

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

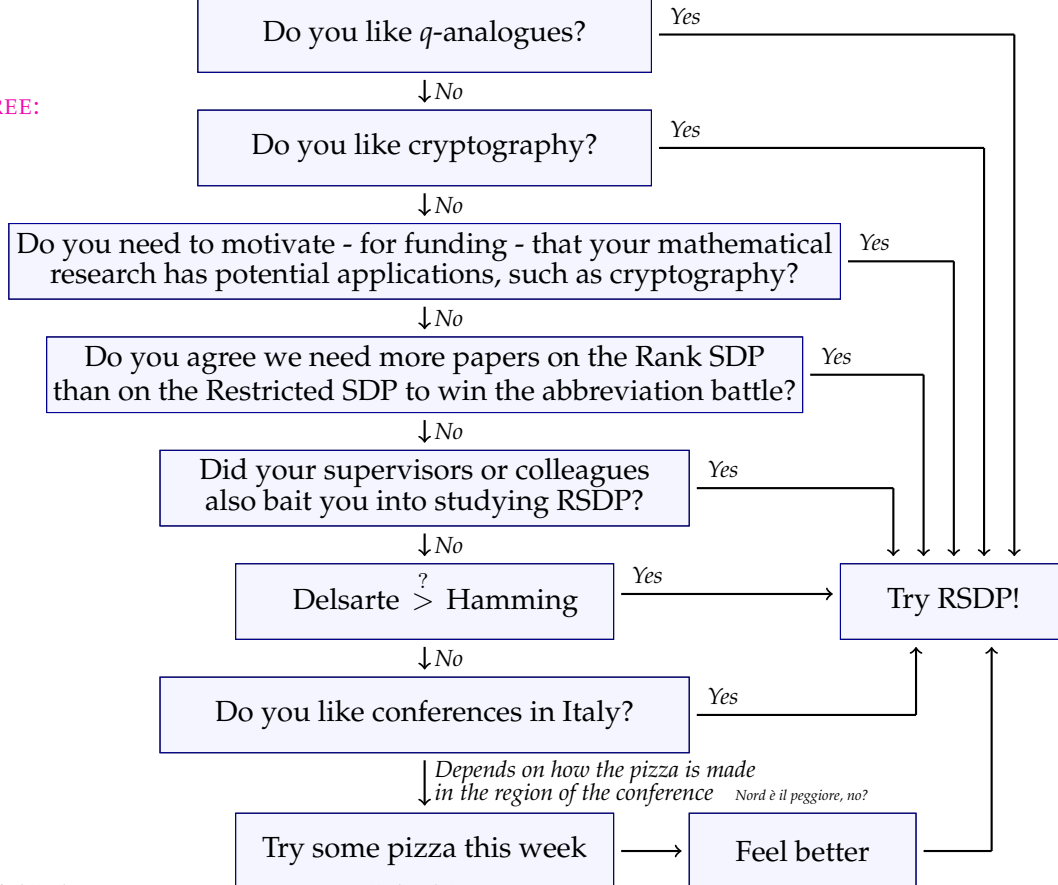
CONTENTS

- ▶ 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*TM

SHOULD YOU STUDY/CARE ABOUT RANK SYNDROME DECODING PROBLEM (RSDP)?

DECISION TREE:

DECISION TREE:



Part

PROBLEM INTRODUCTION

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

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

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

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

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

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

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

- ▶ \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

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

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

- ▶ \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
- ▶ \mathbb{F}_{q^m} -lin. vector code, rank weight wt_R , error $\mathbf{e} \in \mathbb{F}_{q^m}^n$: \mathbb{F}_{q^m} -linear RSDP

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

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

- ▶ \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
- ▶ \mathbb{F}_{q^m} -lin. vector code, rank weight wt_R , error $\mathbf{e} \in \mathbb{F}_{q^m}^n$: \mathbb{F}_{q^m} -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: $m \sim Mn$, $k \sim Rn$, $t \sim Tn$ 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: $m \sim Mn$, $k \sim Rn$, $t \sim Tn$ 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: $m \sim Mn$, $k \sim Rn$, $t \sim Tn$ 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: $m \sim Mn$, $k \sim Rn$, $t \sim Tn$ 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: $m \sim Mn$, $k \sim Rn$, $t \sim Tn$ 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:
 $q^{\min\{M,1\}RTn^2 + O(n)}$

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:

$$q^{\min\{M,1\}RTn^2 + O(n)}$$

▶

$$\lim_{n \rightarrow \infty} \frac{1}{n^2} \log_q(\text{complexity})$$

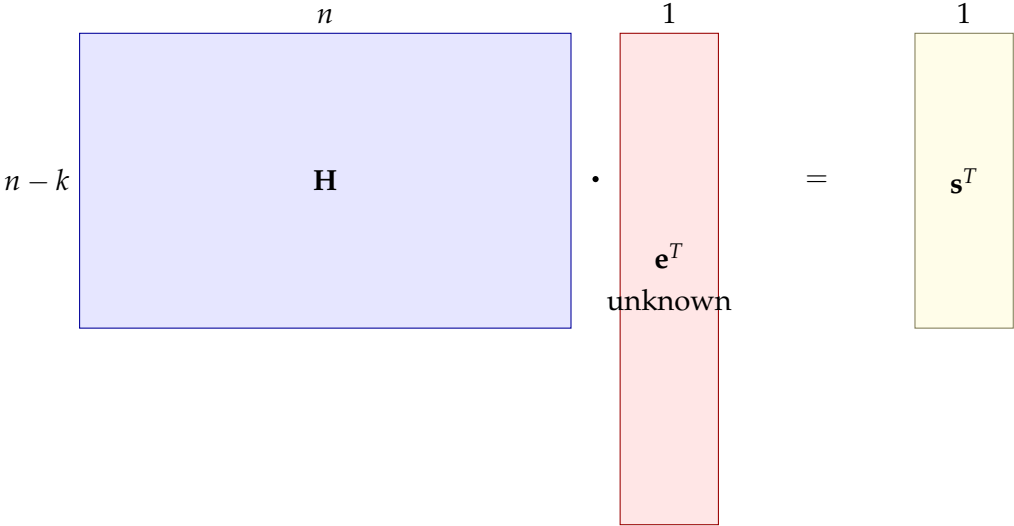
$$= \min\{M, 1\}RT$$

Can we improve asymptotically?

Part I

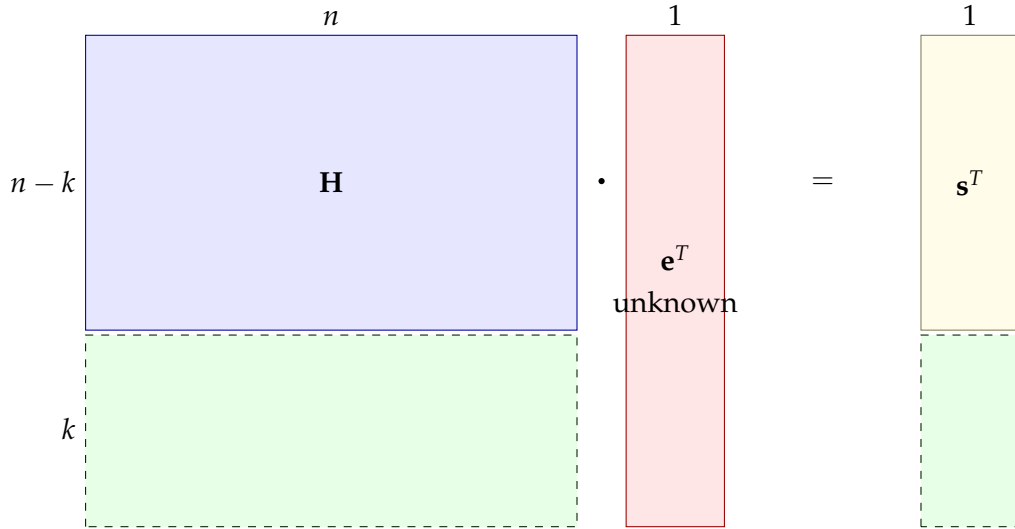
FIRST APPROACH

HAMMING METRIC, PRANGE DECODER



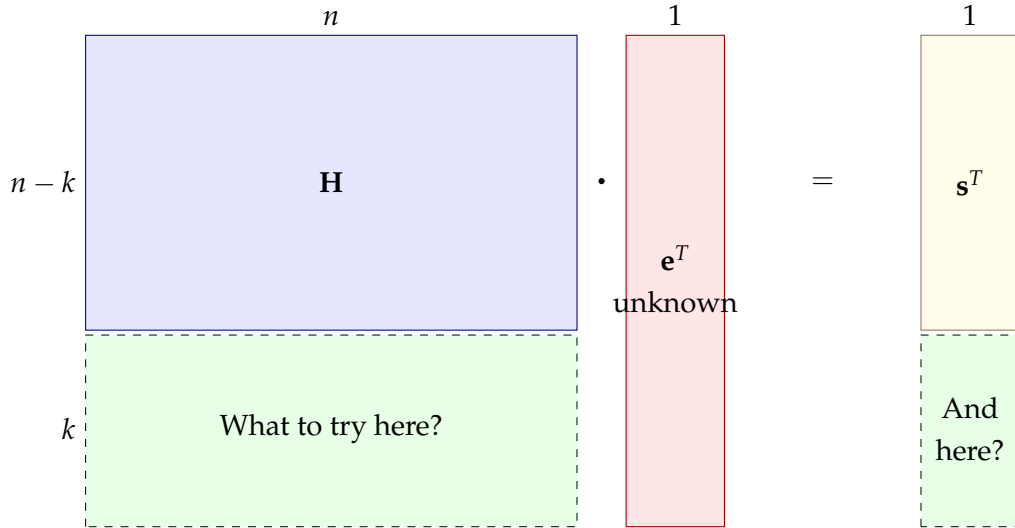
The diagram illustrates the equation $\mathbf{H} \cdot \mathbf{e}^T = \mathbf{s}^T$. On the left, a light blue rectangle represents the matrix \mathbf{H} , with its height labeled $n - k$ and its width labeled n . To its right is a light red vertical rectangle representing the vector \mathbf{e}^T , with its height labeled 1 and the text "unknown" below it. An equals sign follows, and on the right is a light yellow vertical rectangle representing the vector \mathbf{s}^T , with its height labeled 1 .

HAMMING METRIC, PRANGE DECODER



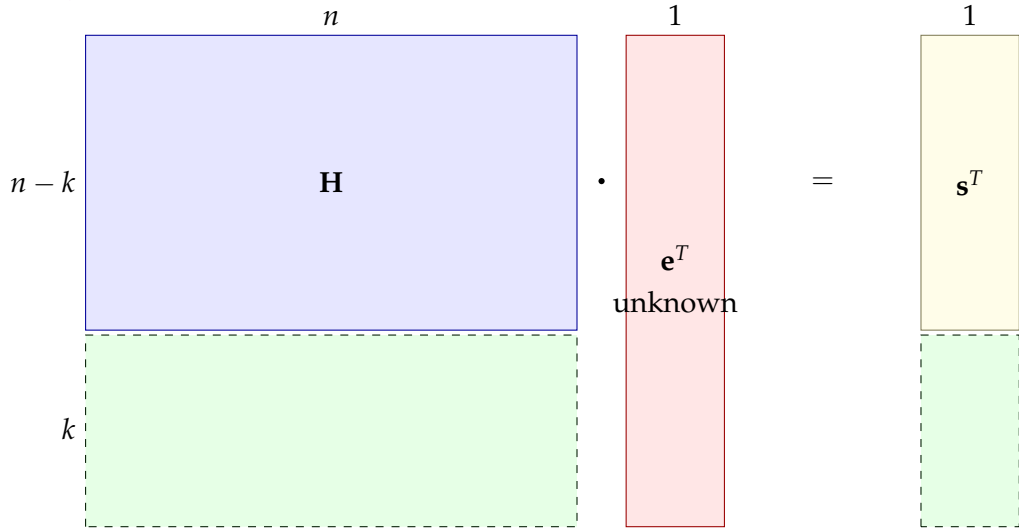
Idea: $\hat{\mathbf{e}}^T := \left(\begin{array}{c} \mathbf{H} \\ \text{something} \end{array} \right)^{-1} \cdot \left(\begin{array}{c} \mathbf{s}^T \\ \text{something else} \end{array} \right)$, try many times until $wt_H(\hat{\mathbf{e}}) \leq t \rightarrow \hat{\mathbf{e}} = \mathbf{e}$

HAMMING METRIC, PRANGE DECODER



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

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

$$\begin{array}{c}
 n \\
 \text{---} \\
 \begin{array}{|c|} \hline \mathbf{H} \\ \hline \end{array} \\
 n - k \\
 \cdot \\
 \begin{array}{|c|} \hline 1 \\ \hline \mathbf{e}^T \\ \hline \text{unknown} \\ \hline \end{array} \\
 = \\
 \begin{array}{|c|} \hline 1 \\ \hline \mathbf{s}^T \\ \hline \end{array} \\
 \text{---} \\
 \begin{array}{|c|} \hline 0 \\ \hline \end{array} \\
 k
 \end{array}$$

The diagram illustrates the matrix multiplication $\mathbf{H} \mathbf{e}^T = \mathbf{s}^T$. The matrix \mathbf{H} is partitioned into two parts: a top part of size $(n-k) \times n$ and a bottom part of size $k \times n$. The bottom part is shown as a dashed box containing a lower triangular matrix with 1s on the diagonal and $-v_i$ in the sub-diagonal. The vector \mathbf{e}^T is a column vector of size n , with the top element being 1 and the rest unknown. The resulting vector \mathbf{s}^T is a column vector of size n , with the top element being 1 and the bottom k elements being 0.

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

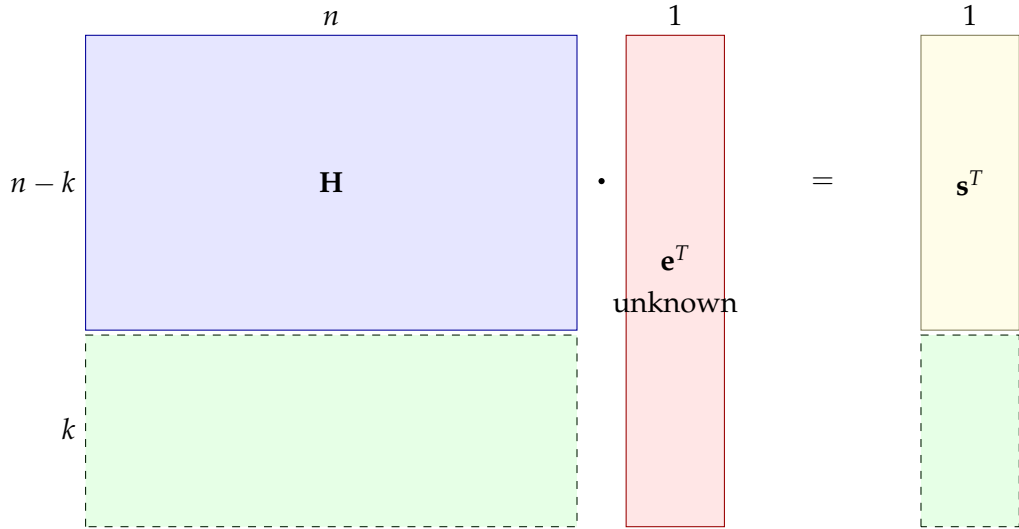
$$\begin{array}{ccc}
 & n & 1 & 1 \\
 & \begin{array}{|c|} \hline \mathbf{H} \\ \hline \end{array} & \cdot & = \\
 n-k & & \mathbf{e}^T & \mathbf{s}^T \\
 & & \text{unknown} & \\
 & \begin{array}{|c|} \hline \begin{array}{cccc} 1 & -v_{i_1} & & \\ & 1 & -v_{i_2} & \\ & & 1 & \vdots \\ & & & -v_{i_{k-1}}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

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 $v_i \rightarrow \binom{n}{k}$ choices, $\binom{n-t}{k}$ successful if all $i \in \text{Support}(\mathbf{e})^c$

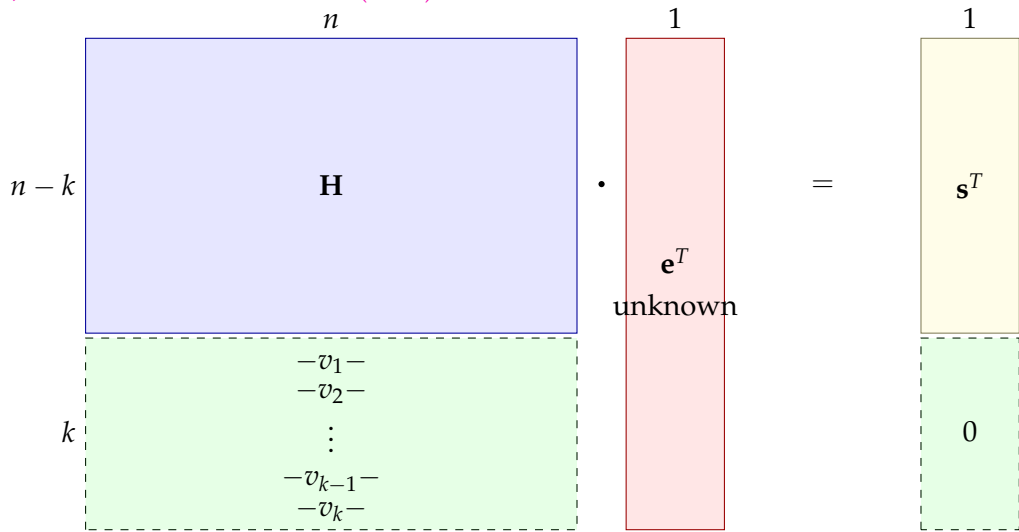
RANK METRIC, GABORIT-RUATTA-SCHREK (GRS)



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)

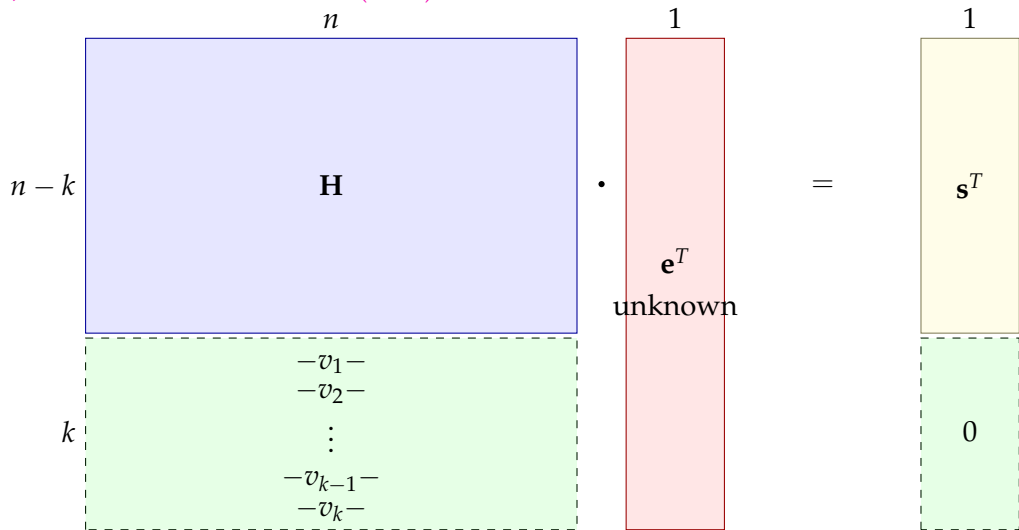


LEFT: rows that are orthogonal to many \mathbf{e} 's with $wt_R(\mathbf{e}) \leq t$,

RIGHT: 0's.

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

RANK METRIC, GABORIT-RUATTA-SCHREK (GRS)



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

RIGHT: 0's.

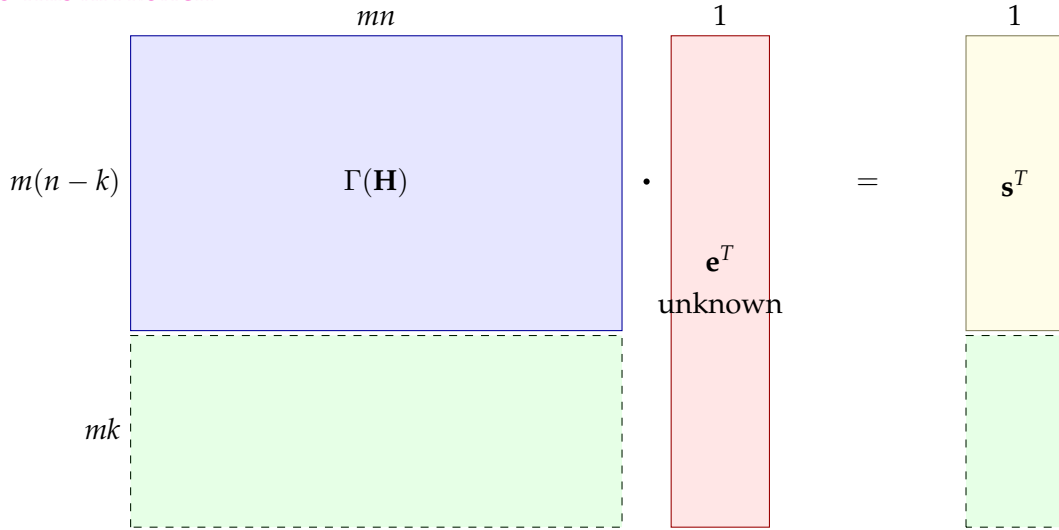
Try space spanned by k indep. vectors $v_i \in \mathbb{F}_q^n \rightarrow \begin{bmatrix} n \\ k \end{bmatrix}_q$ choices, $\begin{bmatrix} n-t \\ k \end{bmatrix}_q$ successful if all $v_i \in \text{RowSpan}_{\mathbb{F}_q}(\mathbf{e})^\perp$

BOUNDS TO THIS APPROACH

The diagram illustrates the dimensions of matrices and vectors in a rank metric decoding problem. It shows the following components:

- A purple rectangle representing a matrix \mathbf{H} with dimensions $(n-k) \times n$. The top edge is labeled n and the left edge is labeled $n-k$.
- A red vertical rectangle representing a vector \mathbf{e}^T with dimension 1. The top edge is labeled 1. The text \mathbf{e}^T and "unknown" are written inside the rectangle.
- An equals sign $=$ between the two rectangles.
- A yellow vertical rectangle representing a vector \mathbf{s}^T with dimension 1. The top edge is labeled 1. The text \mathbf{s}^T is written inside the rectangle.
- A green dashed rectangle representing a vector of dimension k . The left edge is labeled k . This dashed rectangle is positioned below the purple rectangle and the red rectangle, indicating that the bottom k rows of \mathbf{H} and the bottom k elements of \mathbf{e}^T are unknown.

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

$$\begin{array}{c}
 mn \\
 \Gamma(\mathbf{H}) \\
 m(n-k) \\
 mk \\
 \cdot \\
 \mathbf{e}^T \\
 \text{unknown} \\
 = \\
 \mathbf{s}^T \\
 1
 \end{array}$$

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

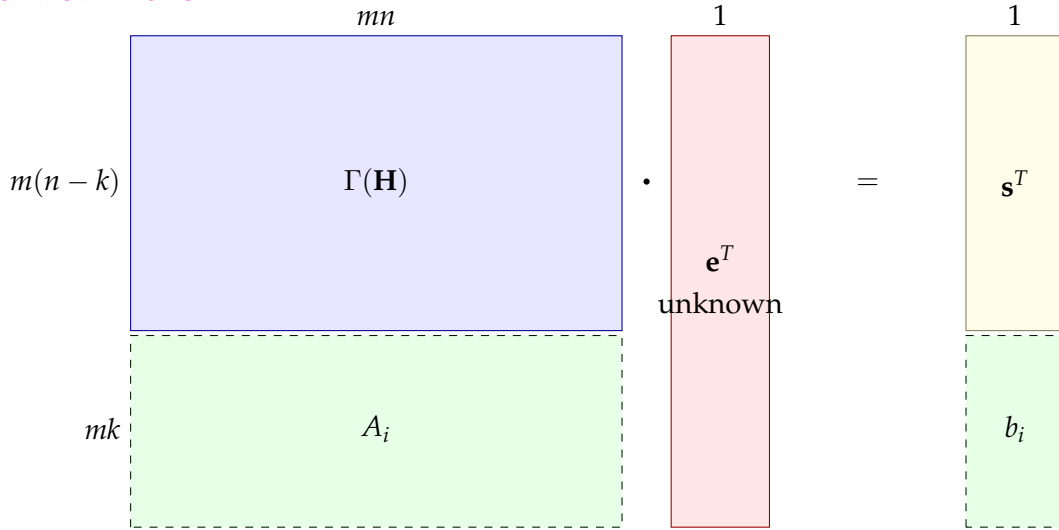
(Additional step: can use parity-check matrix of $\mathcal{C} + \langle \mathbf{e} \rangle$ instead of \mathcal{C})

BOUNDS TO THIS APPROACH

$$\begin{array}{c}
 mn \\
 \Gamma(\mathbf{H}) \\
 m(n-k) \\
 \cdot \\
 \mathbf{e}^T \\
 \text{unknown} \\
 = \\
 \mathbf{s}^T \\
 1 \\
 \end{array}
 \begin{array}{c}
 1 \\
 \mathbf{s}^T \\
 \end{array}$$

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 $N_{\mathcal{T}}(\mathbf{e}) := \frac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i \mathbf{e}^T = b_i\}|}$

BOUNDS TO THIS APPROACH

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

BOUNDS TO THIS APPROACH

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

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 $N_{\mathcal{T}}(\mathbf{e}) := \frac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i \mathbf{e}^T = b_i\}|}$
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 $N_{\mathcal{T}}(\mathbf{e}) := \frac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i \mathbf{e}^T = b_i\}|}$
Average of $N_{\mathcal{T}}(\mathbf{e})$ over all \mathbf{e} 's of weight t : $N_{\mathcal{T}} =$ expected run-time/complexity.

Lemma

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

BOUNDS TO THIS APPROACH

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

Lemma

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

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

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

BOUNDS TO THIS APPROACH

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

Lemma

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

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 $N_{\mathcal{T}}(\mathbf{e}) := \frac{|\mathcal{T}|}{|\{(A_i, b_i) \in \mathcal{T} \mid A_i \mathbf{e}^T = b_i\}|}$
Average of $N_{\mathcal{T}}(\mathbf{e})$ over all \mathbf{e} 's of weight t : $N_{\mathcal{T}} = \text{expected run-time/complexity}$.

Lemma

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

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} .

BOUNDS TO THIS APPROACH

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

Lemma

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

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

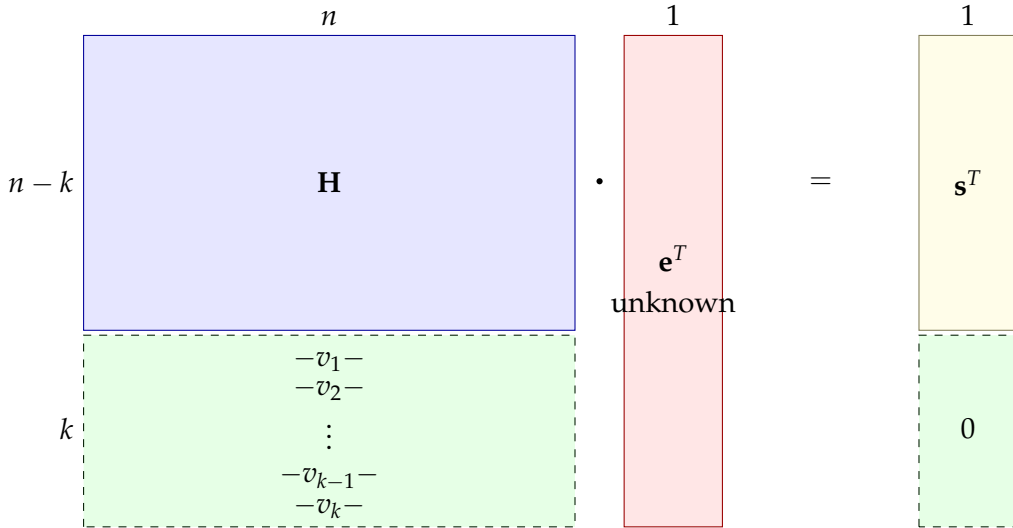
SECOND APPROACH

GRS-LIKE DECODER

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

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 $\text{Span}(v_i) \subseteq \text{RowSpan}_{\mathbb{F}_q}(\mathbf{e})^\perp$

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 $\text{Span}(v_i) \subseteq \text{RowSpan}_{\mathbb{F}_q}(\mathbf{e})^\perp$

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

GRS-LIKE DECODER

Normal algorithm

GRS-LIKE DECODER

Normal algorithm

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

GRS-LIKE DECODER

Normal algorithm

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

GRS-LIKE DECODER

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.

GRS-LIKE DECODER

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 DECODER APPROACH

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 DECODER APPROACH

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!**

ADAPTIVE DECODER APPROACH

Open Problem (Magic¹ Step)

¹Official terminology by V. Weger (2023)

ADAPTIVE DECODER APPROACH

Open Problem (Magic¹ Step)

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

¹Official terminology by V. Weger (2023)

Open Problem (Magic¹ 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).

¹Official terminology by V. Weger (2023)

ADAPTIVE DECODER APPROACH

Open Problem (Magic¹ Step)

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

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

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

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

¹Official terminology by V. Weger (2023)

ADAPTIVE DECODER APPROACH

Open Problem (Magic¹ Step)

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

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

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

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

Magically enhanced algorithm idea

¹Official terminology by V. Weger (2023)

ADAPTIVE DECODER APPROACH

Open Problem (Magic¹ Step)

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

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

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

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

¹Official terminology by V. Weger (2023)

ADAPTIVE DECODER APPROACH

Open Problem (Magic¹ Step)

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

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

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

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 $v_i \in W^\perp$

¹Official terminology by V. Weger (2023)

ADAPTIVE DECODER APPROACH

Open Problem (Magic¹ 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

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

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 $wt_R \leq t$.

¹Official terminology by V. Weger (2023)

ADAPTIVE DECODER APPROACH

Open Problem (Magic¹ 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

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

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.

¹Official terminology by V. Weger (2023)

Open Problem (Magic¹ 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

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

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 $U := \text{RowSpan}(\mathbf{x})$.

Go back to 1. but narrow down the search to only spaces W with $W \cap U$ non-trivial.

¹Official 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

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

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

ADAPTIVE DECODER APPROACH

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

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

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

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

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} .