Decoding Random Linear Codes in $\tilde{O}(2^{0.054n})$

Alexander May, Alexander Meurer, & Enrico Thomae

Parameters:

- n: block-length
- k: code dimension
- $r = n-k$: redundancy
- w: target weight
- ℓ: parameter – dimension of vector subset sum problem
- p: target weight of subset sum problem

First, we put the matrix $H \in \mathbb{F}_2^{(n-k)\times n}$ in the following form.

- Sample unif. rand. permutation mtx U_P.
- Perform row-reduction so that, if U_G denotes the appropriate change of basis

$$\begin{array}{c} \\ n-k \end{array}\left\{\begin{array}{c} \overbrace{\hphantom{I_{n-k-\ell}}\quad\hphantom{H_1}}^{n} \\ \left[\begin{array}{c|c} I_{n-k-\ell} & H_1 \\ \hline \underbrace{0_{\ell\times(n-k-\ell)}}_{n-k-\ell} & \underbrace{H_2}_{k+\ell} \end{array}\right] \end{array}\right. \begin{array}{l} \}\, n-k-\ell \\ \}\, \ell \end{array} = U_G H U_P .$$

Takeaway: we are reduced to solving the following problem:

Submatrix Matching Problem / Vector Subset Sum

Parameters: $\ell, k, p \leq k+\ell$

Input: $Q = [q_1 \cdots q_{k+\ell}] \in_R \mathbb{F}_2^{\ell \times (k+\ell)}$

Target vector $s \in \mathbb{F}_2^{\ell}$

Output: $I \subseteq [k+\ell]$, $|I| \leq p$ s.t.

$$\sum_{i \in I} q_i = s$$

MMT's proposed solution to this problem is algorithm COLUMN MATCH.

Outline & Intuition

- Spse I is solution.

1. Choose $I_1 \cup I_2 = I$, where both $I_1, I_2 \subseteq [k+\ell]$

Gives $\binom{p}{p/2} \approx 2^p$ representations for I. Hope:

$$\sum_{i \in I_1} q_i = \sum_{i \in I_2} q_i + s \in \mathbb{F}_2^{\ell}.$$

<u>N.B.</u> in Finiasz-Sendrier [FS'09] algorithm, I_1 and I_2 we required to come from disjoint sets, e.g.,

$I_1 \subseteq [1, \frac{k+\ell}{2}]$, $I_2 \subseteq [\frac{k+\ell}{2}+1, k+\ell]$. MMT will actually require $|I_1 \cap [1, \frac{k+\ell}{2}]| = \frac{p}{4}$, $|I_1 \cap [\frac{k+\ell}{2}+1, k+\ell]| = \frac{p}{4}$, and similarly for I_2. Still $\binom{p/2}{p/4}^2 \approx 2^{p(1-o(1))}$ choices.

2. Choose partition $L_1 \cup L_2 = [\ell]$, $|L_i| = \ell_i$.

"shortening parameters"; tuneable.

Construct lists:

$$\mathcal{L}_1 := \left\{ (I_1, \pi_{L_1}(Q_{I_1})) : \pi_{L_2}(Q_{I_1}) = 0 \in \mathbb{F}_2^{\ell_2} \right\}$$

$I_1 \subset [k+\ell]$, $|I_1| = \frac{p}{2}$ w/ fine print.

$$\mathcal{L}_2 := \left\{ (I_2, \pi_{L_1}(Q_{I_2}) + s_{L_1}) : \pi_{L_2}(Q_{I_2}) = s_{L_2} \in \mathbb{F}_2^{\ell_2} \right\}.$$

$I_2 \subset [k+\ell]$, $|I_2| = \frac{p}{2}$ w/ fine print.

In the above:

$s_L \in \mathbb{F}_2^{|L|}$ = "s restricted to coords in L"

$Q_I \in \mathbb{F}_2^{\ell \times |I|}$ = "Q restricted to columns in I"

$\pi_L(Q_I) = \sum_{i \in I} (q_i)_L \in \mathbb{F}_2^{|L|}$ = "sum of columns in Q_I restricted to coords in L"

<u>N.B.</u> Of the $\approx 2^p$ expressions

$$\sum_{i \in I_1} q_i = \sum_{i \in I_2} q_i + s \in \mathbb{F}_2^{\ell},$$

we restrict search to those where

$$\left(\sum_{i \in I_1} q_i \right)_{L_2} = 0 \in \mathbb{F}_2^{\ell_2}.$$

So, $\approx 2^{p-\ell_2}$ solutions survive.

3. Sort $\mathcal{L}_2$ according to labels $\pi_{L_1}(Q_{I_2}) + s_{L_1}$. Search amongst labels $\pi_{L_1}(Q_{I_1})$ in $\mathcal{L}_1$ for match.

<u>N.B.</u> Even if $J = I_1 \cap I_2 \neq \emptyset$, $\sum_{i \in I_1} q_i + \sum_{i \in I_2} q_i$ is

still 0 (double-counted vectors cancel) & we have solution $I' = I_1 \cup I_2 \setminus J$.

How to construct $\mathcal{L}_1, \mathcal{L}_2$?

<u>Answer</u>: "classical sort-and-match".

<u>For $\mathcal{L}_1$</u> ($\mathcal{L}_2$ analogous): Construct 2 lists:

$$\mathcal{L}_{1,1} := \left\{ \left(I_{1,1}, \pi_{L_2}(Q_{I_{1,1}}) \right) : I_{1,1} \subset \left[1, \tfrac{k+\ell}{2}\right], \; |I_{1,1}| = \tfrac{p}{4} \right\}$$

$$\mathcal{L}_{1,2} := \left\{ \left(I_{1,2}, \pi_{L_2}(Q_{I_{1,2}}) \right) : I_{1,2} \subset \left[\tfrac{k+\ell}{2}+1, k+\ell\right], \; |I_{1,2}| = \tfrac{p}{4} \right\}$$

Then, sort $\mathcal{L}_{1,2}$ w.r.t. second component; search for matches in $\mathcal{L}_{1,1}$. Merge matches into $\mathcal{L}_1$, i.e., $\mathcal{L}_1 \leftarrow \mathcal{L}_1 \cup \left\{ \left(I_{1,1} \cup I_{1,2}, \pi_{L_1}(Q_{I_{1,1} \cup I_{1,2}}) \right) \right\}$.

<u>Here's some pseudocode:</u>

Algorithm: ColumnMatch

Input: $Q \in \mathbb{F}_2^{\ell \times (k+\ell)}$, $s \in \mathbb{F}_2^{\ell}$, $p \leq k+\ell$.

Output: list $\mathcal{L}$ of all $I \subset [k+\ell]$ w/ $\pi(Q_I) = s$.

Params. h_1, h_2 w/ $[\ell] = h_1 \cup h_2$ & $|h_i| = \ell_i$, $i = 1,2$.

1. Construct $\mathcal{L}_{1,1}, \mathcal{L}_{1,2}, \mathcal{L}_{2,1}, \mathcal{L}_{2,2}$.
2. Sort $\mathcal{L}_{1,2}$ according to label $\pi_{h_2}(Q_{I_{1,2}})$.
   Sort $\mathcal{L}_{2,2}$ according to label $\pi_{h_2}(Q_{I_{2,2}}) + s_{h_2}$.
3. Join $\mathcal{L}_{1,1}$ & $\mathcal{L}_{1,2}$ to $\mathcal{L}_1$. That is:

   for all $(I_{1,1}, \pi_{h_2}(Q_{I_{1,1}})) \in \mathcal{L}_{1,1}$ do:

   for all $(I_{1,2}, \pi_{h_2}(Q_{I_{1,2}})) \in \mathcal{L}_{1,2}$ w/

   $\pi_{h_2}(Q_{I_{1,1}}) = \pi_{h_2}(Q_{I_{1,2}})$ do:

   - $I_1 := I_{1,1} \cup I_{1,2}$
   - $\mathcal{L}_1.\text{insert}(I_1, \pi_{h_1}(Q_{I_1}))$.
4. Join $\mathcal{L}_{2,1}$ & $\mathcal{L}_{2,2}$ to $\mathcal{L}_2$. That is:

   for all $(I_{2,1}, \pi_{h_2}(Q_{I_{2,1}})) \in \mathcal{L}_{2,1}$ do:

   for all $(I_{2,2}, \pi_{h_2}(Q_{I_{2,2}}) + s_{h_1}) \in \mathcal{L}_{1,2}$ w/

$\pi_{h_2}(Q_{I_{2,1}}) = \pi_{h_2}(Q_{I_{2,2}}) + s_{h_1}$ do:

- $I_2 := I_{2,1} \uplus I_{2,2}$
- $\mathcal{L}_2.\text{insert}(I_2, \pi_{h_1}(Q_{I_2}) + s_{h_1})$.

5. Sort $\mathcal{L}_2$ according to label $\pi_{h_1}(Q_{I_2}) + s_{h_1}$.

6. Join $\mathcal{L}_1$ & $\mathcal{L}_2$ to $\mathcal{L}$. That is:

for all $(I_1, \pi_{h_1}(Q_{I_1})) \in \mathcal{L}_1$ do:

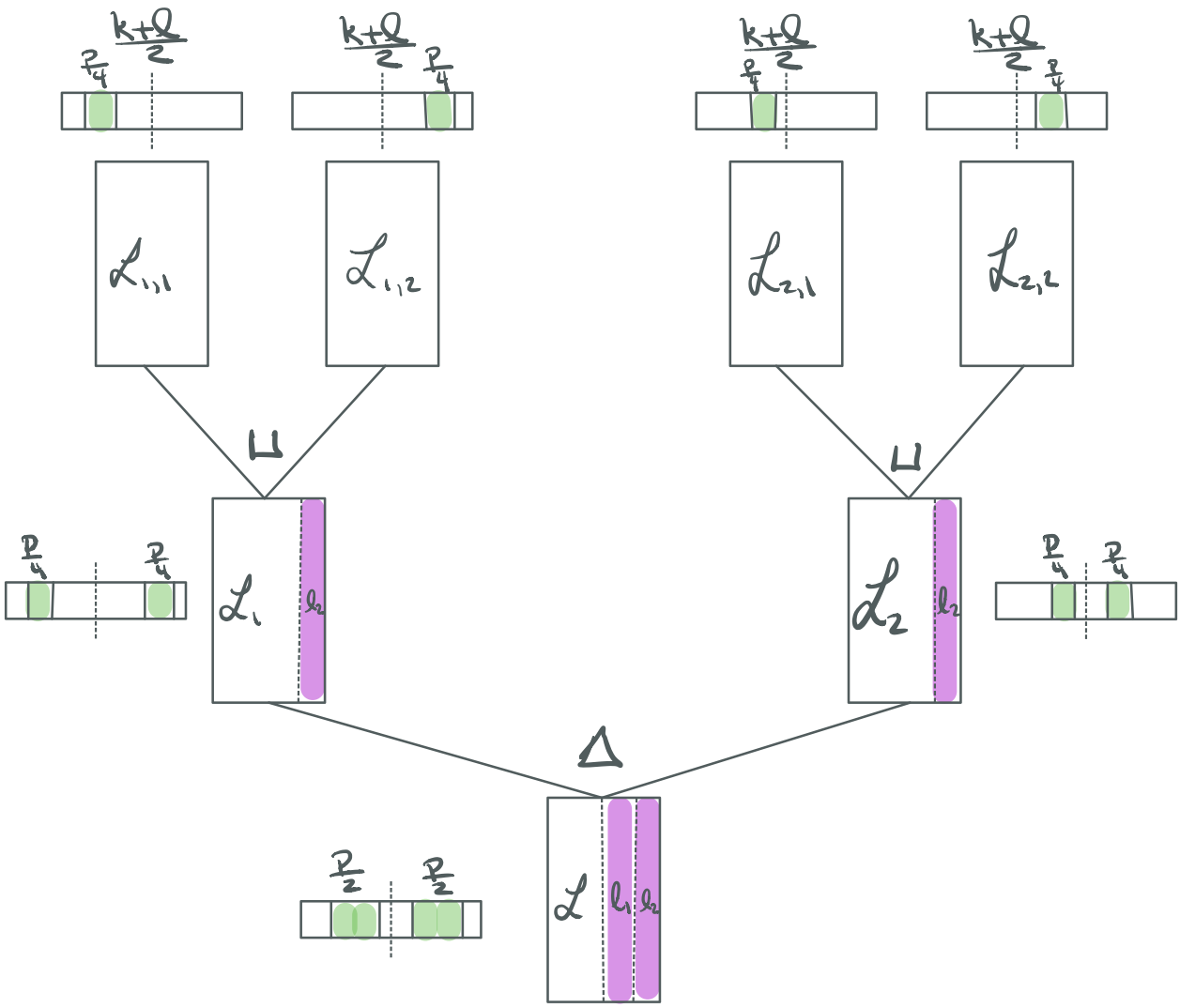
for all $(I_2, \pi_{h_1}(Q_{I_2}) + s_{h_1}) \in \mathcal{L}_2$ w/

$\pi_{h_1}(Q_{I_1}) = \pi_{h_1}(Q_{I_2}) + s_{h_1}$ do:

- $I := I_1 \Delta I_2 = I_1 \cup I_2 \setminus (I_1 \cap I_2)$.
- $\mathcal{L}.\text{insert}(I)$.

7. Output $\mathcal{L}$.

Here's an illustration:



Exponents of time & space complexities. 2

level	space	time
2	$S_2(k,p,\ell) := \frac{k+\ell}{2} H\left(\frac{p}{2(k+\ell)}\right)$	$\max\{S_2(k,p,\ell), 2S_2(k,p,\ell)-\ell_2\}$
1	$S_1(k,p,\ell,\ell_2) := 2S_2(k,p,\ell)-\ell_2$	$\max\{S_1(k,p,\ell,\ell_2), 2S_1(k,p,\ell,\ell_2)-\ell_1\}$