# Quantum Decoding For Optimization

Goals and overview

Stephen Jordan, Google Quantum AI

# What does quantum decoding have to do with optimization?

We are given an optimization problem.

Using a quantum Fourier transform we can reduce this to a *quantum decoding problem*.

Sometimes, this reduction is advantageous!

**Plan:** We will explore new ways to solve quantum decoding problems.

**Goals:** Improve upon current quantum state of the art, ideally by so much that we find new exponential quantum speedups.

# Example: max-XORSAT / Nearest Codeword Problem

max-XORSAT:

$$\mathbf{b}_i \cdot \mathbf{x} = v_i \qquad i = 1, \ldots, m$$

all over $\mathbb{F}_2$

nearest codeword:

$$C = \{B\mathbf{x} : \mathbf{x} \in \mathbb{F}_2^n\} \qquad \text{find} \qquad \min_{\mathbf{c} \in C} |\mathbf{c} - \mathbf{v}|$$

# Example: max-XORSAT / Nearest Codeword Problem

max-XORSAT:

$$\mathbf{b}_i \cdot \mathbf{x} = v_i \qquad i = 1, \ldots, m$$

all over $\mathbb{F}_2$

nearest codeword:

$$C = \{B\mathbf{x} : \mathbf{x} \in \mathbb{F}_2^n\} \qquad \text{find} \qquad \min_{\mathbf{c} \in C} |\mathbf{c} - \mathbf{v}|$$

The same!

# Example: max-XORSAT / Nearest Codeword Problem

nearest codeword:

$$C = \{B\mathbf{x} : \mathbf{x} \in \mathbb{F}_2^n\} \qquad \text{find} \qquad \min_{\mathbf{c}\in C} |\mathbf{c} - \mathbf{v}|$$

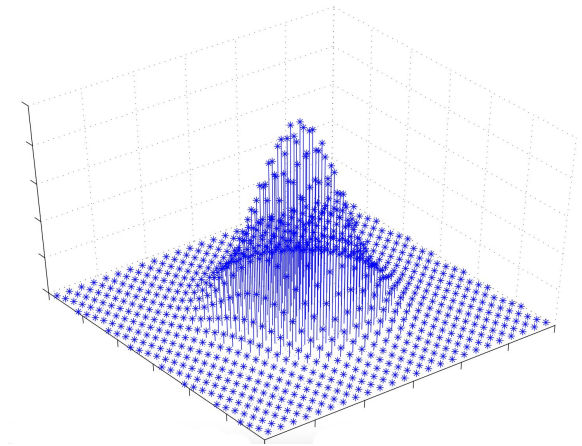


Image credit: O. Regev

If we can make a superposition over codewords close to **v**, we can find approximate solutions to the Nearest Codeword Problem.

# A strategy

Make this:

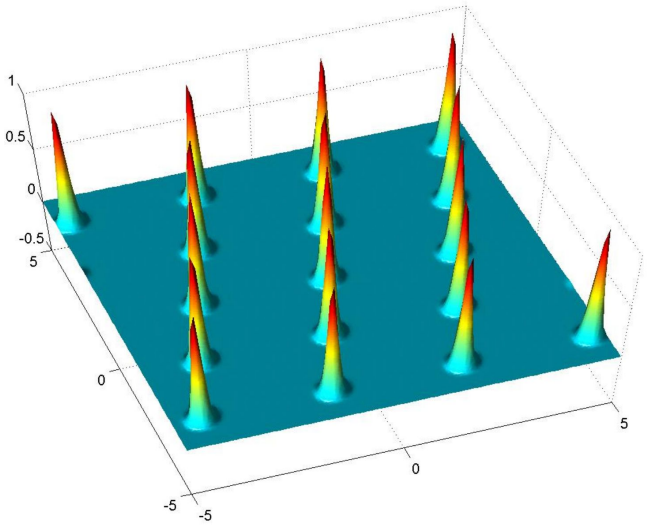
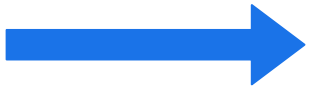



Image credit: O. Regev

Fourier Transform



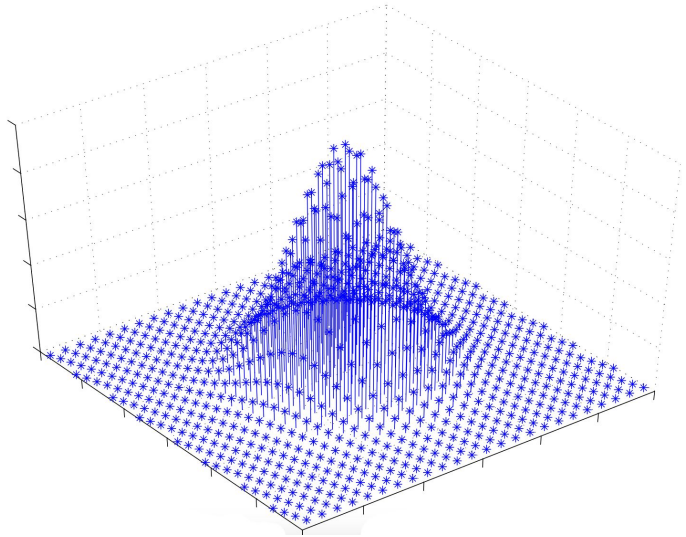


Image credit: O. Regev

# Ok, but how do we make the initial state?

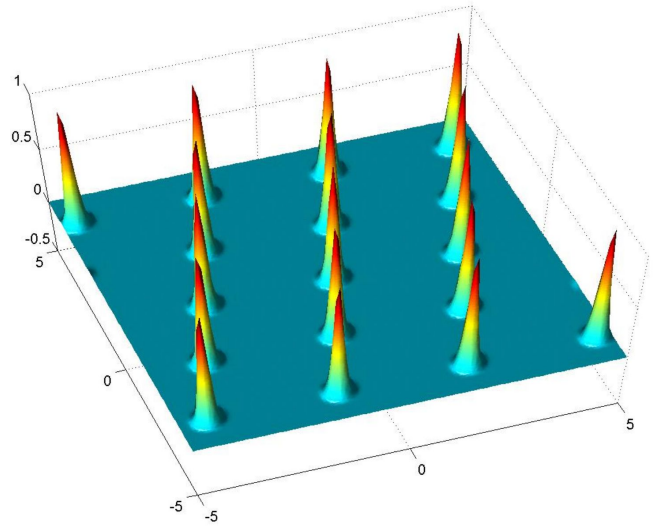



Image credit: O. Regev

$$\sum_{\mathbf{d}\in C^{\perp}} \sum_{\mathbf{e}} \sqrt{p(\mathbf{e})}\,|\mathbf{d}\rangle\,|\mathbf{d}+\mathbf{e}\rangle$$

uncompute **d**

$$\sum_{\mathbf{d}\in C^{\perp}} \sum_{\mathbf{e}} \sqrt{p(\mathbf{e})}\,|\mathbf{0}\rangle\,|\mathbf{d}+\mathbf{e}\rangle$$

# Ok, but how do we make the initial state?

suppose $p(\mathbf{e}) = \prod_{i=1}^{m} p(e_i)$

then our state $\sum_{\mathbf{d} \in C^{\perp}} \sum_{\mathbf{e}} \sqrt{p(\mathbf{e})} \, |\mathbf{d}\rangle \, |\mathbf{d} + \mathbf{e}\rangle$ is simply

$$\sum_{\mathbf{d} \in C^{\perp}} |\mathbf{d}\rangle \bigotimes_{i=1}^{m} \left( \sqrt{p(0)} \, |d_i\rangle + \sqrt{p(1)} \, |d_1 \oplus 1\rangle \right)$$

# The Quantum Decoding Problem:

given $\sum_{\mathbf{d}\in C^{\perp}} \bigotimes_{i=1}^{m} \left( \sqrt{p(0)}\,|d_i\rangle + \sqrt{p(1)}\,|d_1 \oplus 1\rangle \right)$ find **d**

the quantum channel we wish to decode from is:

$$|0\rangle \rightarrow \sqrt{1-\epsilon}\,|0\rangle + \sqrt{\epsilon}\,|1\rangle$$

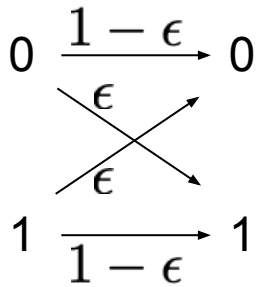
$$|1\rangle \rightarrow \sqrt{\epsilon}\,|0\rangle + \sqrt{1-\epsilon}\,|1\rangle$$

The quantum channel we wish to decode from is:

$$|0\rangle \rightarrow \sqrt{1-\epsilon}\,|0\rangle + \sqrt{\epsilon}\,|1\rangle$$

$$|1\rangle \rightarrow \sqrt{\epsilon}\,|0\rangle + \sqrt{1-\epsilon}\,|1\rangle$$

If we measure in the computational basis, we recover the classical binary symmetric channel:




…we could then use classical decoding algorithms.

# Beyond the Classical Strategy

Measuring each bit in the computational basis is not information-theoretically optimal; the Shannon bound is lower than the Holevo bound.

Reaching the Shannon bound requires classical decoding algorithms with exponential runtime.

Truly optimal decoding requires entangled operations across the qubits. These may require exponentially many gates to implement.

But one can get surprisingly far using optimized unentangled measurements and polynomial-time classical postprocessing!

# General Framework

for reducing optimization to quantum decoding

# ProductSample: more natural than it appears

Given:

$$C = \{B\mathbf{x} : \mathbf{x} \in \mathbb{F}_q^n\} = \{\mathbf{y} \in \mathbb{F}_q^m : A\mathbf{y} = \mathbf{0}\}$$

$$p_j : \mathbb{F}_q \to [0,1] \quad j = 1, \ldots, m$$

Sample:

$$\mathbf{y} \in C \qquad p(\mathbf{y}) = \prod_{i=1}^{m} p_i(y_i)$$

# ProductSample, Application 1

Given: $\mathbf{v} \in \mathbb{F}_2^m$ $B \in \mathbb{F}_2^{m \times n}$ $\epsilon \in [0, 1]$

Let:

$$C = \{\mathbf{y} = B\mathbf{x} : \mathbf{x} \in \mathbb{F}_2^n\}$$

$$p_i(y) = \begin{cases} 1 - \epsilon & \text{if } y = v_i \\ \epsilon & \text{otherwise} \end{cases}$$

# ProductSample, Application 1

$$C = \{\mathbf{y} = B\mathbf{x} : \mathbf{x} \in \mathbb{F}_2^n\} \qquad p_i(y) = \begin{cases} 1-\epsilon & \text{if } y = v_i \\ \epsilon & \text{otherwise} \end{cases}$$

---

Then $p(\mathbf{y}) = \prod_{i=1}^{m} p_i(y_i)$ implies

$$p(\mathbf{x}) = \epsilon^{|\mathbf{v}-B\mathbf{x}|}\ (1-\epsilon)^{m-|\mathbf{v}-B\mathbf{x}|}$$

# ProductSample, Application 1

If $\epsilon$ is small, then sampling from:

$$p(\mathbf{x}) = \epsilon^{|\mathbf{v}-B\mathbf{x}|}\ (1-\epsilon)^{m-|\mathbf{v}-B\mathbf{x}|}$$

yields: $\mathbf{y} \in \{B\mathbf{x} : \mathbf{x} \in \mathbb{F}_2^n\}$ close to $\mathbf{v}$

i.e. finds approximate solutions to the nearest codeword problem (= max-XORSAT): $B\mathbf{x} \overset{\max}{=} \mathbf{v}$

# ProductSample, Application 2

Let: $\mathbf{v} \in \mathbb{F}_2^m$ $C = \{\mathbf{y} = B\mathbf{x} : \mathbf{x} \in \mathbb{F}_2^n\}$

$$p_i(y) = \begin{cases} 1 - \epsilon_i & \text{if } y = v_i \\ \epsilon_i & \text{otherwise} \end{cases}$$

$$\epsilon_i = \begin{cases} 0 & \text{if } i \leq c \\ \epsilon & \text{otherwise} \end{cases}$$

Can you see what problem this solves?

# ProductSample, Application 2

Let: $B = \begin{bmatrix} B^{(1)} \\ B^{(2)} \end{bmatrix}$ $B^{(1)} = \begin{bmatrix} -\mathbf{b}_1- \\ \vdots \\ -\mathbf{b}_c- \end{bmatrix}$ $B^{(2)} = \begin{bmatrix} -\mathbf{b}_{c+1}- \\ \vdots \\ -\mathbf{b}_m- \end{bmatrix}$

Recall:

$$p_i(y) = \begin{cases} 1-\epsilon_i & \text{if } y = v_i \\ \epsilon_i & \text{otherwise} \end{cases} \qquad \epsilon_i = \begin{cases} 0 & \text{if } i \le c \\ \epsilon & \text{otherwise} \end{cases}$$

So, our samples come from: $\left\{\mathbf{x} \in \mathbb{F}_2^n : B^{(1)}\mathbf{x} = \mathbf{v}^{(1)}\right\}$

# ProductSample, Application 2

This is constrained max-XORSAT!

Our samples will come from: $\left\{\mathbf{x} \in \mathbb{F}_2^n : B^{(1)}\mathbf{x} = \mathbf{v}^{(1)}\right\}$

According to:

$$p(\mathbf{x}) = \epsilon^{|\mathbf{v}^{(2)} - B^{(2)}\mathbf{x}|} \, (1-\epsilon)^{m - |\mathbf{v}^{(2)} - B^{(2)}\mathbf{x}|}$$

# ProductSample, Application 2

$B^{(1)}\mathbf{x} = \mathbf{v}^{(1)}$ are the hard constraints.

$B^{(2)}\mathbf{x} = \mathbf{v}^{(2)}$ are the soft constraints, in other words:

$|B^{(2)}\mathbf{x} - \mathbf{v}^{(2)}|$ is the objective function.

# ProductSample, Application 3

Given: $\mathbf{v} \in \mathbb{F}_3^m$ $A \in \mathbb{F}_3^{h \times m}$

Let:

$$C = \{\mathbf{y} \in \mathbb{F}_3^m : A\mathbf{y} = \mathbf{0}\}$$

$$p_i(y) = \begin{cases} 0 & \text{if } y = v_i \\ 1/2 & \text{otherwise} \end{cases}$$

# ProductSample, Application 3

$$C = \{\mathbf{y} \in \mathbb{F}_3^m : A\mathbf{y} = \mathbf{0}\} \qquad p_i(y) = \begin{cases} 0 & \text{if } y = v_i \\ 1/2 & \text{otherwise} \end{cases}$$

---

Then $p(\mathbf{y}) = \prod_{i=1}^{m} p_i(y_i)$ uniformly samples from

$$\{\mathbf{y} \in C : y_i \neq v_i \ \forall i\}$$

# ProductSample, Application 3

Finding an element of $\{\mathbf{y} \in C : y_i \neq v_i \ \forall i\}$

is the Chen-Liu-Zhandry problem ($SIS_\infty$)

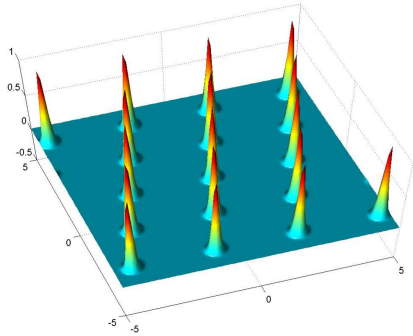
Quantum computers efficiently solve this in a parameter regime where no efficient classical algorithm is known!

# How can we solve ProductSample?

## Convolution Theorem:

$$\mathcal{F} \sum_{x \in \mathbb{F}_q^m} f(\mathbf{x}) g(\mathbf{x}) \, |\mathbf{x}\rangle = \sum_{\mathbf{y} \in \mathbb{F}_q^m} \sum_{\mathbf{z} \in \mathbb{F}_q^m} \tilde{f}(\mathbf{y}) \tilde{f}(\mathbf{z}) \, |\mathbf{y} + \mathbf{z}\rangle$$

$$\cdot \overset{FT}{\longleftrightarrow} \star$$



FT

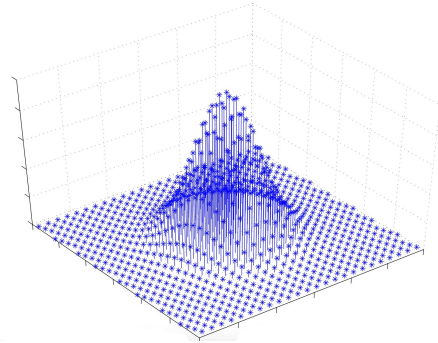


Image credit: O. Regev

Image credit: O. Regev

# How can we solve ProductSample?

First, make:

$$|\psi_{\mathrm{Pr}}\rangle = \left(\sum_{y_1 \in \mathbb{F}_q} \sqrt{p_1(y_1)}\,|y_1\rangle\right) \otimes \ldots \otimes \left(\sum_{y_m \in \mathbb{F}_q} \sqrt{p_m(y_m)}\,|y_m\rangle\right) = \sum_{\mathbf{y} \in \mathbb{F}_q^m} p(\mathbf{y})\,|\mathbf{y}\rangle$$

and:

$$|\psi_C\rangle = \frac{1}{\sqrt{|C|}} \sum_{\mathbf{y} \in C} |\mathbf{y}\rangle = \frac{1}{\sqrt{|C|}} \sum_{\mathbf{y} \in \mathbb{F}_q^m} \mathbb{1}_C(\mathbf{y})\ \ |\mathbf{y}\rangle$$

Our final goal is to make: $|\psi_C \cdot \psi_{\mathrm{Pr}}\rangle = \sum_{\mathbf{y} \in \mathbb{F}_q^n} p(\mathbf{y}) \cdot \mathbb{1}_C(\mathbf{y})\ \ |\mathbf{y}\rangle$

# How can we solve ProductSample?

Next, apply quantum Fourier transforms, yielding:

$$\mathcal{F}\,|\psi_C\rangle = \frac{1}{|C^\perp|}\sum_{\mathbf{d}\in C^\perp}|\mathbf{d}\rangle$$

and:

$$\mathcal{F}\,|\psi_{\mathrm{Pr}}\rangle = \sum_{\mathbf{e}\in\mathbb{F}_q^m}\widetilde{\sqrt{p}}(\mathbf{e})\,|\mathbf{e}\rangle \quad \text{where:} \quad \widetilde{\sqrt{p}}(\mathbf{e}) = \prod_{i=1}^{m}\widetilde{\sqrt{p_i}}(e_i)$$

# How can we solve ProductSample?

Now we have:

$$\frac{1}{\sqrt{|C^{\perp}|}} \sum_{\mathbf{d} \in C^{\perp}} \sum_{\mathbf{e} \in \mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e}) \, |\mathbf{d}\rangle \, |\mathbf{e}\rangle$$

Using reversible addition we get:

$$\frac{1}{\sqrt{|C^{\perp}|}} \sum_{\mathbf{d} \in C^{\perp}} \sum_{\mathbf{e} \in \mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e}) \, |\mathbf{d} + \mathbf{e}\rangle \, |\mathbf{d}\rangle$$

# How can we solve ProductSample?

Now we have:

$$\frac{1}{\sqrt{|C^{\perp}|}} \sum_{\mathbf{d} \in C^{\perp}} \sum_{\mathbf{e} \in \mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e}) \, |\mathbf{d} + \mathbf{e}\rangle \, |\mathbf{d}\rangle$$

Recall, what we want is:

$$|\psi_C \cdot \psi_{\mathrm{Pr}}\rangle = \sum_{\mathbf{y} \in \mathbb{F}_q^n} p(\mathbf{y}) \cdot \mathbb{1}_C(\mathbf{y}) \;\; |\mathbf{y}\rangle$$

$$= \mathcal{F} \frac{1}{\sqrt{|C^{\perp}|}} \sum_{\mathbf{d} \in C^{\perp}} \sum_{\mathbf{e} \in \mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e}) \, |\mathbf{d} + \mathbf{e}\rangle$$

by convolution thm

# How can we solve ProductSample?

Thus our last two tasks are:

1) to uncompute e

$$\frac{1}{\sqrt{|C^{\perp}|}} \sum_{\mathbf{d}\in C^{\perp}} \sum_{\mathbf{e}\in\mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e}) \, |\mathbf{d}+\mathbf{e}\rangle \, |\mathbf{d}\rangle \rightarrow \frac{1}{\sqrt{|C^{\perp}|}} \sum_{\mathbf{d}\in C^{\perp}} \sum_{\mathbf{e}\in\mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e}) \, |\mathbf{d}+\mathbf{e}\rangle \, |\mathbf{0}\rangle$$

2) apply a Fourier transform

# The Quantum Decoding Problem

$$\frac{1}{\sqrt{|C^{\perp}|}} \sum_{\mathbf{d} \in C^{\perp}} \sum_{\mathbf{e} \in \mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e}) \, |\mathbf{d}+\mathbf{e}\rangle \, |\mathbf{d}\rangle \rightarrow \frac{1}{\sqrt{|C^{\perp}|}} \sum_{\mathbf{d} \in C^{\perp}} \sum_{\mathbf{e} \in \mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e}) \, |\mathbf{d}+\mathbf{e}\rangle \, |\mathbf{0}\rangle$$

For each codeword d, we have a coherent superposition over errors e. The probability of error on symbol i is:

$$1 - \left| \widetilde{\sqrt{p}}_i(0) \right|^2$$

# The Quantum Decoding Problem

If we have a method that works on any given codeword, then by linearity it works on the superposition.

$$\sum_{\mathbf{e}\in\mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e})\,|\mathbf{d}+\mathbf{e}\rangle\,|\mathbf{d}\rangle \rightarrow \sum_{\mathbf{e}\in\mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e})\,|\mathbf{d}+\mathbf{e}\rangle\,|\mathbf{0}\rangle$$

So, we can forget about superposition over the code.

# The Quantum Decoding Problem

If we have a method that works using measurements we can always replace these with controlled operations.

$$\sum_{\mathbf{e}\in\mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e})\,|\mathbf{d}+\mathbf{e}\rangle \to \mathbf{d}$$

So, we can forget about maintaining coherence.

# The Quantum Decoding Problem

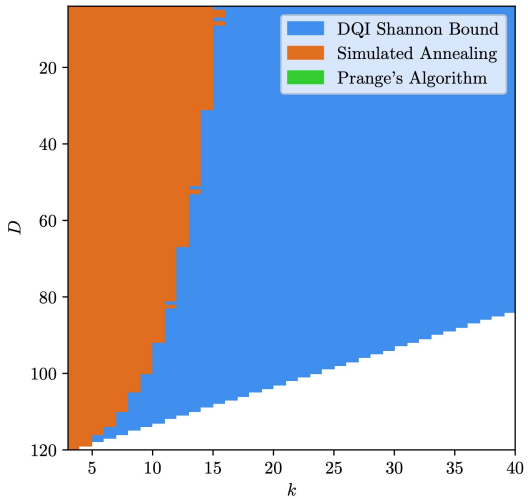
$$\sum_{\mathbf{e}\in\mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e})\,|\mathbf{d}+\mathbf{e}\rangle \to \mathbf{d}$$

The classical strategy:

1) measure in the computational basis
2) use a classical decoding algorithm

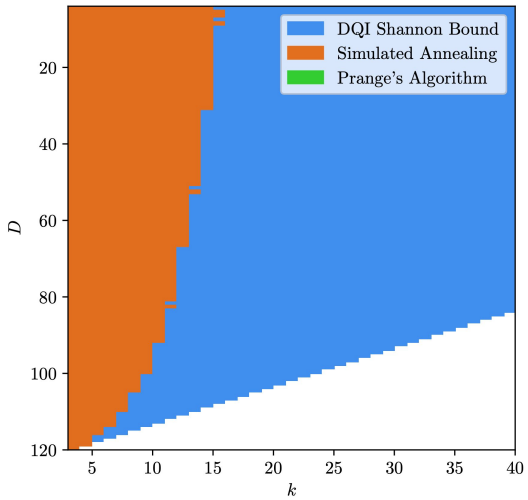
# The Quantum Decoding Problem

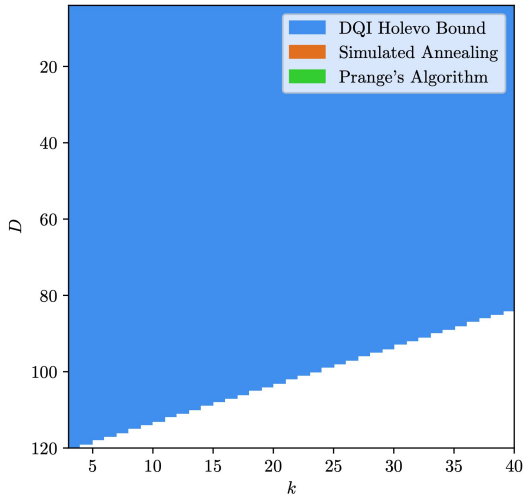
The classical strategy sometimes yields good results. See Yamakawa-Zhandry and DQI for OPI. But it is not optimal even information-theoretically.



# The Quantum Decoding Problem

The classical strategy sometimes yields good results. See Yamakawa-Zhandry and DQI for OPI. But it is not optimal even information-theoretically.



# The Quantum Decoding Problem

$$\sum_{\mathbf{e}\in\mathbb{F}_q^m} \widetilde{\sqrt{p}}(\mathbf{e})\,|\mathbf{d}+\mathbf{e}\rangle \to \mathbf{d}$$

Unentangled strategies:

1) Measure each symbol in some carefully chosen basis
2) Classically decode the results

# The Quantum Decoding Problem

Unentangled strategies are also not optimal.

But they are simpler to think about than general quantum strategies.

They have already gotten some great results and led to promising research directions.

See talks by Mark Zhandry and Noah Shutty!

# Key Papers


Yilei Chen, Qipeng Liu, and Mark Zhandry. Quantum algorithms for variants of average-case lattice problems via filtering. In *Annual international conference on the theory and applications of cryptographic techniques (EUROCRYPT)*, pages 372–401. Springer, 2022.

Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 69–74. IEEE, 2022.

André Chailloux and Jean-Pierre Tillich. The quantum decoding problem. *arXiv:2310.20651*, 2023.

Thomas Debris-Alazard, Maxime Remaud, and Jean-Pierre Tillich. Quantum reduction of finding short code vectors to the decoding problem. *IEEE Transactions on Information Theory*, 2023.

Stephen P. Jordan, Noah Shutty, Mary Wootters, Adam Zalcman, Alexander Schmidhuber, Robbie King, Sergei V. Isakov, Tanuj Khattar, and Ryan Babbush. Optimization by decoded quantum interferometry. 2024. arXiv:2408.08292.

André Chailloux and Jean-Pierre Tillich. Quantum advantage from soft decoders. *arXiv:2411.12553*, 2024.

# Quantum Advantage

We have neither NP-hardness nor query complexity lower bounds to rule out classical algorithms.

We just need to play cat and mouse.

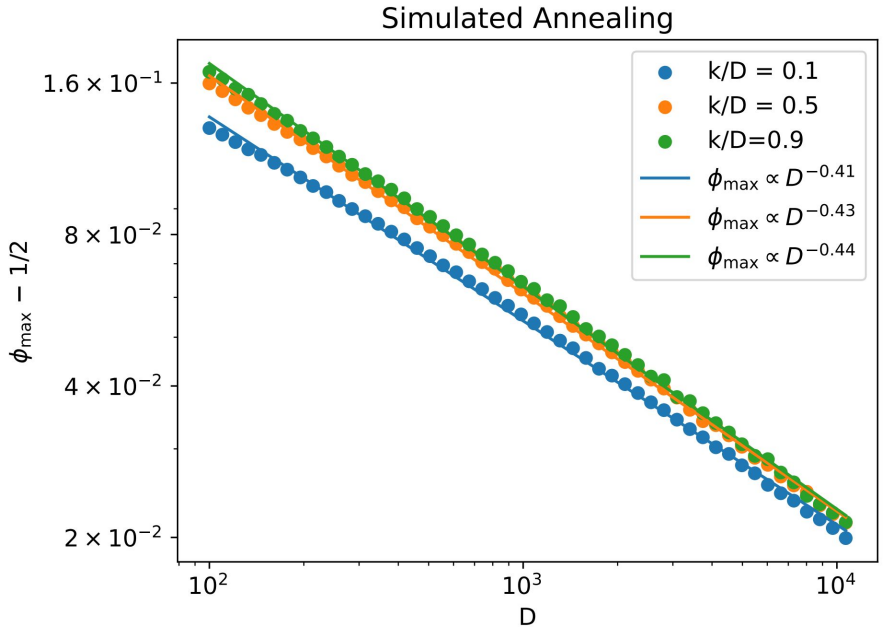
Two key competitors:

- Simulated annealing
- Prange's algorithm

# Simulated Annealing

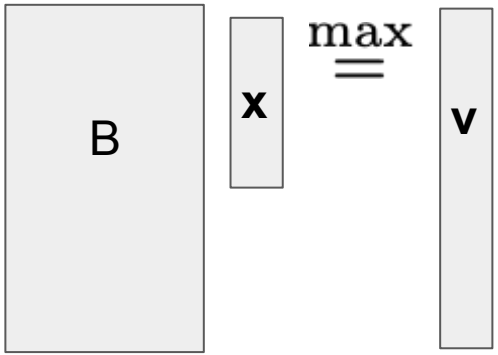
Simulated annealing is formidable when the generator matrix of C is sparse.

$$\phi_{\max} = \frac{1}{2} + \frac{\text{const}}{\sqrt{D}}$$



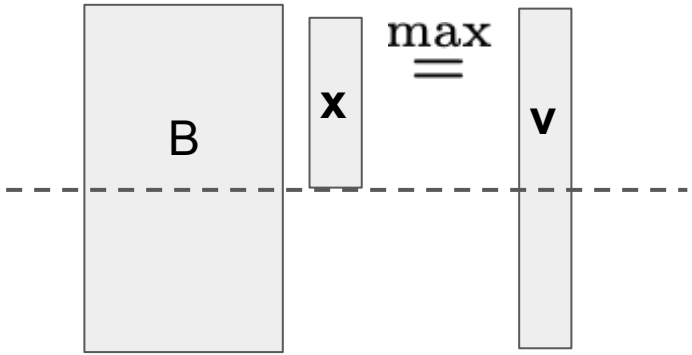
# Prange's Algorithm

Example: max-XORSAT



# Prange's Algorithm

Example: max-XORSAT (n variables, m constraints)




1) Pick n of the m constraints
2) Solve the resulting linear system

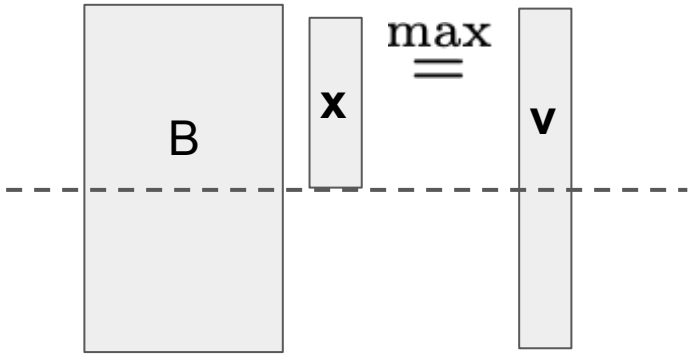
Result:

n constraints satisfied with certainty

(n-m) constraints each satisfied with prob. 1/2

# Prange's Algorithm

Example: max-XORSAT (n variables, m constraints)




1) Pick n of the m constraints
2) Solve the resulting linear system

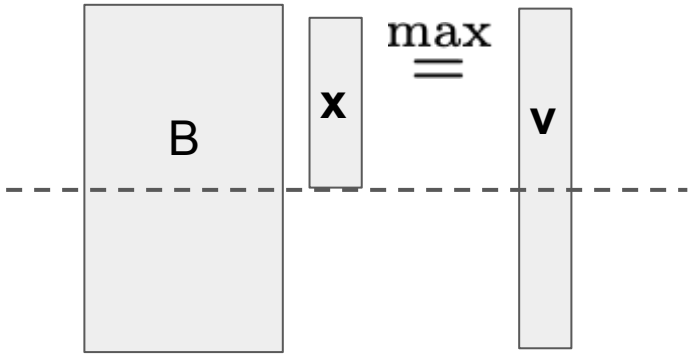
Result:

n constraints satisfied with certainty

(n-m) constraints each satisfied with prob. 1/2

# Prange's Algorithm

Example: max-XORSAT (n variables, m constraints)




1) Pick n of the m constraints
2) Solve the resulting linear system

If you can beat SA & Prange you might be onto something!

Good Luck!

Result:

n constraints satisfied with certainty

(n-m) constraints each satisfied with prob. 1/2