Information Set Decoding

Violetta Weger

Encode Summer School 2025

July 2025

Organization

Lecture Notes

Slides

Exercises

Thursday

Short recap on codes

Motivation: code-based crypto

Set up the problem and assumptions

The first ISD: Prange

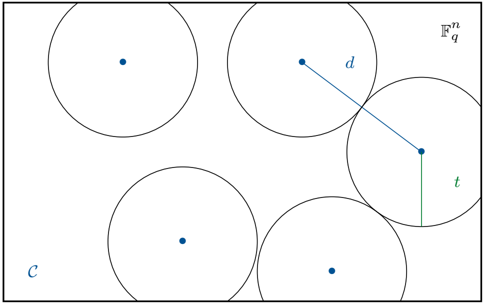
Friday

The usual solver: Stern

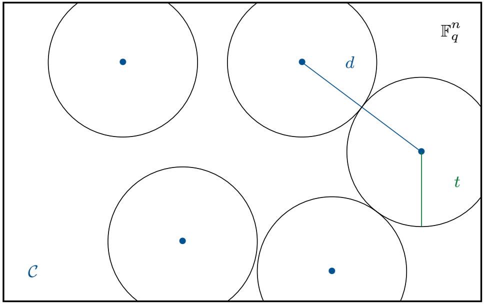
How to compare algorithms

More fancy algorithms

Open problems

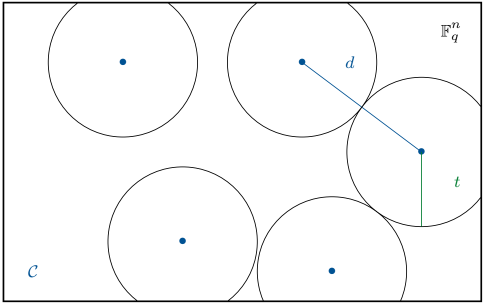


- Code $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear subspace
- Generator matrix $G \in \mathbb{F}_q^{k \times n}$ $\quad \mathcal{C} = \langle G \rangle$
- Codewords $c \in \mathcal{C}$ $\quad c = mG$
- Parity-check matrix $H \in \mathbb{F}_q^{n-k \times n}$ $\quad \mathcal{C} = \ker(H^\top)$
- Syndrome $s = xH^\top$
- Hamming weight $\mathrm{wt}(x) = |\{i \mid x_i \neq 0\}|$
- Minimum distance $d(\mathcal{C}) = \min\{\mathrm{wt}(c) \mid 0 \neq c \in \mathcal{C}\}$



- Code $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear subspace
- Generator matrix $G \in \mathbb{F}_q^{k \times n}$ $\quad \mathcal{C} = \langle G \rangle$
- Codewords $c \in \mathcal{C}$ $\quad c = mG$
- Parity-check matrix $H \in \mathbb{F}_q^{n-k \times n}$ $\quad \mathcal{C} = \ker(H^\top)$
- Syndrome $s = xH^\top$
- Hamming weight $\mathrm{wt}(x) = |\{i \mid x_i \neq 0\}|$
- Minimum distance $d(\mathcal{C}) = \min\{\mathrm{wt}(c) \mid 0 \neq c \in \mathcal{C}\}$

Information set: $I \subset \{1, \ldots, n\}$, $|I| = k = \dim(\mathcal{C})$ with $|\mathcal{C}_I| = |\mathcal{C}|$



- Code $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear subspace
- Generator matrix $G \in \mathbb{F}_q^{k \times n}$ $\quad \mathcal{C} = \langle G \rangle$
- Codewords $c \in \mathcal{C}$ $\quad c = mG$
- Parity-check matrix $H \in \mathbb{F}_q^{n-k \times n}$ $\quad \mathcal{C} = \ker(H^\top)$
- Syndrome $s = xH^\top$
- Hamming weight $\mathrm{wt}(x) = |\{i \mid x_i \neq 0\}|$
- Minimum distance $d(\mathcal{C}) = \min\{\mathrm{wt}(c) \mid 0 \neq c \in \mathcal{C}\}$

Information set: $I \subset \{1, \ldots, n\}$, $|I| = k = \dim(\mathcal{C})$ with $|\mathcal{C}_I| = |\mathcal{C}|$

Systematic form $\quad UGP = \begin{pmatrix} \mathrm{Id}_k & A \end{pmatrix} \quad UHP = \begin{pmatrix} -A^\top & \mathrm{Id}_{n-k} \end{pmatrix}$

ISD - The Problem

Decoding Problem

Given $G \in \mathbb{F}_q^{k \times n}$, $r \in \mathbb{F}_q^n$ and t
find $e \in \mathbb{F}_q^n$ with $\text{wt}(e) \leq t$ and $r - e \in \langle G \rangle$

ISD - The Problem

Decoding Problem Given $G \in \mathbb{F}_q^{k \times n}$, $r \in \mathbb{F}_q^n$ and t
find $e \in \mathbb{F}_q^n$ with $\mathrm{wt}(e) \leq t$ and $r - e \in \langle G \rangle$

algebraic structure → efficient decoders

ISD - The Problem

Decoding Problem

Given $G \in \mathbb{F}_q^{k \times n}$, $r \in \mathbb{F}_q^n$ and t

find $e \in \mathbb{F}_q^n$ with $\text{wt}(e) \leq t$ and $r - e \in \langle G \rangle$

algebraic structure → efficient decoders

if no (known) structure → generic decoders

ISD - The Problem

Decoding Problem

Given $G \in \mathbb{F}_q^{k \times n}$, $r \in \mathbb{F}_q^n$ and t

find $e \in \mathbb{F}_q^n$ with $\text{wt}(e) \leq t$ and $r - e \in \langle G \rangle$

algebraic structure → efficient decoders

if no (known) structure → generic decoders

best generic decoder = Information Set Decoding (ISD)

ISD - The Problem

♡

Decoding Problem Given $G \in \mathbb{F}_q^{k \times n}$, $r \in \mathbb{F}_q^n$ and t

find $e \in \mathbb{F}_q^n$ with $\mathrm{wt}(e) \leq t$ and $r - e \in \langle G \rangle$

The heart of code-based cryptography

algebraic structure → efficient decoders

if no (known) structure → generic decoders

best generic decoder = Information Set Decoding (ISD)

ISD - The Problem

Decoding Problem Given $G \in \mathbb{F}_q^{k \times n}$, $r \in \mathbb{F}_q^n$ and t
find $e \in \mathbb{F}_q^n$ with $\mathrm{wt}(e) \leq t$ and $r - e \in \langle G \rangle$

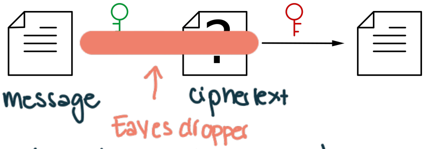
The heart of code-based cryptography → ISD is the attack on any code-based system

algebraic structure → efficient decoders

if no (known) structure → generic decoders

best generic decoder = Information Set Decoding (ISD)

Public-key encryption (PKE)



generates two keys
secret & public

computational security:
Security level 2^λ means best (known) attack has cost $\geq 2^\lambda$

McEliece System

Alice

Bob

ISD - McEliece System

Alice

Bob

Key generation

secret key: $G, \mathcal{D}$ efficient dec. up to t errors

$S \in \mathrm{GL}_q(k), P \in S_n$

public key: $G' = SGP, t$

McEliece System

Alice

Key generation

secret key: $G, \mathcal{D}$ efficient dec. up to t errors

$S \in \mathrm{GL}_q(k), P \in S_n$

public key: $G' = SGP, t$

Bob

Encryption

message $m \in \mathbb{F}_q^k$

random $e \in \mathbb{F}_q^n, \mathrm{wt}(e) \leq t$

ciphertext $c = mG' + e$

McEliece System

Alice

Bob

Key generation

secret key: $G, \mathcal{D}$ efficient dec. up to t errors

$S \in \mathrm{GL}_q(k), P \in S_n$

public key: $G' = SGP, t$

Encryption

message $m \in \mathbb{F}_q^k$

random $e \in \mathbb{F}_q^n, \mathrm{wt}(e) \leq t$

ciphertext $c = mG' + e$

Decryption

$$\mathcal{D}(cP^{-1})S^{-1} = \mathcal{D}(\underbrace{mS}_{m'}G + \underbrace{eP^{-1}}_{e'})S^{-1} = m'S^{-1} = m$$

$$\mathrm{wt}(e') = \mathrm{wt}(e) \leq t$$

Related Problems

Decoding Problem

Given $G \in \mathbb{F}_q^{k \times n}$, $r \in \mathbb{F}_q^n$ and t
find $e \in \mathbb{F}_q^n$ with $\text{wt}(e) \leq t$ and $r - e \in \langle G \rangle$

Decoding Problem

Given $G \in \mathbb{F}_q^{k \times n}$, $r \in \mathbb{F}_q^n$ and t

find $e \in \mathbb{F}_q^n$ with $\text{wt}(e) \leq t$ and $r - e \in \langle G \rangle$

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k) \times n}$, $s \in \mathbb{F}_q^{n-k}$ and t

find $e \in \mathbb{F}_q^n$ such that $\text{wt}(e) \leq t$ and $eH^\top = s$

Related Problems

Decoding Problem

Given $G \in \mathbb{F}_q^{k \times n}$, $r \in \mathbb{F}_q^n$ and t
find $e \in \mathbb{F}_q^n$ with $\mathrm{wt}(e) \leq t$ and $r - e \in \langle G \rangle$

$\Updownarrow$ Equivalent

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k) \times n}$, $s \in \mathbb{F}_q^{n-k}$ and t
find $e \in \mathbb{F}_q^n$ such that $\mathrm{wt}(e) \leq t$ and $eH^\top = s$

$\Updownarrow$ Equivalent

Codeword Finding Problem

Given $H \in \mathbb{F}_q^{(n-k) \times n}$ and t
find $c \in \mathbb{F}_q^n$ such that $\mathrm{wt}(c) \leq t$ and $cH^\top = 0$

DP: Given G, r, t find e with $\mathrm{wt}(e) \le t$ and $r = mG + e$

SDP: Given H, s, t find e with $\mathrm{wt}(e) \le t$ and $s = eH^\top$

1. DP → SDP : Given G compute systematic form $UGP = [Id_k | A]$

$\rightarrow HP = [-A^T \,|\, Id_{n-k}]$ get H

compute $rH^T = s$ → instance H, s, t

2. SDP → DP : Given H compute systematic form $UHP = [Id_{n-k} \,|\, A]$

$\rightarrow GP = [-A^T \,|\, Id_k]$ get G How to get r?

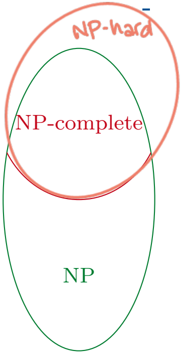
solution set $\mathcal{L}$ to $s = xH^T$ ⊛

There are n variables & $n-k$ equations → $|\mathcal{L}| = q^k = N$ many sol $x_1, \dots, x_N$

There are also q^k codewords $c_1, \dots, c_N \in \mathcal{L}$.

Every $c_i + e$ is a solution to ⊛ hence any sol $x_i = c_i + e$ can be used as r → instance G, r, t

ISD - Hardness



Polynomial time reduction $\mathcal{Q} \to \mathcal{P}$

- take random instance I of $\mathcal{Q}$
- transform to instance I' of $\mathcal{P}$
- assume find solution s' to I'
- transform to solution s of I

→ hardness($\mathcal{P}$) ≥ hardness($\mathcal{Q}$)

read: "If we can solve P, we can also solve Q"

Problem $\mathcal{P} \in NP$: when given a candidate solution x for an instance I of $\mathcal{P}$, can check in polynomial time if really a solution ← essential for cryptography

Problem $\mathcal{P} \in$ NP-hard: for every problem $\mathcal{Q} \in NP$, there exists a polynomial time reduction from $\mathcal{Q} \to \mathcal{P}$ ← hardest problems in math

NP-complete = NP-hard ∩ NP

to show $\mathcal{P} \in$ NP-hard: choose known NP-hard problem $\mathcal{Q}$ and give poly. time reduction $\mathcal{Q} \to \mathcal{P}$ since then any problem from NP can be reduced to $\mathcal{P}$

SDP is NP-hard

3-dim. Matching Problem Given T a finite set and $U \subseteq T \times T \times T$ find $W \subseteq U$ s.t. $|W| = |T|$ and no two elements of W agree in any coordinate

SDP: Given H, s, t find e with $\text{wt}(e) \leq t$ and $s = eH^\top$

3DM: Given U, T find W with $|W| = |T|$ and $w_i \neq w_i'$

Proof by example ☺ $T = \{A, B, C, D\}$ $|T| = t = 4$

$U = \{(DAB), (CBA), (DAB), (BCD), (CDA), (ADA), (ABC)\}$ → find 4 words in U such that each element of T appears in every pos. (*)

↑ possible solution

set up incidence matrix H

$$H^T = \begin{array}{r} \\ DAB \rightarrow \\ CBA \rightarrow \\ \\ \end{array} \left[\begin{array}{c|c|c} \overbrace{0001}^{1.\text{ pos}} & \overbrace{1000}^{2.\text{ pos}} & \overbrace{0100}^{3.\text{ pos}} \\ 0010 & 0100 & 1000 \\ \vdots & \vdots & \vdots \end{array}\right]$$

$\uparrow\uparrow\uparrow\uparrow$
A B C D

3 sections one for each pos
each section has 4 columns
one for each element in T

rows are the words in U
put a 1 at pos j in section i
if $u_i = t_j$

to select $t = 4$ words from U ⇔ $t = 4$ rows from H^T ⇔ multiply eH^T where $\text{wt}(e) = t$
if they satisfy (*) $eH^T = (1 \dots 1) = s$ → instance H, s, t and sol e reveals which words in W

ISD - Task

||

"Information Set Detectives"

NP-hard Case

SDP Given H, s, t find e with 1. $\text{wt}(e) \leq t$ 2. $eH^\top = s$

ISD - Task

NP-hard Case

SDP   Given H, s, t find e with 1. $\mathrm{wt}(e) \leq t$ 2. $eH^\top = s$

Task   find e

ISD - Task

NP-hard Case

SDP Given H, s, t find e with 1. $\mathrm{wt}(e) \leq t$ 2. $eH^\top = s$

Task find e

Crime scene parity-check matrix H

ISD - Task

NP-hard Case

SDP Given H, s, t find e with 1. $\mathrm{wt}(e) \leq t$ 2. $eH^\top = s$

Task	find e
Crime scene	parity-check matrix H
Clue 1	weight t

ISD - Task

NP-hard Case

SDP Given H, s, t find e with 1. $\text{wt}(e) \leq t$ 2. $eH^\top = s$

Task	find e
Crime scene	parity-check matrix H
Clue 1	weight t
Clue 2	syndrome s

ISD - What is a random code?

- $G = \begin{pmatrix} B & \mathrm{Id}_k \end{pmatrix} \quad H = \begin{pmatrix} \mathrm{Id}_{n-k} & B \end{pmatrix}$

ISD - What is a random code?

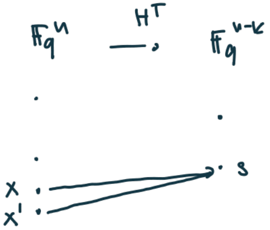
- $G = \begin{pmatrix} B & \mathrm{Id}_k \end{pmatrix} \quad H = \begin{pmatrix} \mathrm{Id}_{n-k} & B \end{pmatrix}$
- H random → $xH^\top = s$ random

What is a random code?

- $G = \begin{pmatrix} B & \mathrm{Id}_k \end{pmatrix} \quad H = \begin{pmatrix} \mathrm{Id}_{n-k} & B \end{pmatrix}$
- H random → $xH^\top = s$ random
- $\mathbb{P}(x \in \mathbb{F}_q^n : xH^\top = s)$

What is a random code?

- $G = \begin{pmatrix} B & \mathrm{Id}_k \end{pmatrix}$ $\quad H = \begin{pmatrix} \mathrm{Id}_{n-k} & B \end{pmatrix}$
- H random → $xH^\top = s$ random
- $\mathbb{P}(x \in \mathbb{F}_q^n : xH^\top = s) = q^{-(n-k)}$



clearly not injective. If $x \neq x' \in \mathbb{F}_q^n$ with $xH^T = x'H^T$ then $(x-x')H^T = 0 \rightarrow x - x' \in \mathcal{C}$

→ for every $s \in \mathbb{F}_q^{n-k}$ $\exists\, q^k = N$ many $x_1, \ldots, x_N \in \mathbb{F}_q^n$ such that $x_i H^T = s$

$$\mathbb{P}(x \in \mathbb{F}_q^n \mid xH^T = s) = \frac{|\{x \in \mathbb{F}_q^n : xH^T = s\}|}{|\{x \in \mathbb{F}_q^n\}|} = \frac{q^k}{q^n}$$

ISD - What is a random code?

- $G = \begin{pmatrix} B & \mathrm{Id}_k \end{pmatrix} \quad H = \begin{pmatrix} \mathrm{Id}_{n-k} & B \end{pmatrix}$
- H random → $xH^\top = s$ random
- $\mathbb{P}(x \in \mathbb{F}_q^n : xH^\top = s) = q^{-(n-k)}$

- for large n: $d(\mathcal{C}) =$

What is a random code?

- $G = (B \quad \mathrm{Id}_k) \qquad H = (\mathrm{Id}_{n-k} \quad B)$
- H random → $xH^\top = s$ random
- $\mathbb{P}(x \in \mathbb{F}_q^n : xH^\top = s) = q^{-(n-k)}$

- for large n: $d(\mathcal{C}) = \delta n$
- GV: $H_q(\delta) = 1 - R$

$H_q(x) = x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x)$

q-ary entropy function

$$V_H(\delta n, n, q) = |\{x \in \mathbb{F}_q^n \mid \mathrm{wtH}(x) \leq \delta n\}| = \sum_{i=0}^{\delta n} \binom{n}{i} (q-1)^i$$

$$\lim_{n \to \infty} 1/n \log_q(V_H(\delta n, n, q)) = H_q(\delta)$$

GV-bound: There ex. a (not necessarily linear) code $\mathcal{C} \subset \mathbb{F}_q^n$ with $d(\mathcal{C}) \geq d$ and

$$|\mathcal{C}| \geq \frac{q^n}{V_H(d-1, n, q)}$$

Asymptotic GV : $R \geq 1 - H_q(\delta)$

ISD - What is a random code?

- $G = \begin{pmatrix} B & \mathrm{Id}_k \end{pmatrix} \quad H = \begin{pmatrix} \mathrm{Id}_{n-k} & B \end{pmatrix}$
- H random → $xH^\top = s$ random
- $\mathbb{P}(x \in \mathbb{F}_q^n : xH^\top = s) = q^{-(n-k)}$

- for large n: $d(\mathcal{C}) = \delta n$
- GV: $H_q(\delta) = 1 - R$
- e unique → $\mathrm{wt}(e) \leq \frac{d-1}{2}$

Asymptotic GV $H_q(\delta) = 1 - R$

Thm: q prime power $\delta \in [0, 1-1/q)$, $\varepsilon > 0$, n pos. integer

$k \leq n(1 - H_q(\delta) - \varepsilon)$. $\mathcal{C} \subseteq \mathbb{F}_q^n$ random of dim k

$\hookrightarrow$ $R = k/n = 1 - H_q(\delta)$ on GV

Then w.h.p (for $n \to \infty$) $d(\mathcal{C}) \geq \delta n$.

Proof To show $\mathbb{P}(d(\mathcal{C}) \geq \delta n) \geq 1 - q^{-\varepsilon n} \xrightarrow[n \to \infty]{} 1$. Will show counterprob

$\mathbb{P}(d(\mathcal{C}) < \delta n) = 1 - \mathbb{P}(d(\mathcal{C}) \geq \delta n) \leq q^{-\varepsilon n}$ $\left(\xrightarrow[n \to \infty]{} 0\right)$

$d(\mathcal{C}) < \delta n$ means $\exists m \in \mathbb{F}_q^k \setminus \{0\}$ s.t. $\mathrm{wt}(mG) < \delta n$

(*) $\mathbb{P}(\mathrm{wt}(mG) < \delta n) = \dfrac{V_H(\delta n - 1, n, q)}{q^n - 1} \leq q^{n(H_q(\delta) - 1)}$

$$\mathbb{P}(d(\mathcal{C}) < \delta n) = \mathbb{P}(\exists\, m \in \mathbb{F}_q^k \setminus \{0\} : \mathrm{wt}(mG) < \delta n) \overset{\text{union bound}}{\leq} \sum_{m \in \mathbb{F}_q^k \setminus \{0\}} \mathbb{P}(\mathrm{wt}(mG) < \delta n) \overset{(*)}{\leq} \sum_{m \in \mathbb{F}_q^k \setminus \{0\}} q^{n(H_q(\delta) - 1)}$$

$$\leq (q^k - 1)\, q^{n(H_q(\delta) - 1)} \underset{\text{choice of } k}{=} q^{n(1 - H_q(\delta) - \varepsilon + H_q(\delta) - 1)} = q^{-\varepsilon n} \to 0$$

ISD - Break ☕

SDP Given H, s, t find e with 1. $\mathrm{wt}(e) \leq t$ 2. $eH^\top = s$

How would you solve the SDP?

ISD - Brute Force

SDP Given H, s, t find e with 1. $\mathrm{wt}(e) \leq t$ 2. $eH^\top = s$

Brute Force I

1. Find the solution set $\mathcal{L}$ for the linear system $xH^\top = s$.
2. For each $x \in \mathcal{L}$ check if $\mathrm{wt}(e) \leq t$

ISD - Brute Force

SDP Given H, s, t find e with 1. $\text{wt}(e) \leq t$ 2. $eH^\top = s$

Brute Force I

1. Find the solution set $\mathcal{L}$ for the linear system $xH^\top = s$.

2. For each $x \in \mathcal{L}$ check if $\text{wt}(e) \leq t$

→ cost in $\mathcal{O}(q^k)$

ISD - Brute Force

SDP Given H, s, t find e with 1. $\text{wt}(e) \leq t$ 2. $eH^\top = s$

Brute Force I

1. Find the solution set $\mathcal{L}$ for the linear system $xH^\top = s$.
2. For each $x \in \mathcal{L}$ check if $\text{wt}(e) \leq t$

→ cost in $\mathcal{O}(q^k)$

Exercise: Do Brute Force II: where you first solve for 1. $\text{wt}(x) \leq t$

What is the cost?

Idea ISD

use information sets!

systematic form $UHP = \begin{pmatrix} \mathrm{Id}_{n-k} & A \end{pmatrix}$ $I \subset \{1, \ldots, n\}, |I| = k$, I is information set

Idea ISD

use information sets!

systematic form $UHP = \begin{pmatrix} \mathrm{Id}_{n-k} & A \end{pmatrix}$ $\quad$ $I \subset \{1, \ldots, n\}, |I| = k$, I is information set

quasi-systematic form $UHP = \begin{pmatrix} \mathrm{Id}_{n-k-\ell} & A \\ 0 & B \end{pmatrix}$ $\quad$ $J \subset \{1, \ldots, n\}, |J| = k + \ell$, $J \supseteq I$ contains information set

Idea ISD

use information sets!

systematic form $UHP = \begin{pmatrix} \mathrm{Id}_{n-k} & A \end{pmatrix}$

$I \subset \{1, \dots, n\}, |I| = k$, I is information set

quasi-systematic form $UHP = \begin{pmatrix} \mathrm{Id}_{n-k-\ell} & A \\ 0 & B \end{pmatrix}$

$J \subset \{1, \dots, n\}, |J| = k + \ell$, $J \supseteq I$ contains information set

$eH^\top = s \rightarrow$ $$\underbrace{e}_{e'}P\underbrace{(P^\top H^\top U^\top)}_{H'^\top} = \underbrace{sU^\top}_{s'}$$

use information sets!

systematic form $UHP = \begin{pmatrix} \mathrm{Id}_{n-k} & A \end{pmatrix}$

$I \subset \{1, \dots, n\}, |I| = k$, I is information set

quasi-systematic form $UHP = \begin{pmatrix} \mathrm{Id}_{n-k-\ell} & A \\ 0 & B \end{pmatrix}$

$J \subset \{1, \dots, n\}, |J| = k + \ell$, $J \supseteq I$ contains information set

$eH^\top = s \rightarrow$

$$e' \quad \begin{array}{|c|c|}\hline e_{J^C} & e_J \\ \hline \end{array}$$

$$\cdot$$

$$H' \quad \begin{array}{|c|c|}\hline \mathrm{Id}_{n-k-\ell} & A \\ \hline 0 & B \\ \hline \end{array} = \begin{array}{|c|}\hline s_1 \\ \hline s_2 \\ \hline \end{array}$$

→ 1) $e_{J^C} + e_J A^\top = s_1$

2) $e_J B^\top = s_2$

⊛ Assume $\mathrm{wt}(e_J) = w < t$

→ smaller SDP instance

⊛ this does not need to happen!

ISD - Cost ISD

$$\text{cost of ISD} \quad = \quad (\text{cost of 1 iteration}) \cdot (\text{average number of iterations})$$

Cost ISD

$$\text{cost of ISD} \quad = \quad (\text{cost of 1 iteration}) \cdot (\text{average number of iterations})$$

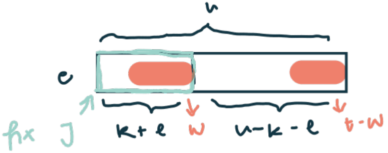
$$\text{average nr. of iterations} \quad = \quad \frac{1}{\mathbb{P}(\text{iteration is successful})}$$

$$\text{cost of ISD} = (\text{cost of 1 iteration}) \cdot (\text{average number of iterations})$$

$$\text{average nr. of iterations} = \frac{1}{\mathbb{P}(\text{iteration is successful})}$$

Fix $J \subset \{1, \ldots, n\}$ of size $k + \ell$. Compute

$$\frac{|\{e \in \mathbb{F}_q^n : \mathrm{wt}(e) = t, \mathrm{wt}(e_J) = w\}|}{|\{e \in \mathbb{F}_q^n : \mathrm{wt}(e) = t\}|}$$



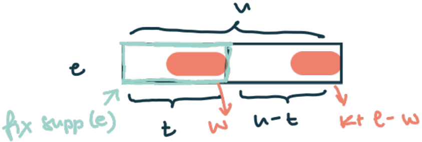
$$\frac{\binom{k+\ell}{w}\binom{n-k-\ell}{t-w}}{\binom{n}{t}}$$

same

=

Fix $e \in \mathbb{F}_q^n$ with $\mathrm{wt}(e) = t$. Compute

$$\frac{|\{J \subset \{1, \ldots, n\} : |J| = k + \ell, |J \cap \mathrm{supp}(e)| = w\}|}{|\{J \subset \{1, \ldots, n\} : |J| = k + \ell\}|}$$

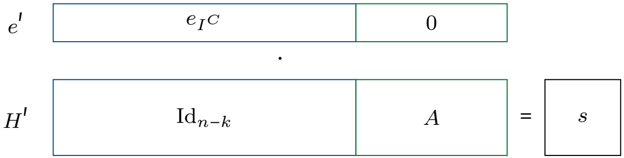


$$\frac{\binom{t}{w}\binom{n-t}{k+\ell-w}}{\binom{n}{k+\ell}}$$

Prange's ISD

Prange's ISD

Assumption $\mathrm{supp}(e) \cap I = \varnothing$



→ $e_{I^c} \cdot \mathrm{Id}_{n-k} + 0 \cdot A = s$

→ $e_{I^c} = s$

only need to check if $\mathrm{wt}(s) = t$

Cost in $\mathcal{O}\left(\binom{n}{t} \binom{n-k}{t}^{-1} \right)$

- each iteration consists of computing UHP, sU^T (polynomial in n)
- average number of iteration $= 1/\text{success prob.} = \binom{n}{t}\binom{n-k}{t}^{-1}$

ISD - Algorithm

Algorithm 1 Prange's Algorithm

```
Input: $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, $t \in \mathbb{N}$.
Output: $e \in \mathbb{F}_q^n$ with $eH^\top = s$ and $\mathrm{wt}(e) = t$.
1: Choose an information set $I \subset \{1, \dots, n\}$ of size $k$.
2: Compute $U \in \mathbb{F}_q^{(n-k)\times(n-k)}$, such that
       $$(UH)_I = A \text{ and } (UH)_{I^C} = \mathrm{Id}_{n-k},$$
   where $A \in \mathbb{F}_q^{(n-k)\times k}$.
3: Compute $s' = sU^\top$.
4: **if** $\mathrm{wt}(s') = t$ **then**
5:     Return $e$ such that $e_I = 0$ and $e_{I^C} = s'$.
6: Start over with Step 1 and a new selection of $I$.
```

ISD - Example

Over $\mathbb{F}_5$

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 2 & 3 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix}, \qquad s = (2,4,1), \qquad t = 1$$

Example

Over $\mathbb{F}_5$

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 2 & 3 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix}, \qquad s = (2,4,1), \qquad t = 1$$

If $I_1 = \{4,5\} \rightarrow U_1 = \mathrm{Id}_3$, but $\mathrm{wt}(s) \neq 1$

ISD - Example

Over $\mathbb{F}_5$

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 2 & 3 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix}, \qquad s = (2,4,1), \qquad t = 1$$

If $I_1 = \{4,5\} \to U_1 = \mathrm{Id}_3$, but $\mathrm{wt}(s) \neq 1$

$I_2 = \{1,2\} \to$

$$U_2 = \begin{pmatrix} 1 & 3 & 1 \\ 2 & 2 & 0 \\ 2 & 4 & 0 \end{pmatrix}, \quad \text{i.e.,} \quad U_2 H = \begin{pmatrix} 1 & 3 & 1 & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 \\ 2 & 4 & 0 & 0 & 1 \end{pmatrix}$$

$\to s' = sU_2^\top = (0,2,0)$

$$\to \quad e = (0,0,0,2,0).$$

Summary

- Decoding problem is equivalent to Syndrome Decoding Problem (SDP)
- To decode random linear code is hard!
- Assume code is random, distance on GV
- Information Set Decoding (ISD) use information sets
- Can reduce SDP instance to smaller instance
- Tomorrow: Smarter way to solve small instance

SDP Given H, s, t find e with 1. $\mathrm{wt}(e) \leq t$ 2. $eH^\top = s$

ISD - Recap yesterday

SDP Given H, s, t find e with 1. $\mathrm{wt}(e) \leq t$ 2. $eH^\top = s$

quasi-systematic form $UHP = \begin{pmatrix} \mathrm{Id}_{n-k-\ell} & A \\ 0 & B \end{pmatrix}$

$J \subset \{1, \ldots, n\}, |J| = k + \ell$, $J \supseteq I$ contains information set

$$eH^\top = s \rightarrow (eP)(P^\top H^\top U^\top) = sU^\top$$

ISD - Recap yesterday

SDP Given H, s, t find e with 1. $\mathrm{wt}(e) \leq t$ 2. $eH^\top = s$

quasi-systematic form $UHP = \begin{pmatrix} \mathrm{Id}_{n-k-\ell} & A \\ 0 & B \end{pmatrix}$

$J \subset \{1, \ldots, n\}, |J| = k + \ell$, $J \supseteq I$ contains information set

! Renaming !

$$eH^\top = s \to (eP)(P^\top H^\top U^\top) = sU^\top$$

1. perform reduction step:

$$e = \begin{array}{|c|c|} \hline \tilde{e} & e' \\ \hline \end{array} \cdot \quad H = \begin{array}{|c|c|} \hline \mathrm{Id}_{n-k-\ell} & \tilde{H} \\ \hline 0 & H' \\ \hline \end{array} = \begin{array}{|c|} \hline \tilde{s} \\ \hline s' \\ \hline \end{array}$$

$\longrightarrow$

1) $\tilde{e} + e'\tilde{H}^\top = \tilde{s}$

2) $e'H'^\top = s'$

Assume $\mathrm{wt}(e') = w$

smaller instance

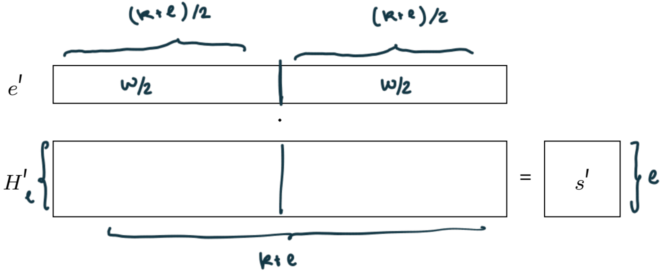
2. solve smaller instance

3. check if $\mathrm{wt}(\tilde{e}) = t - w$

Prange solves 2. by setting $e' = 0$

ISD - Stern's idea

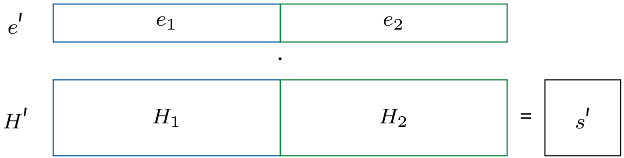
Smaller instance: given $H' \in \mathbb{F}_q^{\ell \times k+\ell}$, $s' \in \mathbb{F}_q^{\ell}$, find $e' \in \mathbb{F}_q^{k+\ell}$, of weight w and $s' = e'H^\top$



stern assumes wt of e' splits equally into two halves

ISD - Stern's idea

Smaller instance: given $H' \in \mathbb{F}_q^{\ell \times k+\ell}$, $s' \in \mathbb{F}_q^{\ell}$, find $e' \in \mathbb{F}_q^{k+\ell}$, of weight w and $s' = e'H^\top$



e' e_1 e_2

$\cdot$

H' H_1 H_2 $=$ s'

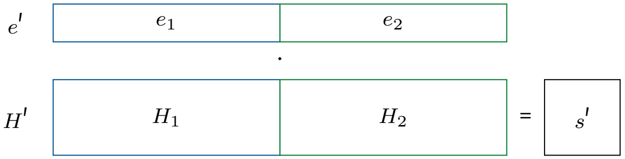
$e_i \in \mathbb{F}_q^{(k+\ell)/2}$ $\quad wt(e_i) = w/2$

$e_1 H_1^T + e_2 H_2^T = s'$

$\rightarrow e_1 H_1^T = s' - e_2 H_2^T$

ISD - Stern's idea

Smaller instance: given $H' \in \mathbb{F}_q^{\ell \times k+\ell}$, $s' \in \mathbb{F}_q^{\ell}$, find $e' \in \mathbb{F}_q^{k+\ell}$, of weight w and $s' = e'H^\top$



Build two lists

$\mathcal{L}_1 = \{($ [redacted] $, e_1) \mid e_1 \in \mathbb{F}_q^{(k+\ell)/2},$ [redacted] $\},$

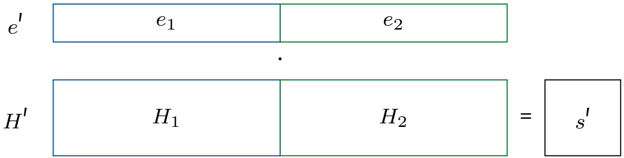
$\mathcal{L}_2 = \{($ [redacted] $, e_2) \mid e_2 \in \mathbb{F}_q^{(k+\ell)/2},$ [redacted]

$\}$ wt $(e_1\ e_2) = w$

if equal then $(e_1\ e_2) H'^{\,T} = s'$

ISD - Stern's idea

Smaller instance: given $H' \in \mathbb{F}_q^{\ell \times k+\ell}, s' \in \mathbb{F}_q^{\ell}$, find $e' \in \mathbb{F}_q^{k+\ell}$, of weight w and $s' = e'H^\top$



Build two lists

$$\mathcal{L}_1 = \{(e_1 H_1^\top, e_1) \mid e_1 \in \mathbb{F}_q^{(k+\ell)/2}, \mathrm{wt}(e_1) = w/2\},$$
$$\mathcal{L}_2 = \{(s' - e_2 H_2^\top, e_2) \mid e_2 \in \mathbb{F}_q^{(k+\ell)/2}, \mathrm{wt}(e_2) = w/2\}$$

Collision search: find $((a, e_1), (a, e_2)) \in \mathcal{L}_1 \times \mathcal{L}_2$ (without sorting / Hash tables)

ISD - Cost of Stern

Need to update success probability! Before $e = \big[\underbrace{\;w\;}_{k+\ell} \big| \underbrace{\;t-w\;}_{n-k-\ell}\big] \to \binom{k+\ell}{w}\binom{n-k-\ell}{t-w}\binom{n}{t}^{-1}$

Now $e = \big[\underbrace{\;w/2\;}_{(k+\ell)/2} \big| \underbrace{\;w/2\;}_{(k+\ell)/2} \big| \underbrace{\;t-w\;}_{n-k-\ell}\big] \to \binom{(k+\ell)/2}{w/2}^2\binom{n-k-\ell}{t-w}\binom{n}{t}^{-1}$

cost of one iteration:

1. Build lists : cost $=$ poly $\cdot |\mathcal{L}_i|$, $|\mathcal{L}_i| = L = \binom{(k+\ell)/2}{w/2}(q-1)^{w/2}$
2. Collision search: cost $=$ poly $\frac{|\mathcal{L}_1 \times \mathcal{L}_2|}{q^\ell}$ $=$ poly L^2/q^ℓ

   Probability to have collision →

→ cost Stern $O\left(\binom{n}{t}\binom{n-k-\ell}{t-w}^{-1}\binom{(k+\ell)/2}{w/2}^{-2}\left(L + L^2/q^\ell\right)\right)$ minimize for $0 \leq w \leq \min\{t, k+\ell\}$, $0 \leq \ell \leq n-k$

Algorithm 2 Stern's Algorithm

```
Input: $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, $w < t, \ell < n-k$.
Output: $e \in \mathbb{F}_q^n$ with $eH^\top = s$ and $\text{wt}(e) = t$.
1: Choose a set $J \subset \{1, \dots, n\}$ of size $k+\ell$.
2: Compute $U \in \mathbb{F}_q^{n-k \times n-k}$, s.t. $(UH)_J = \begin{pmatrix} \tilde{H} \\ H' \end{pmatrix}$, $(UH)_{J^C} = \begin{pmatrix} \text{Id}_{n-k-\ell} \\ 0 \end{pmatrix}$, $\tilde{H} \in \mathbb{F}_q^{n-k-\ell \times k+\ell}$, $H' \in \mathbb{F}_q^{\ell \times k+\ell}$.
3: Split $H' = (H_1, H_2)$, with $H_i \in \mathbb{F}_q^{\ell \times (k+\ell)/2}$.
4: Compute $sU^\top = \begin{pmatrix} \tilde{s} & s' \end{pmatrix}$, where $\tilde{s} \in \mathbb{F}_q^{n-k-\ell}$ and $s' \in \mathbb{F}_q^{\ell}$.
5: Compute the sets
       $\mathcal{L}_1 = \{(e_1 H_1^\top, e_1) \mid e_1 \in \mathbb{F}_q^{(k+\ell)/2}, \text{wt}(e_1) = w/2\}$,
       $\mathcal{L}_2 = \{(s' - e_2 H_2^\top, e_2) \mid e_2 \in \mathbb{F}_q^{(k+\ell)/2}, \text{wt}(e_2) = w/2\}$.
6: for $((a, e_1), (a, e_2)) \in \mathcal{L}_1 \times \mathcal{L}_2$ do
7:     if $\text{wt}(\tilde{s} - (e_1, e_2)\tilde{H}^\top) = t - w$ then
8:         Return $e$ such that $e_J = (e_1, e_2)$, $e_{J^C} = \tilde{s} - (e_1, e_2)\tilde{H}^\top$.
9: Start over with Step 1 and a new selection of $J$.
```

How to compare costs?

Asymptotic cost: write cost as $q^{n(e(R,T,q)+o(1))}$

$$R = \lim_{n \to \infty} \frac{k(n)}{n} \qquad T = \lim_{n \to \infty} \frac{t(n)}{n}$$

How to compare costs?

Asymptotic cost: write cost as $q^{n(e(R,T,q)+o(1))}$

Compute $e(R,T,q) = \lim_{n\to\infty} \frac{1}{n} \log_q(\text{cost})$

How to compare costs?

Asymptotic cost: write cost as $q^{n(e(R,T,q)+o(1))}$

Compute $e(R,T,q) = \lim_{n\to\infty} \frac{1}{n} \log_q(\text{cost})$

Recall cost Prange

$$\binom{n}{t}\binom{n-k}{t}^{-1}$$

ISD - How to compare costs?

Asymptotic cost: write cost as $q^{n(e(R,T,q)+o(1))}$

Compute $e(R,T,q) = \lim_{n\to\infty} \frac{1}{n} \log_q(\text{cost})$

Recall cost Prange

$$\binom{n}{t}\binom{n-k}{t}^{-1}$$

Sterling $\lim_{n\to\infty} \frac{1}{n} \log_q \left(\binom{a(n)}{b(n)}\right) =$

How to compare costs?

Asymptotic cost: write cost as $q^{n(e(R,T,q)+o(1))}$

Compute $e(R,T,q) = \lim_{n\to\infty} \frac{1}{n} \log_q(\text{cost})$

Recall cost Prange

$$\binom{n}{t}\binom{n-k}{t}^{-1}$$

$\lim 1/n \log_q(V_H(d)) = H_q(\delta)$

Sterling $\lim_{n\to\infty} \frac{1}{n} \log_q\left(\binom{a(n)}{b(n)}\right) = A\log_q(A) - B\log_q(B) - (A-B)\log_q(A-B)$

where $A = \lim_{n\to\infty} a(n)/n, B = \lim_{n\to\infty} b(n)/n$

ISD - How to compare costs?

Asymptotic cost: write cost as $q^{n(e(R,T,q)+o(1))}$

Compute $e(R,T,q) = \lim_{n\to\infty} \frac{1}{n}\log_q(\text{cost})$

Recall cost Prange

$$\binom{n}{t}\binom{n-k}{t}^{-1}$$

Sterling $\lim_{n\to\infty} \frac{1}{n}\log_q\left(\binom{a(n)}{b(n)}\right) = A\log_q(A) - B\log_q(B) - (A-B)\log_q(A-B)$

where $A = \lim_{n\to\infty} a(n)/n$, $B = \lim_{n\to\infty} b(n)/n$

Asymptotic cost of Prange:

$$e(R,T,q) = -((1-R)\log_q(1-R) - T\cancel{\log_q}(T) - (1-R-T)\log_q(1-R-T))$$
$$+ (\underbrace{1\cdot\log_q(1)}_{0} - T\cancel{\log_q}(T) - (1-T)\log_q(1-T)]$$

$$= -(1-T)\log_q(1-T) - (1-R)\log_q(1-R) - (1-R-T)\log_q(1-R-T)$$

Exercise

$$= H_q(T) - (1-R)\,H_q\left(\frac{T}{1-R}\right)$$

Asymptotic Cost Stern

Recall cost of Stern:

$$\underbrace{\binom{(k+\ell)/2}{w/2}}_{\to A}^{-2}\underbrace{\binom{n-k-\ell}{t-w}}_{\to B}^{-1}\underbrace{\binom{n}{t}}_{\to C}\left(\binom{(k+\ell)/2}{w/2}(q-1)^{w/2}+\binom{(k+\ell)/2}{w/2}^{2}(q-1)^{w-\ell}\right)$$

Asymptotic cost of Stern:

$$A = \lim_{n\to\infty} 1/n \log_q \binom{(k+\ell)/2}{w/2} = \left(\frac{R+L}{2}\right)\log_q\left(\frac{R+L}{2}\right) - \frac{W}{2}\log_q\left(\frac{W}{2}\right) - \left(\frac{R+L-W}{2}\right)\log_q\left(\frac{R+L-W}{2}\right)$$

$$B = \lim_{n\to\infty} 1/n \log_q \binom{n-k-\ell}{t-w} = (1-R-L)\log_q(1-R-L) - (T-W)\log_q(T-W) - (1-R-L-T+W)\log_q(1-R-L-T+W)$$

$$C = \lim_{n\to\infty} 1/n \log_q \binom{n}{t} = -T\log_q(T) - (1-T)\log_q(1-T)$$

$$\to \quad e(q,R,T) = \min_{W,L}\left\{-2A - B + C + \max\left\{A + \frac{W}{2}\log_q(q-1),\ 2A + (W-L)\log_q(q-1)\right\}\right\}$$

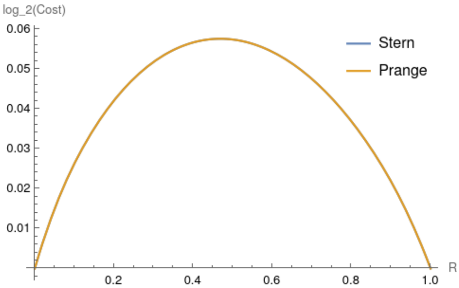
$$\text{where } L < 1-R-T+W,\ W < \min\{T, R+L\}$$

ISD - Prange vs. Stern

set $q=2$ $T = H_q^{-1}(1-R)/2$ → only have parameter R

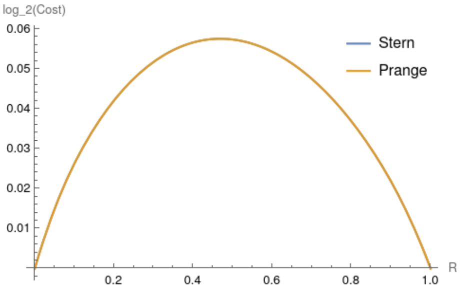
→ can plot $e(R)$

Prange vs. Stern



(probably my bad programming skills)

Prange vs. Stern

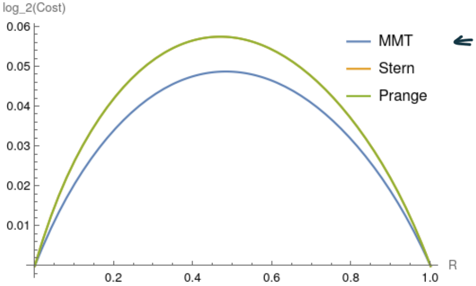


$$e^*(q) = \max\{e(R,q) \mid R \in [0,1]\}.$$

We then get for $q = 2$ that

Algorithm	$e^*(q)$
Prange	0.05747
Stern	0.05563

Prange vs. Stern vs. more fancy



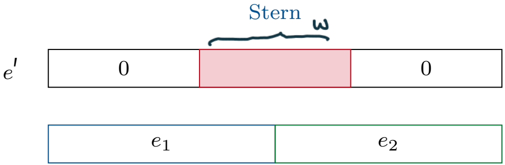
← special case of BJMM with $\varepsilon = 0$

$$e^*(q) = \max\{e(R,q) \mid R \in [0,1]\}.$$

We then get for $q = 2$ that

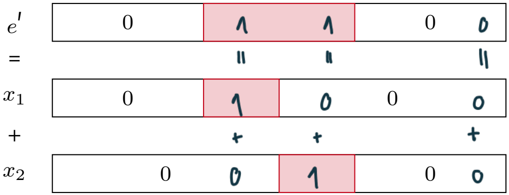
Algorithm	$e^*(q)$	year
Prange	0.05747	62
Stern	0.05563	88
MMT	0.05363	11

ISD - More fancy (binary)



More fancy (binary)

Stern



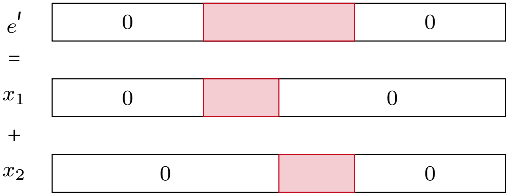
$e_i = 1 \rightarrow x_{1,i} = 1, x_{2,i} = 0$ or $x_{1,i} = 0, x_{2,i} = 1$

$e_i = 0 \rightarrow x_{1,i} = 0, x_{2,i} = 0$

$\rightarrow \mathrm{wt}(x_i) = w/2$

ISD - More fancy (binary)

Stern

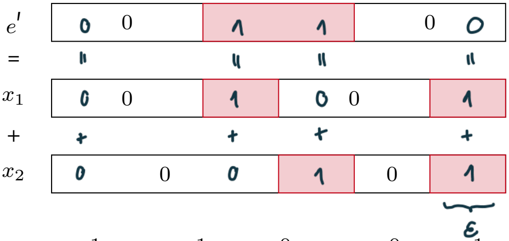


$e_i = 1 \to x_{1,i} = 1, x_{2,i} = 0$ or $x_{1,i} = 0, x_{2,i} = 1$

$e_i = 0 \to x_{1,i} = 0, x_{2,i} = 0$

$\to \mathrm{wt}(x_i) = w/2$

BJMM



$e_i = 1 \to x_{1,i} = 1, x_{2,i} = 0$ or $x_{1,i} = 0, x_{2,i} = 1$

$e_i = 0 \to x_{1,i} = 0, x_{2,i} = 0$ or $x_{1,i} = 1, x_{2,i} = 1$

$\to \mathrm{wt}(x_i) = w/2 + \varepsilon$

Representations

Let $e' \in \mathbb{F}_2^{k+\ell}$ of weight w

Representation A pair (x_1, x_2) of weight $w/2 + \varepsilon$ such that $x_1 + x_2 = e'$

Example $e' = (1, 0, 1, 0, 1, 1)$ with $w = 4$. For $\varepsilon = 1$ we have

$$(1, 0, 1, 1, 0, 0) + (0, 0, 0, 1, 1, 1)$$

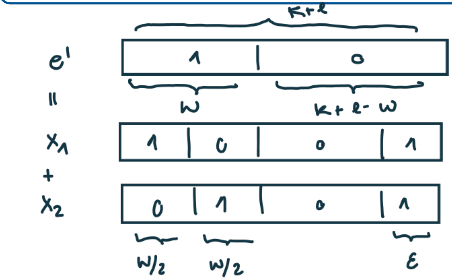
Exercise Find all representations of e'

Exercise How many representations are there in general?

ISD - Nr. of Representations

Let $e' \in \mathbb{F}_2^{k+\ell}$ of weight w

Number of representations of weight $w/2+\varepsilon$ is $\quad R(\varepsilon, w, \ell) = \binom{w}{w/2}\binom{k+\ell-w}{\varepsilon}$



$$\binom{w}{w/2} \cdot \binom{k+\ell-w}{\varepsilon}$$

ISD - How to use this?

1. Attempt construct $\mathcal{L} = \{x \in \mathbb{F}_q^{k+\ell} \mid \mathrm{wt}(x) = w/2 + \varepsilon\}$

Merge $\mathcal{L} \times \mathcal{L} \to \mathcal{L}' = \{e' \in \mathbb{F}_q^{k+\ell} \mid \mathrm{wt}(e') = w, x_1 + x_2 = e', x_1 H'^{\top} + x_2 H'^{\top} = s'\}$

→ cost $|\mathcal{L}|^2 q^{-\ell}$

ISD - How to use this?

1. Attempt construct $\mathcal{L} = \{x \in \mathbb{F}_q^{k+\ell} \mid \mathrm{wt}(x) = w/2 + \varepsilon\}$

Merge $\mathcal{L} \times \mathcal{L} \to \mathcal{L}' = \{e' \in \mathbb{F}_q^{k+\ell} \mid \mathrm{wt}(e') = w, x_1 + x_2 = e', x_1 H'^\top + x_2 H'^\top = s'\}$

→ cost $|\mathcal{L}|^2 q^{-\ell}$

→ optimizes at $\varepsilon = 0$ → Stern!

ISD - How to use this?

1. Attempt construct $\mathcal{L} = \{x \in \mathbb{F}_q^{k+\ell} \mid \mathrm{wt}(x) = w/2 + \varepsilon\}$

Merge $\mathcal{L} \times \mathcal{L} \to \mathcal{L}' = \{e' \in \mathbb{F}_q^{k+\ell} \mid \mathrm{wt}(e') = w, x_1 + x_2 = e', x_1 H'^\top + x_2 H'^\top = s'\}$

→ cost $|\mathcal{L}|^2 q^{-\ell}$

→ optimizes at $\varepsilon = 0$ → Stern!

would store several times same e' → no need to construct the whole $\mathcal{L}$!

To construct (some) $x \in \mathcal{L}$ use Stern!

$$x = (y_1, y_2), \qquad \mathrm{wt}(y_i) = w/4 + \varepsilon/2$$

Base lists: $\mathcal{B} = \{y \in \mathbb{F}_q^{(k+\ell)/2} \mid \mathrm{wt}(y) = w/4 + \varepsilon/2\}$

Subroutine: Stern

To construct (some) $x \in \mathcal{L}$ use Stern!

$$x = (y_1, y_2), \qquad \mathrm{wt}(y_i) = w/4 + \varepsilon/2$$

Base lists: $\mathcal{B} = \{y \in \mathbb{F}_q^{(k+\ell)/2} \mid \mathrm{wt}(y) = w/4 + \varepsilon/2\}$

Problem: If we merge $x_1 = (y_1, y_2)$ and $x_2 = (y_1', y_2')$ How to ensure $x_1 H'^{\top} + x_2 H'^{\top} = s'$?

ISD - Subroutine: Stern

To construct (some) $x \in \mathcal{L}$ use Stern!

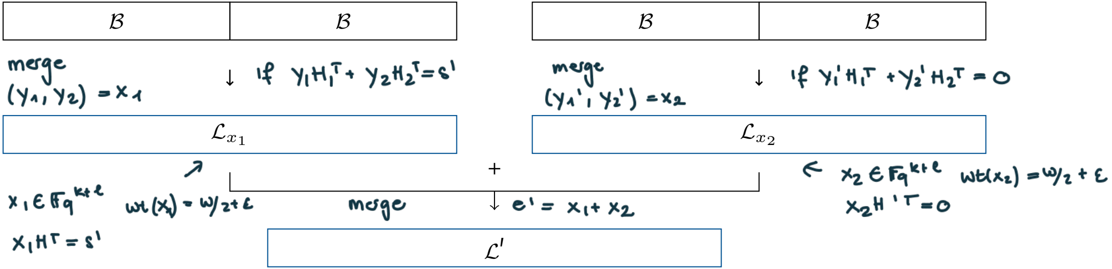
$$x = (y_1, y_2), \qquad \mathrm{wt}(y_i) = w/4 + \varepsilon/2$$

Base lists: $\mathcal{B} = \{y \in \mathbb{F}_q^{(k+\ell)/2} \mid \mathrm{wt}(y) = w/4 + \varepsilon/2\}$

Problem: If we merge $x_1 = (y_1, y_2)$ and $x_2 = (y_1', y_2')$ How to ensure $x_1 H'^\top + x_2 H'^\top = s'$?

Solution: Set $x_1 H'^\top = t_1 = s'$, $x_2 H'^\top = t_2 = 0$ and build two lists $\mathcal{L}_{x_1}, \mathcal{L}_{x_2}$

$\mathcal{B} = \{ y \in \mathbb{F}_q^{(k+\ell)/2} \mid \mathrm{wt}(y) = w/4 + \varepsilon/2 \}$



$\mathcal{B}$ | $\mathcal{B}$ | $\mathcal{B}$ | $\mathcal{B}$

merge $(y_1, y_2) = x_1$ ↓ if $y_1 H_1^T + y_2 H_2^T = s'$

merge $(y_1', y_2') = x_2$ ↓ if $y_1' H_1^T + y_2' H_2^T = 0$

$\mathcal{L}_{x_1}$ $\mathcal{L}_{x_2}$

$x_1 \in \mathbb{F}_q^{k+\ell}$ $\mathrm{wt}(x_1) = w/2 + \varepsilon$

$x_1 H^T = s'$

$x_2 \in \mathbb{F}_q^{k+\ell}$ $\mathrm{wt}(x_2) = w/2 + \varepsilon$

$x_2 H'^T = 0$

+

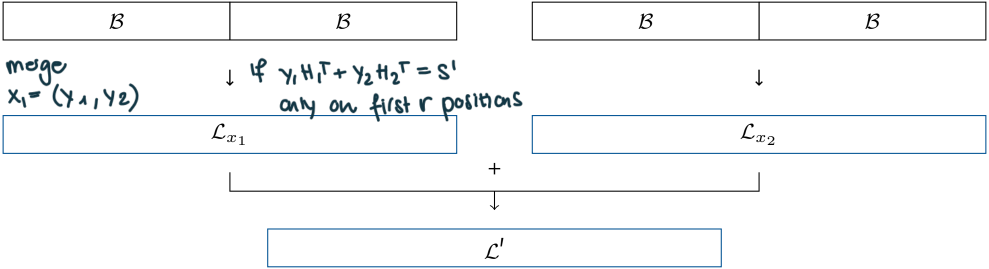
merge ↓ $e' = x_1 + x_2$

$\mathcal{L}'$

Usually: $|\mathcal{L}_{x_i}| = |\mathcal{B}|^2 q^{-\ell}$

don't need R many of the same $e' \in \mathcal{L}'$

ISD - Subroutine: Stern



$\mathcal{B}$ $\mathcal{B}$ $\mathcal{B}$ $\mathcal{B}$

merge
$x_1 = (y_1, y_2)$

if $y_1 H_1^T + y_2 H_2^T = s'$
only on first r positions

$\mathcal{L}_{x_1}$ $\mathcal{L}_{x_2}$

+

$\mathcal{L}'$

Usually: $|\mathcal{L}_{x_i}| = |\mathcal{B}|^2 q^{-\ell}$ $|\mathcal{L}_{x_i}| = |\mathcal{B}|^2 q^{-r} = |\mathcal{B}|^2 / R$

let $r = \log_q (R(\varepsilon, w, e))$

↳ ensures at least one
$e' \in \mathcal{L}'$ for each of the R

BJMM Summary

1. Choose $J \subset \{1, \dots, n\}$ of size $k + \ell$
2. Find $U \in \mathbb{F}_q^{(n-k)\times(n-k)}$, P, such that
$$UHP = \begin{pmatrix} \mathrm{Id}_{n-k-\ell} & \tilde{H} \\ 0 & H' \end{pmatrix}$$
3. Compute $sU^\top$ and split it into $\tilde{s}, s'$ split $H' = (H_1, H_2)$
4. Build the base list
$$\mathcal{B} = \{y \in \mathbb{F}_q^{(k+\ell)/2} \mathrm{wt}_H(y) = w/4 + \varepsilon/2\}$$
5. Merge $\mathcal{L}_{x_1} = \mathcal{B} \times \mathcal{B}$ on the target s' for r many positions
6. Merge $\mathcal{L}_{x_2} = \mathcal{B} \times \mathcal{B}$ on the target 0 for r many positions
7. Merge $\mathcal{L}' = \mathcal{L}_{x_1} \times \mathcal{L}_{x_2}$
8. For all $e_J \in \mathcal{L}'$: check if $\mathrm{wt}_H(e_{J^C}) = \mathrm{wt}_H(\tilde{s} - e_J\tilde{H}^\top) = t - w$
9. If yes: output $e = (e_J, e_{J^C})$, if no; start over with a new choice of J

actually not BJMM
as we only do 2 levels
BJMM suggests 3 levels

ISD - Summary

SDP Given H, s, t find e with 1. $\text{wt}(e) \leq t$ 2. $eH^\top = s$

- To decode random linear code is hard!
- Information Set Decoding (ISD) use information sets
- Can reduce SDP instance to smaller instance
- Prange: $e_J = 0$
- Stern: $e_J = (e_1, e_2)$
- BJMM: $e_J = x_1 + x_2$

ISD - Conclusion

After 60 years of ISD

	1962	1988	2011	2012	2015
	Prange	Stern	MMT	BJMM	MO
$e^*(R)$	0.057	0.055	0.053	0.049	0.047

Drop of asymptotic cost e^* only from 0.057 to 0.047

.. Still many open questions:

1. How to decode a (quasi-)cyclic code?
2. How to decode a q-ary code (faster)?
3. How to decode for large weights?
4. How to decode using quantum algorithms?
5. How to decode a regular error?
6. How to decode a restricted error?

ISD - Open Questions