $\mathbf{e}$'s of weight t: $N_{\mathcal{T}}$ = expected run-time/complexity.

Lemma

$$\boxed{N_{\mathcal{T}} \geq \frac{|\{\mathbf{e} \mid wt(\mathbf{e}) = t\}|}{\max_{(A,b)\in\mathcal{T}} |\{\mathbf{e} \mid wt(\mathbf{e}) = t,\, A\mathbf{e}^T = b\}|}}$$

Open Problem

v.3: Let $\mathcal{S} = \mathcal{D}\,(+v) \subset \mathbb{F}_q^{m\times n}$ be a (translated) matrix code with $|\mathcal{S}| = q^{m(n-k)}$. Give an upper-bound on

$$W_t(\mathcal{S}) := |\{X \in \mathcal{S} \mid wt_R(X) = t\}|,$$

in terms of q, m, n, k, t that holds for all $\mathcal{S}$.

Test set $\mathcal{T} = \{(A_i, b_i) \mid i \in \mathcal{I}\}$. Expected number of pairs to try is $N_{\mathcal{T}}(\mathbf{e}) := \dfrac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i \mathbf{e}^T = b_i\}|}$
Average of $N_{\mathcal{T}}(\mathbf{e})$ over all $\mathbf{e}$'s of weight t: $N_{\mathcal{T}}$ = expected run-time/complexity.

Lemma

$$\boxed{N_{\mathcal{T}} \geq \frac{|\{\mathbf{e} \mid wt(\mathbf{e}) = t\}|}{\max_{(A,b)\in\mathcal{T}} |\{\mathbf{e} \mid wt(\mathbf{e}) = t,\ A\mathbf{e}^T = b\}|}}$$

Open Problem

v.3: Let $\mathcal{S} = \mathcal{D}\,(+v) \subset \mathbb{F}_q^{m\times n}$ be a (translated) matrix code with $|\mathcal{S}| = q^{m(n-k)}$. Give an upper-bound on

$$W_t(\mathcal{S}) := |\{X \in \mathcal{S} \mid wt_R(X) = t\}|,$$

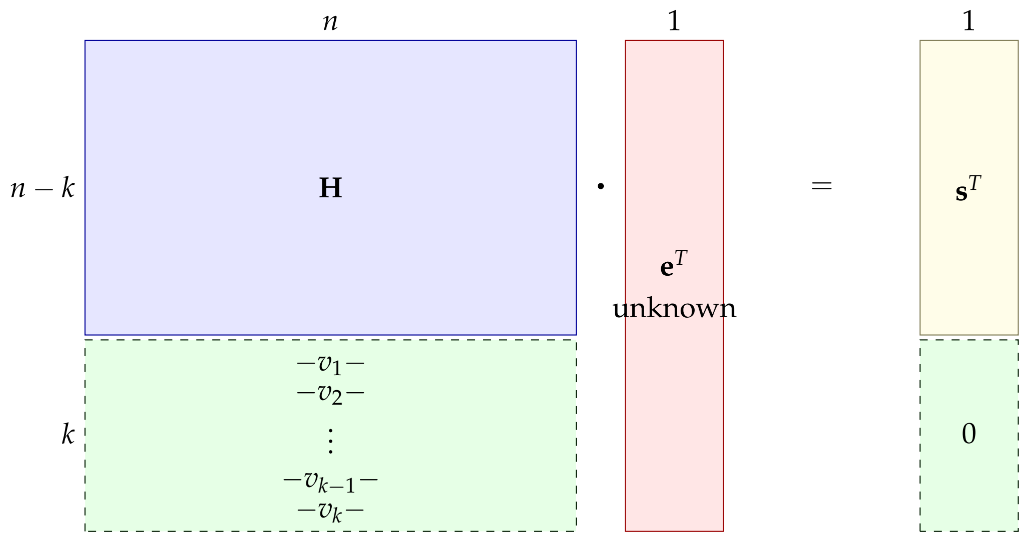
in terms of q, m, n, k, t that holds for all $\mathcal{S}$.

Any upper bound on $W_t(\mathcal{S})$ will imply a **lower bound on the complexity** possible with this approach.

Part II

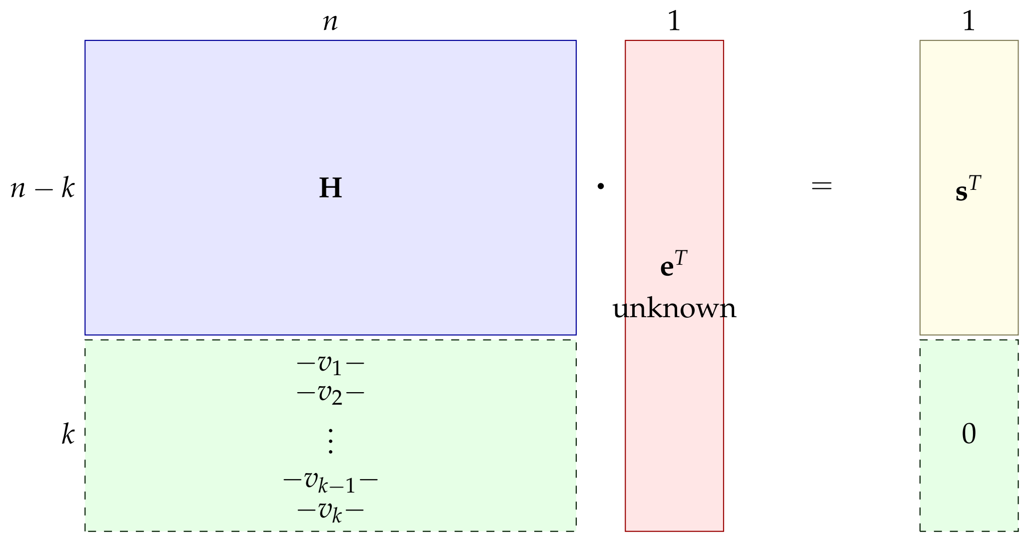
Second Approach

GRS-like decoder



Try space spanned by k indep. vectors $v_i \in \mathbb{F}_q^n \quad \rightarrow \quad \begin{bmatrix} n \\ k \end{bmatrix}_q$ choices, $\begin{bmatrix} n-t \\ k \end{bmatrix}_q$ successful if $\mathrm{Span}(v_i) \subseteq \mathrm{RowSpan}_{\mathbb{F}_q}(\mathbf{e})^\perp$

GRS-like decoder



Try space spanned by k indep. vectors $v_i \in \mathbb{F}_q^n$ $\rightarrow$ $\begin{bmatrix} n \\ k \end{bmatrix}_q$ choices, $\begin{bmatrix} n-t \\ k \end{bmatrix}_q$ successful if $\mathrm{Span}(v_i) \subseteq \mathrm{RowSpan}_{\mathbb{F}_q}(\mathbf{e})^\perp$

Equivalent: choosing an $(n-k)$-dim space $W = \mathrm{Span}(v_i)^\perp$, successful if $W \supseteq \mathrm{RowSpan}_{\mathbb{F}_q}(\mathbf{e})$

Normal algorithm

Normal algorithm

1. Choose random $(n-k)$-dim space W

Normal algorithm

1. Choose random $(n-k)$-dim space W
2. Solve system lin. equations with $v_i \in W^{\perp}$

Normal algorithm

1. Choose random $(n-k)$-dim space W
2. Solve system lin. equations with $v_i \in W^{\perp}$
3. Check if solution has $wt_R \leq t$.
   If not, go back to 1.

Normal algorithm

1. Choose random $(n-k)$-dim space W
2. Solve system lin. equations with $v_i \in W^\perp$
3. Check if solution has $wt_R \leq t$.
   If not, go back to 1.

Idea: learn from each failed solution

Adaptive algorithm

1. Choose random $(n-k)$-dim space W
2. Solve system lin. equations with $v_i \in W^{\perp}$
3. Check if solution has $wt_R \leq t$.
   If not, **learn from solution**, go back to 1. and **choose more effectively**/narrow down your search

Idea: learn from each failed solution

***Adaptive* algorithm**

1. Choose random $(n-k)$-dim space W
2. Solve system lin. equations with $v_i \in W^{\perp}$
3. Check if solution has $wt_R \leq t$.
   If not, **learn from solution**, go back to 1. and **choose more effectively**/narrow down your search

Idea: learn from each failed solution $\rightarrow$ requires **magic!**

Open Problem (Magic[1] Step)

[1] Official terminology by V. Weger (2023)

Open Problem (Magic[1] Step)

Let $(\mathbf{H}, \mathbf{s}, t)$ *be an instance of RSDP with unique solution* $\mathbf{e}$ *satisfying* $wt_R(\mathbf{e}) = t$.

[1] Official terminology by V. Weger (2023)

Open Problem (Magic[1] Step)

Let $(\mathbf{H}, \mathbf{s}, t)$ *be an instance of RSDP with unique solution* $\mathbf{e}$ *satisfying* $wt_R(\mathbf{e}) = t$.
Let $\mathbf{x}$ *be a solution to* $\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ *(without weight constraint).*

[1] Official terminology by V. Weger (2023)

Open Problem (Magic[1] Step)

Let $(\mathbf{H}, \mathbf{s}, t)$ *be an instance of RSDP with unique solution* $\mathbf{e}$ *satisfying* $wt_R(\mathbf{e}) = t$.
Let $\mathbf{x}$ *be a solution to* $\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ *(without weight constraint).*

Give an algorithm to decide if the intersection

$$\mathrm{RowSpan}(\mathbf{x}) \ \cap \ \mathrm{RowSpan}(\mathbf{e})$$

*is **non-trivial** (dim > 0) with probability* $\geq p$*, for some fixed* $p \in [0, 1]$.

[1] Official terminology by V. Weger (2023)

Open Problem (Magic[1] Step)

Let $(\mathbf{H}, \mathbf{s}, t)$ be an instance of RSDP with unique solution $\mathbf{e}$ satisfying $wt_R(\mathbf{e}) = t$.
Let $\mathbf{x}$ be a solution to $\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ (without weight constraint).

Give an algorithm to decide if the intersection

$$\mathrm{RowSpan}(\mathbf{x}) \ \cap \ \mathrm{RowSpan}(\mathbf{e})$$

*is **non-trivial** (dim > 0) with probability $\geq p$, for some fixed $p \in [0, 1]$.*

Magically enhanced algorithm idea

[1] Official terminology by V. Weger (2023)

Open Problem (Magic[1] Step)

Let $(\mathbf{H}, \mathbf{s}, t)$ be an instance of RSDP with unique solution $\mathbf{e}$ satisfying $wt_R(\mathbf{e}) = t$.
Let $\mathbf{x}$ be a solution to $\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ (without weight constraint).

Give an algorithm to decide if the intersection

$$\mathrm{RowSpan}(\mathbf{x}) \; \cap \; \mathrm{RowSpan}(\mathbf{e})$$

*is **non-trivial** (dim > 0) with probability $\geq p$, for some fixed $p \in [0, 1]$.*

Magically enhanced algorithm idea

1. Choose random $(n-k)$-dim space W

[1] Official terminology by V. Weger (2023)

Open Problem (Magic[1] Step)

Let $(\mathbf{H}, \mathbf{s}, t)$ be an instance of RSDP with unique solution $\mathbf{e}$ satisfying $wt_R(\mathbf{e}) = t$.
Let $\mathbf{x}$ be a solution to $\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ (without weight constraint).

Give an algorithm to decide if the intersection

$$\mathrm{RowSpan}(\mathbf{x}) \cap \mathrm{RowSpan}(\mathbf{e})$$

is ***non-trivial*** *(dim > 0) with probability $\geq p$, for some fixed $p \in [0, 1]$.*

Magically enhanced algorithm idea

1. Choose random $(n-k)$-dim space W
2. Solve system lin. equations with $v_i \in W^\perp$

[1] Official terminology by V. Weger (2023)

Open Problem (Magic[1] Step)

Let $(\mathbf{H}, \mathbf{s}, t)$ be an instance of RSDP with unique solution $\mathbf{e}$ satisfying $wt_R(\mathbf{e}) = t$.
Let $\mathbf{x}$ be a solution to $\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ (without weight constraint).

Give an algorithm to decide if the intersection

$$\mathrm{RowSpan}(\mathbf{x}) \;\cap\; \mathrm{RowSpan}(\mathbf{e})$$

*is **non-trivial** (dim > 0) with probability $\geq p$, for some fixed $p \in [0, 1]$.*

Magically enhanced algorithm idea

1. Choose random $(n-k)$-dim space W
2. Solve system lin. equations with $v_i \in W^{\perp}$
3. Check if solution $\mathbf{x}$ has $wt_R \leq t$.

[1] Official terminology by V. Weger (2023)

Open Problem (Magic[1] Step)

Let $(\mathbf{H}, \mathbf{s}, t)$ *be an instance of RSDP with unique solution* $\mathbf{e}$ *satisfying* $wt_R(\mathbf{e}) = t$.
Let $\mathbf{x}$ *be a solution to* $\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ *(without weight constraint).*

Give an algorithm to decide if the intersection

$$\mathrm{RowSpan}(\mathbf{x}) \;\cap\; \mathrm{RowSpan}(\mathbf{e})$$

is ***non-trivial*** *(dim* > 0*) with probability* $\geq p$*, for some fixed* $p \in [0, 1]$.

Magically enhanced algorithm idea

1. Choose random $(n-k)$-dim space W
2. Solve system lin. equations with $v_i \in W^{\perp}$
3. Check if solution $\mathbf{x}$ has $wt_R \leq t$.
   If not, and MagicStep outputs "*trivial*", go back to 1.

[1] Official terminology by V. Weger (2023)

Open Problem (Magic[1] Step)

Let $(\mathbf{H}, \mathbf{s}, t)$ be an instance of RSDP with unique solution $\mathbf{e}$ satisfying $wt_R(\mathbf{e}) = t$.
Let $\mathbf{x}$ be a solution to $\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ (without weight constraint).

Give an algorithm to decide if the intersection

$$\mathrm{RowSpan}(\mathbf{x}) \ \cap \ \mathrm{RowSpan}(\mathbf{e})$$

is ***non-trivial*** *(dim > 0) with probability $\geq p$, for some fixed $p \in [0, 1]$.*

Magically enhanced algorithm idea

1. Choose random $(n-k)$-dim space W
2. Solve system lin. equations with $v_i \in W^{\perp}$
3. Check if solution $\mathbf{x}$ has $wt_R \leq t$.
   If not, and MagicStep outputs "*trivial*", go back to 1.
   If not, and MagicStep outputs "*non-trivial*", let $U := \mathrm{RowSpan}(\mathbf{x})$.
      Go back to 1. but narrow down the search to only spaces W with $W \cap U$ non-trivial.

[1] Official terminology by V. Weger (2023)

Open Problem (Magic Step)

Let $(\mathbf{H}, \mathbf{s}, t)$ be an instance of RSDP with unique solution $\mathbf{e}$ satisfying $wt_R(\mathbf{e}) = t$.
Let $\mathbf{x}$ be a solution to $\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ (without weight constraint).

Give an algorithm to decide if the intersection

$$\mathrm{RowSpan}(\mathbf{x}) \ \cap \ \mathrm{RowSpan}(\mathbf{e})$$

*is **non-trivial** (dim > 0) with probability $\geq p$, for some fixed $p \in [0, 1]$.*

Open Problem (Magic Step)

Let $(\mathbf{H}, \mathbf{s}, t)$ be an instance of RSDP with unique solution $\mathbf{e}$ satisfying $wt_R(\mathbf{e}) = t$.
Let $\mathbf{x}$ be a solution to $\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ (without weight constraint).

Give an algorithm to decide if the intersection

$$\mathrm{RowSpan}(\mathbf{x}) \ \cap \ \mathrm{RowSpan}(\mathbf{e})$$

*is **non-trivial** (dim > 0) with probability $\geq p$, for some fixed $p \in [0, 1]$.*

For some trivial magic steps (slow & large p or fast & small p), we get GRS up to polynomial factor.

Can we do better?

Thank you for listening! and for your solutions to:

Open Problem (Magic Step)

Let $(\mathbf{H}, \mathbf{s}, t)$ be an instance of RSDP with unique solution $\mathbf{e}$ satisfying $wt_R(\mathbf{e}) = t$.
Let $\mathbf{x}$ be a solution to $\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ (without weight constraint).

Give an algorithm to decide if the intersection

$$\mathrm{RowSpan}(\mathbf{x}) \ \cap \ \mathrm{RowSpan}(\mathbf{e})$$

*is **non-trivial** (dim > 0) with probability $\geq p$, for some fixed $p \in [0, 1]$.*

Open Problem (Weight Upper-Bound)

Let $\mathcal{S} = \mathcal{D}\,(+v) \subset \mathbb{F}_q^{m \times n}$ be a (translated) matrix code with $|\mathcal{S}| = q^{m(n-k)}$. Give an upper-bound on

$$W_t(\mathcal{S}) := |\{X \in \mathcal{S} \mid wt_R(X) = t\}|,$$

in terms of q, m, n, k, t that holds for all $\mathcal{S}$.