The Quantum Decoding Problem : Tight Achievability Bounds and Application to Regev's Reduction

25e Forum des jeunes mathématiciennes et mathématiciens

Agathe Blanvillain, André Chailloux, Jean-Pierre Tillich

27 Novembre 2025

Inria Paris, COSMIQ

Linear codes

Consider $\mathcal{C}$ an $[n, k]$ linear code on a finite field $\mathbb{Z}_q$ i.e $\mathbb{Z}_q$-linear subspace of $\mathbb{Z}_q^n$ of length n and dimension k. q is prime

A parity check matrix $\mathcal{H}$ of a code $\mathcal{C}$ is such that $\ker(\mathcal{H}) = \mathcal{C}$.

Linear codes

Consider $\mathcal{C}$ an $[n, k]$ linear code on a finite field $\mathbb{Z}_q$ i.e $\mathbb{Z}_q$-linear subspace of $\mathbb{Z}_q^n$ of length n and dimension k. q is prime

A parity check matrix $\mathcal{H}$ of a code $\mathcal{C}$ is such that $\ker(\mathcal{H}) = \mathcal{C}$.

The decoding problem

Input $y = c + e \in \mathbb{Z}_q^n$ with $c \in \mathcal{C}$ and $e \in \mathbb{Z}_q^n$ an error chosen with distribution p.

Output c or e

Linear codes

Consider $\mathcal{C}$ an $[n, k]$ linear code on a finite field $\mathbb{Z}_q$ i.e $\mathbb{Z}_q$-linear subspace of $\mathbb{Z}_q^n$ of length n and dimension k. q is prime

A parity check matrix $\mathcal{H}$ of a code $\mathcal{C}$ is such that $\ker(\mathcal{H}) = \mathcal{C}$.

The decoding problem

Input $y = c + e \in \mathbb{Z}_q^n$ with $c \in \mathcal{C}$ and $e \in \mathbb{Z}_q^n$ an error chosen with distribution p.

Output c or e

The Short Codeword Problem (SCP)

Input $\mathcal{C}$ linear code $[n, k]$, a metric $|\cdot|$ on $\mathbb{Z}_q^n$ and a bound ω

Output c a non-zero codeword verifying $|c| \leqslant \omega$

Why are we interested in these problems?

Uses in cryptography:

- Decoding Problem:
  - Encryption : Bike, McEliece, HQC, Kyber
  - Signature : SDitH
- Short Codeword Problem:
  - Signature :Wave , Dillithium

Idea : Study the difficulty to solve these problems with the quantum computer.

Quantum

Qubit:

Basis states : $|0\rangle$ and $|1\rangle$

Linear quantum superposition of the basis states : $\alpha, \beta \in \mathbb{C}$ with $|\alpha|^2 + |\beta|^2 = 1$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Quantum register of size n : quantum system with n qubits

elements of a Hilbert space of dimension 2^n

$\mathcal{H}_n = \mathcal{H} \otimes \ldots \otimes \mathcal{H}$ with $\mathcal{H} = Vect(|0\rangle) \oplus^{\perp} Vect(|1\rangle)$

Evolution of a quantum state :

- Unitary transformation
- measurement

Evolution of the quantum states

Measurement:

Decomposition of the ambiant space into orthogonal subspaces E_i

$|\psi\rangle \in \mathcal{H}$ with $\mathcal{H} = \bigoplus^{\perp} E_i$ and Π_i the orthogonal projection on E_i

Measurement of the state $|\psi\rangle$:

$$|\psi\rangle \to \frac{\Pi_i|\psi\rangle}{\|\Pi_i|\psi\rangle\|}$$

with probability $\|\Pi_i|\psi\rangle\|^2$

Example : $\mathbb{C}^2$: qubit space

$Vect(|0\rangle) \oplus^{\perp} Vect(|1\rangle)$

$$\alpha|0\rangle + \beta|1\rangle \to \begin{cases} |0\rangle & \text{with probability} |\alpha|^2 \\ |1\rangle & \text{with probability} |\beta|^2 \end{cases}$$

General algorithm (Regev)

Quantum algorithm : quantum reduction SCP (multiple solutions) $<$ DP (one solution)
Solve SCP using :

- a classical algorithm solving the decoding problem
- the quantum fourier transform

General algorithm (Regev)

Classical Fourier transform : $\widehat{f}(x) = \frac{1}{\sqrt{q^n}} \sum_{y \in \mathbb{Z}_q^n} e^{\frac{2i\pi \langle x,y \rangle}{q}} f(y)$

Quantum Fourier transform : $\mathrm{QFT}|x\rangle = \frac{1}{\sqrt{q^n}} \sum_{y \in \mathbb{Z}_q^n} e^{\frac{2i\pi \langle x,y \rangle}{q}} |y\rangle$

We denote the dual code of $\mathcal{C}$ as :$\mathcal{C}^\perp = \{x \in \mathbb{Z}_q^n \mid x.c^T = 0 \text{ for all } c \in \mathcal{C}\}$

Lemma

$$\mathrm{QFT}\Big(\sum_{c \in C} \sum_{e} F(e)|c+e\rangle\Big) = \sum_{c^\perp \in C^\perp} \hat{F}(c^\perp)|c^\perp\rangle$$

General algorithm (Regev)

1. *Construct* $\frac{1}{\sqrt{q^k}} \sum_{c \in C} |c\rangle \otimes \sum_e F(e)|e\rangle$
2. *Intricate* $\sum_{c \in C} \sum_e F(e)|c\rangle \otimes |c+e\rangle$
3. *Decode* Quantumly solve the decoding problem : from $c+e$, find c
   $\frac{1}{Z} \sum_{c \in C} \sum_e F(e)|0\rangle|c+e\rangle.$
4. *Quantum Fourier Transform* $\frac{1}{Z} \sum_{c^\perp \in C^\perp} \hat{F}(c^\perp)|0\rangle|c^\perp\rangle$
5. *Measure*

Regev's algorithm modified (Chen, Liu, Zhandry)

1. *Construct* $\frac{1}{\sqrt{q^k}} \sum_{c \in C} |c\rangle \otimes \sum_{e} F(e)|e\rangle$
2. *Intricate* $\sum_{c \in C} \sum_{e} F(e)|c\rangle \otimes |c+e\rangle = \sum_{c \in C} |c\rangle|\psi_c\rangle$ with $|\psi_c\rangle = \sum_{e \in \mathbb{Z}_q^n} F(e)|c+e\rangle$
3. *Decode* Quantumly solve the decoding problem : from $|\psi_c\rangle$, find c
   $\frac{1}{Z} \sum_{c \in C} |0\rangle|\psi_c\rangle$.
4. *Quantum Fourier Transform* $\frac{1}{Z} \sum_{c^\perp \in C^\perp} \hat{F}(c^\perp)|0\rangle|c^\perp\rangle$
5. *Measure*

The quantum decoding problem

The quantum decoding problem (S-LWE)

Input $|\psi_c\rangle = \sum_{e \in \mathbb{Z}_q^n} F(e)|c+e\rangle$ with $e \in \mathbb{Z}_q^n$ an error and $F(e) = \sqrt{p(e)}$

Output c

The quantum decoding problem is not harder than the classical decoding problem

When we measure $|\psi_c\rangle$, we get $c+e$ noisy codeword with probability $|F(e)|^2$

State of the art

[Chen, Liu, Zhandry 22]
Introduce S-LWE (quantum decoding problem): Quantum algorithms in polynomial time to solve S-LWE and a specific instance of SIS^{∞} (SCP with infinite norm)

- particular zone of parameters : no classical algorithm doing this in polynomial time
- reduction from the quantum algorithm solving QDP to the quantum algorithm solving SCP
- not in a constant rate : tends to 0

State of the art

[Chen, Liu, Zhandry 22]
Introduce S-LWE (quantum decoding problem): Quantum algorithms in polynomial time to solve S-LWE and a specific instance of SIS^{∞} (SCP with infinite norm)

- particular zone of parameters : no classical algorithm doing this in polynomial time
- reduction from the quantum algorithm solving QDP to the quantum algorithm solving SCP
- not in a constant rate : tends to 0

The quantum decoding problem [Chailloux, Tillich 23]

- natural zone of parameters: constant rate
- Bernoulli distribution
- solve the quantum decoding problem in polynomial time
- quantum algorithm in polynomial time to solve SCP equivalent to classical Prange algorithm
- go beyond with a non polynomial time algorithm to find minimal weight codeword in the dual code (PGM)

Latest results

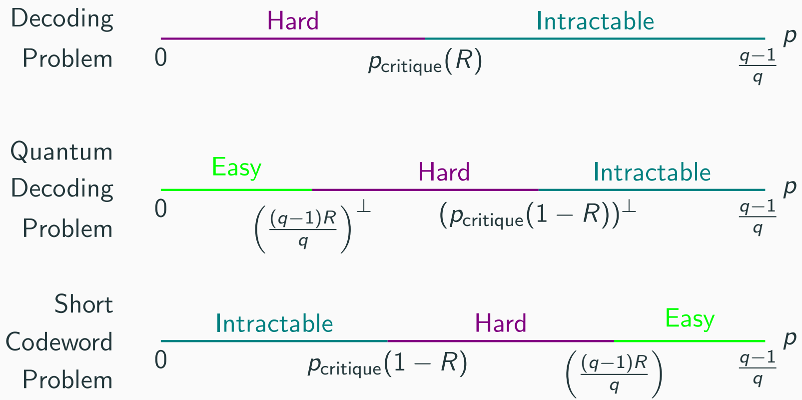
[Chen, Liu, Zhandry 22]
Introduce S-LWE (quantum decoding problem): Quantum algorithms in polynomial time to solve S-LWE and a specific instance of SIS^∞ (SCP with infinite norm)

- particular zone of parameters : no classical algorithm doing this in polynomial time
- reduction from the quantum algorithm solving QDP to the quantum algorithm solving SCP
- not in a constant rate : tends to 0

No exponential quantum speedup for SIS^∞ anymore [Kothary, O'Donnell, Wu 25]

- Classical algorithm that solves SIS^∞ in polynomial time
- No exponential quantum speedup anymore

Why is it interesting?



$$\Pr(e_i = 0) = 1 - p$$

$$\Pr(e_i \neq 0) = \frac{p}{q-1}$$

$$p^{\perp} = \frac{\sqrt{(1-p)(q-1)} - \sqrt{p}}{q}$$

The Pretty Good Measurement

Problem : From an ensemble $\{|\psi_i\rangle\}_{i\in[n]}$ of quantum states , we want to recover i from $|\psi_i\rangle$ when i is chosen at random.

Definition

The PGM associated to the ensemble $\{|\psi_i\rangle\}_{i\in[n]}$ of quantum states is the POVM $\{M_i\}_{i\in[n]}$ with

$$M_i = \rho^{-\frac{1}{2}}|\psi_i\rangle\langle\psi_i|\rho^{-\frac{1}{2}} \text{ given } \rho = \sum_{i\in[n]} |\psi_i\rangle\langle\psi_i|$$

Proposition

The PGM is optimal

Achievability result for random linear codes

We analyse the PGM in a general case of noise distribution $f = g^{\otimes n}$

Let $R = \frac{k}{n}$ be the rate of the code $\mathcal{C}$ and $H_q(|\hat{g}|^2) = -\sum_{e \in \mathbb{Z}_q} |\hat{g}(e)|^2 \log(|\hat{g}(e)|^2)$ be the entropy.

Theorem : Achievability result for random linear codes [Blanvillain, Chailloux, Tillich]

If there exists $\delta > 0$ such that $R < H_q(|\hat{g}|^2) + \delta$, then

$$\mathrm{P}_{\mathrm{PGM}} = 1 - o(1)$$

Achievability result for random linear codes

We analyse the PGM in a general case of noise distribution $f = g^{\otimes n}$

Let $R = \frac{k}{n}$ be the rate of the code $\mathcal{C}$ and $H_q(|\hat{g}|^2) = -\sum_{e \in \mathbb{Z}_q} |\hat{g}(e)|^2 \log(|\hat{g}(e)|^2)$ be the entropy.

Theorem : Achievability result for random linear codes [Blanvillain, Chailloux, Tillich]

If there exists $\delta > 0$ such that $R < H_q(|\hat{g}|^2) + \delta$, then

$$\mathrm{P}_{\mathrm{PGM}} = 1 - o(1)$$

Theorem : Tractability for Hamming distribution [Chailloux, Tillich]

Let $g(e)$ the error function for the Bernoulli distribution such that

$g(0) = \sqrt{1-p}$ and for $e \in \mathbb{Z}_q \backslash \{0\}$, $g(e) = \sqrt{\frac{p}{p-1}}$.

If $p < (\delta_{\min}(1-R))^{\perp}$, then $\mathrm{P}_{\mathrm{PGM}} = 1 - o(1)$

Non-achievability result in the general case

Theorem : Achievability result for random linear codes [Blanvillain, Chailloux, Tillich]

If there exists $\delta > 0$ such that $R < H_q(|\hat{g}|^2) - \delta$, then

$$\mathrm{P}_{\mathrm{PGM}} = 1 - o(1)$$

Theorem : Non-achievability result in the general case [Blanvillain, Chailloux, Tillich]

If there exists $\delta > 0$ such that $R \geqslant H_q(|\hat{g}|^2) + \delta$, then for any quantum algorithm and any code with q^{Rn} codewords,

$$\mathrm{P}_{\mathrm{PGM}} = o(1)$$

The rank metric case

Rank metric

When $n = a \cdot b$, $a \geq b$

Arrange the entries of a vector $\boldsymbol{x} \in \mathbb{Z}_q^n$ in a matrix $\mathbf{X} = \text{Mat}(\boldsymbol{x}) \in \mathbb{Z}_q^{a \times b}$

$$|\boldsymbol{x}|_{\text{rk}} \triangleq \text{rank}(\mathbf{X})$$

$$f_t^{a,b}(\boldsymbol{e}) = \begin{cases} \dfrac{\begin{bmatrix} b - |\boldsymbol{e}|_{\text{rk}} \\ t - |\boldsymbol{e}|_{\text{rk}} \end{bmatrix}_q}{\sqrt{q^{at} Z}} & \text{if } |\boldsymbol{e}|_{\text{rk}} \leqslant t \\ 0 & \text{else} \end{cases} \quad \text{with} \begin{bmatrix} b \\ t \end{bmatrix}_q = \begin{cases} \prod_{i=0}^{t-1} \dfrac{q^b - q^i}{q^t - q^i} & \text{if } t \leqslant b \\ 0 & \text{else} \end{cases}$$

$$\widehat{f_t} = f_{b-t}. \tag{1}$$

The rank metric case

Application in rank metric : case of interest in code-based cryptography : alternative to the usual Hamming metric
The distribution does not correspond to a product distribution

The probability distribution is a decreasing function of the rank weight. We get at the limit where the PGM works elements in the dual code of minimum rank weight.

The Quantum Decoding Problem : Takeaway

☞ Tight achievability results : it is possible from an information theoretic perspective to solve the Quantum Decoding Problem for random linear codes when $R < H_q(|\hat{g}|^2) - \delta$ for $\delta > 0$

The Quantum Decoding Problem : Takeaway

☞ Tight achievability results : it is possible from an information theoretic perspective to solve the Quantum Decoding Problem for random linear codes when $R < H_q(|\hat{g}|^2) - \delta$ for $\delta > 0$

☞ The algorithm can be used in Regev's reduction to solve the Short Codeword Problem to find low weight dual codewords. In a general distribution $|f|^2$, the algorithm permits to find the most probable codeword according to the probability distribution $|\hat{f}|^2$.

The Quantum Decoding Problem : Takeaway

☞ Tight achievability results : it is possible from an information theoretic perspective to solve the Quantum Decoding Problem for random linear codes when $R < H_q(|\hat{g}|^2) - \delta$ for $\delta > 0$

☞ The algorithm can be used in Regev's reduction to solve the Short Codeword Problem to find low weight dual codewords. In a general distribution $|f|^2$, the algorithm permits to find the most probable codeword according to the probability distribution $|\hat{f}|^2$.

When the distribution is a decreasing function of the norm or the weight, we find minimal codewords

The Quantum Decoding Problem : Takeaway

☞ Tight achievability results : it is possible from an information theoretic perspective to solve the Quantum Decoding Problem for random linear codes when $R < H_q(|\hat{g}|^2) - \delta$ for $\delta > 0$

☞ The algorithm can be used in Regev's reduction to solve the Short Codeword Problem to find low weight dual codewords. In a general distribution $|f|^2$, the algorithm permits to find the most probable codeword according to the probability distribution $|\hat{f}|^2$.

When the distribution is a decreasing function of the norm or the weight, we find minimal codewords

Thank you for your attention !