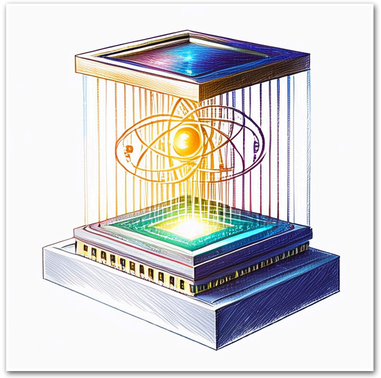
Quantum Advantage via Solving Multivariate Polynomials

Pierre Briaud (Simula UiB),
Itai Dinur (Ben-Gurion Uni., Georgetown Uni.),
Riddhi Ghosal (UCLA),
Aayush Jain (CMU)
Paul Lou (Bocconi Uni., work done while @ UCLA)
Amit Sahai (UCLA)

Quantum Advantage in **NP**-search



vs.

Are there **NP**-search (solutions are classically efficiently verifiable) problems that are

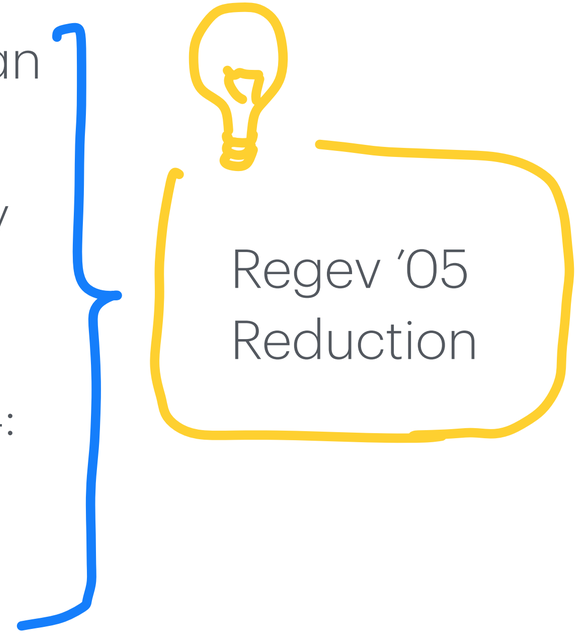
quantum polynomial-time tractable, yet **classically hard-to-solve**?

Quantum Advantage in **NP**-search

Quantumly easy, classically hard?

- **Hidden Subgroup Problems**, e.g. Simon's problem, Bernstein-Vazirani, factoring, discrete-log, Pell's equations, offer conjectured advantage from structured (*periodicity*) **NP**-search problems.

- **Yamakawa-Zhandry (YZ)** '22: Relative to *a random oracle,* there exists an *unstructured* **NP**-search problem that is quantumly easy-to-solve, yet unconditionally hard against any computationally-unbounded adversary making a polynomial number of classical queries.



- Jordan-Shutty-Wootters-Zalcman-Schmidhuber-King-Isakov-Babbush '24: **Decoded Quantum Interferometry (DQI)** speedups for optimization problems (e.g. optimal polynomial intersection).

Our Work: Sampling Roots for a Multivariate Polynomial System

Multivariate Polynomial Systems over Finite Fields

Is solving conjecturably quantumly and classically hard?

- **Worst-case complexity:** Deciding if a multivariate quadratic system over $\mathbb{F}_2$ has roots is **NP** -complete [Fraenkel-Yesha '77, Garey-Johnson '79].
- **Average-case complexity:** Sample *uniform random* $\mathscr{P} \triangleq \{p_i \leftarrow_R \mathbb{F}_2^{d\leq 2}[X_1, \ldots, X_n]\}_{i\in[m]}$. Given $(\mathscr{P}, \mathbf{y} = \mathscr{P}(\mathbf{x}))$, can you recover a preimage of $\mathbf{y}$?
  - Overdetermined regime: When $m = \Omega(n^2)$, polynomial time solvable via a linearization algorithm [Kipnis-Shamir '99]. Otherwise, believed to be $exp(n^2/m)$ hard.
  - Underdetermined regime: When $m = O(\sqrt{n})$, polynomial time solvable via [Section 7 of Kipnis-Patarin-Goubin '99]. Otherwise, believed to be $exp(m)$ hard.

Multivariate Polynomial Systems over Finite Fields

Is solving conjecturably quantumly and classically hard?

- **Quantum complexity:** No exponential speed up known, only polynomial speedups.
  - There's Grover search: $O(2^{n/2})$.
  - [Faugère-Kahrobaei-Kaplan-Kashefi-Perret '17] improve this to $O(2^{0.462n})$ quantum gates for the case of $m = n$ under some algebraic assumption on the system.

Structured Multivariate Polynomial Systems over Finite Fields

Cryptographers use these!

- **Mask easy-to-invert system by hidden linear transformation** [Patarin '96, '97, Kipnis-Patarin-Goubin '99]**.**
  - **Example** (Oil-&-Vinegar [Patarin '97, Kipnis-Patarin-Goubin '99]): Consider coefficient matrix of the form,

$$\mathbf{A} \triangleq \begin{pmatrix} \mathbf{0} & \mathbf{A}_1 \\ \mathbf{A}_2 & \mathbf{A}_3 \end{pmatrix} \in \mathbb{F}_q^{n \times n}.$$

$$\text{e.g. } \mathbf{x}^\top \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \mathbf{x} = 3x_1x_2 + 3x_2^2.$$

  - A random assignment to some fraction of the variables results in a linear system in the remaining variables.
  - Conjecturably, for appropriate parameters, it's hard-to-invert an underdetermined polynomial system $\{\mathbf{T}^\top \cdot \mathbf{A}^{(i)} \cdot \mathbf{T}\}_{i \in [m]}$. In fact, conjecturably quantum hard (in "post-quantum" signature competition).

Are there quantumly easy, yet conjecturably classically-hard, multivariate polynomial systems?

Recalling the YZ Proof of Quantumness

(results extend beyond $\mathbb{F}_2$, as do ours)

- For $i \in [n^2]$, let $H_i : \mathbb{F}_2^n \to \mathbb{F}_2$ be random functions.
- Let $C \subseteq \mathbb{F}_2^{n^3}$ be a code* and view a codeword $\mathbf{c} = \mathbf{c}_1 \| \mathbf{c}_2 \| \cdots \| \mathbf{c}_{n^2}$ where each $\mathbf{c}_i \in \mathbb{F}_2^n$.
- Define $H : C \to \mathbb{F}_2^{n^2}$ as follows:

$$H(\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{n^2}) = (H_1(\mathbf{c}_1), \ldots, H_{n^2}(\mathbf{c}_{n^2}))$$

- YZ shows unconditionally one-way against classical probabilistic algorithms in ROM with polynomially bounded queries to $(H_i)_{i \in [n^2]}$ and there exists an efficient quantum algorithm in the QROM, given any image value y, samples stat. close to uniformly from the set of preimages of y.

Recalling the YZ Proof of Quantumness

(results extend beyond $\mathbb{F}_2$, as do ours)

- For $i \in [n^2]$, let $H_i : \mathbb{F}_2^n \to \mathbb{F}_2$ be random functions.
- Let $C \subseteq \mathbb{F}_2^{n^3}$ be a code* and view

Any instantiation of H_i gives insight into quantum easiness, e.g. LWE, LPN, your favorite problem…

- Define $H : C \to \mathbb{F}_2^{n^2}$ as follows:

$$H(\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{n^2}) = (H_1(\mathbf{c}_1), \ldots, H_{n^2}(\mathbf{c}_{n^2}))$$

- YZ shows unconditionally one-way against classical probabilistic algorithms in ROM with polynomially bounded queries to $(H_i)_{i\in[n^2]}$ and there exists an efficient quantum algorithm in the QROM, given any image value y, samples stat. close to uniformly from the set of preimages of y.

Recalling the YZ Proof of Quantumness

(results extend beyond $\mathbb{F}_2$, as do ours)

- For $i \in [n^2]$, let $H_i : \mathbb{F}_2^n \to \mathbb{F}_2$ be random functions.
- Let $C \subseteq \mathbb{F}_2^{n^3}$ be a code* and view
- Define $H : C \to \mathbb{F}_2^{n^2}$ as follows:

Natural thought: Can we instantiate H_i with random low-degree polynomials?

$$H(\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{n^2}) = (H_1(\mathbf{c}_1), \ldots, H_{n^2}(\mathbf{c}_{n^2}))$$

- YZ shows unconditionally one-way against classical probabilistic algorithms in ROM with polynomially bounded queries to $(H_i)_{i\in[n^2]}$ and there exists an efficient quantum algorithm in the QROM, given any image value y, samples stat. close to uniformly from the set of preimages of y.

Our Work: Instantiation with Random Low-degree Polynomials

Natural thought: Can we instantiate H_i with random low-degree polynomials?

Our work: Yes! For any $d \geq 3$, we can instantiate the H_i with uniform random at most degree d polynomials.

The resulting system is efficiently quantumly invertible, and conjecturably classically hard.

In fact, our results extend to any distribution over polynomials that is (1) shift-invariant and (2) 2-wise independent.

Our Polynomial System

- Fix $d \geq 3$. Total of n^3 variables, organized into n^2 blocks of n variables.

1. **Degree d constraints**: Sample n^2 many **random** at most degree d polynomials, $\{p_i\}_{i \in [n^2]}$, each on a disjoint block of variables.

2. **Linear constraints**: a Generalized Reed-Solomon parity-check matrix over the field extension $\mathbb{F}_{2^n}$:

$$\mathbf{H} \in \mathbb{F}_{2^n}^{(1-\alpha)n^2 \times n^2} \leftrightarrow \overline{\mathbf{H}} \in \mathbb{F}_2^{(1-\alpha)n^3 \times n^3}.$$

$$\overline{\mathbf{H}} \cdot \mathbf{x} = \mathbf{0}.$$

Our Polynomial System

$p_1(x_1, \ldots, x_n)$

$p_2(x_{n+1}, \ldots, x_{2n})$

$\ldots$

$p_{n^2}(x_{n^3-n+1}, \ldots, x_{n^3})$

} degree d

GRS parity check $H =$

$\mathbb{F}_{2^n}^*$ non-zero column multipliers

$$\begin{bmatrix} u_1 & u_2 & \cdots & u_{n^2} \\ u_1 a_1 & u_2 a_2 & \cdots & u_{n^2} a_{n^2} \\ u_1 a_1^2 & u_2 a_2^2 & \cdots & u_{n^2} a_{n^2}^2 \\ \vdots & \vdots & & \vdots \\ u_1 a_1^{(1-\alpha)n^2-1} & u_2 a_2^{(1-\alpha)n^2-1} & \cdots & u_{n^2} a_{n^2}^{(1-\alpha)n^2-1} \end{bmatrix}$$

distinct in $\mathbb{F}_{2^n}$

Our Polynomial System

$p_1(x_1, \ldots, x_n)$

$p_2(x_{n+1}, \ldots, x_{2n})$

$\ddots$

$p_{n^2}(x_{n^3-n+1}, \ldots, x_{n^3})$

} degree d

Converted to $\mathbb{F}_2$

$\overline{H} =$ ← $n \times n$ block matrix over $\mathbb{F}_2$

$$\begin{bmatrix} M(u_1) & M(u_2) & \cdots & M(u_{n^2}) \\ M(u_1 a_1) & M(u_2 a_2) & \cdots & M(u_{n^2} a_{n^2}) \\ M(u_1 a_1^2) & M(u_2 a_2^2) & \cdots & M(u_{n^2} a_{n^2}^2) \\ \vdots & \vdots & \ddots & \vdots \\ M(u_1 a_1^{(1-\alpha)n^2-1}) & & \cdots & M(u_{n^2} a_{n^2}^{(1-\alpha)n^2-1}) \end{bmatrix}$$

Our Polynomial System

$p_1(x_1, \ldots, x_n)$

$p_2(x_{n+1}, \ldots, x_{2n})$

$\ldots$

$p_{n^2}(x_{n^3-n+1}, \ldots, x_{n^3})$

} degree d

$$\ell_1(x_1, \ldots, x_{n^3}) = \sum_{i=1}^{n^3} \alpha_i^{(1)} x_i$$

$$\ell_2(x_1, \ldots, x_{n^3}) = \sum_{i=1}^{n^3} \alpha_i^{(2)} x_i$$

$$\vdots \qquad \vdots$$

$$\ell_{(1-\alpha)n^3}(x_1, \ldots, x_{n^3}) = \sum_{i=1}^{n^3} \alpha_i^{((1-\alpha)n^3)} x_i$$

} $(1-\alpha)n^3$ Linearly indep. linear equations

Our Polynomial System

$p_1(x_1, \ldots, x_n)$

$p_2(x_{n+1}, \ldots, x_{2n})$

$\ldots$

$p_{n^2}(x_{n^3-n+1}, \ldots, x_{n^3})$

} degree d

$x_1 = \sum_{i \neq 1} \alpha_i^{(1)} x_i$

$x_2 = \sum_{i \neq n+1} \alpha_i^{(2)} x_i$

$\vdots$

$x_{(1-\alpha)n^3} = \sum_{i \neq (1-\alpha)n^3}^{(1-\alpha)n^3} \alpha_i x_i$

} $(1-\alpha)n^3$ Linearly indep. linear equations

Each linear constraint allows for the backsubstitution for 1 variable.

Post-substitution, the degree d constraints are in αn^3 variables.

Classical Attacks

Why $d \geq 3$?

- There is a known normal form for degree two polynomials in characteristic two fields [Lidl-Niederreiter '97]:
  - Can be expressed in the form $z_1 z_2 + z_3 z_4 + \ldots + z_{r-1} z_r$ under some efficiently computable linear transformation on the variables $(x_1, \ldots, x_n)$ for some r dependent on the polynomial.
  - Recall, our degree d constraints are on disjoint variables, so for each polynomial constraint, fix $n/2$ of the variables to obtain a underdetermined linear system.

Classical Attacks

Why $d \geq 3$?

- There is a known normal form for degree two polynomials in characteristic two fields [Lidl-Niederreiter '97]:
  - Can be expressed in the form $z_1 z_2 + z_3 z_4 + \ldots + z_{r-1} z_r$ under some efficiently computable linear transformation on the variables $(x_1, \ldots, x_n)$ for some r dependent on the polynomial.
  - Recall, our degree d constraints are on disjoint variables, so for each polynomial constraint, fix $n/2$ of the variables to obtain a underdetermined linear system.

Classical Attacks

Known Attack Strategies Fail

- Similar other attacks on underdetermined quadratic systems also add specific linear constraints to produce an affine system. E.g. [Thomae-Wolf '12, Furue-Nakamura-Takagi '21, Hashimoto '23]—**not known to extend to $d \geq 3$.**
  - $2^{-\Omega(n^2)}$ probability that for a random degree 3 polynomial, no choice of $n - o(n)$ affine equations that reduce it to a degree 2 polynomial.
  - Reduce #vars to $o(n^3)$ results in no solutions (code constraints give $O(n^3)$ equations).
- Other attacks:
  - Non-trivial exhaustive search exponential in n^2 time.
  - Gröbner basis algorithms experimentally exponential, but hard to determine exactly what exponential.

Analysis of the YZ Quantum Algorithm with Multivariate Polynomial Systems

The Prior Algorithmic Framework

[Yamakawa-Zhandry '22, Regev '05]

- A standard measurement of a quantum state

$$|\phi\rangle = \sum_{\mathbf{x}\in\mathbb{F}^n} V(\mathbf{x}) \cdot |\mathbf{x}\rangle$$

observes $\mathbf{x}$ with probability $|V(\mathbf{x})|^2$ where $V : \{0,1\}^n \to \mathbb{C}$.

The Prior Algorithmic Framework

[Yamakawa-Zhandry '22, Regev '05]

- A standard measurement of a quantum state

$$|\phi\rangle = \sum_{\mathbf{x}\in\mathbb{F}^n} V(\mathbf{x}) \cdot |\mathbf{x}\rangle$$

observes $\mathbf{x}$ with probability $|V(\mathbf{x})|^2$ where $V : \{0,1\}^n \to \mathbb{C}$.

- Define

$$|\psi\rangle = \sum_{\mathbf{y}\in\mathbb{F}^N} W(\mathbf{y}) \cdot |\mathbf{y}\rangle.$$

- **Using $|\phi\rangle, |\psi\rangle$, can we produce their coordinate-wise product? i.e.**

$$\sum_{\mathbf{x}\in\mathbb{F}^N} (V \cdot W)(\mathbf{x}) \cdot |\mathbf{x}\rangle.$$

The Prior Algorithmic Framework

[Yamakawa-Zhandry '22, Regev '05]

- A standard measurement of a quantum state

$$|\phi\rangle = \sum_{\mathbf{x}\in\mathbb{F}^n} V(\mathbf{x}) \cdot |\mathbf{x}\rangle$$

observes $\mathbf{x}$ with probability $|V(\mathbf{x})|^2$ where $V : \{0,1\}^n \to \mathbb{C}$.

- Define

$$|\psi\rangle = \sum_{\mathbf{y}\in\mathbb{F}^N} W(\mathbf{y}) \cdot |\mathbf{y}\rangle.$$

- **Using $|\phi\rangle, |\psi\rangle$, can we produce their coordinate-wise product? i.e.**

$$\sum_{\mathbf{x}\in\mathbb{F}^N} (V \cdot W)(\mathbf{x}) \cdot |\mathbf{x}\rangle.$$

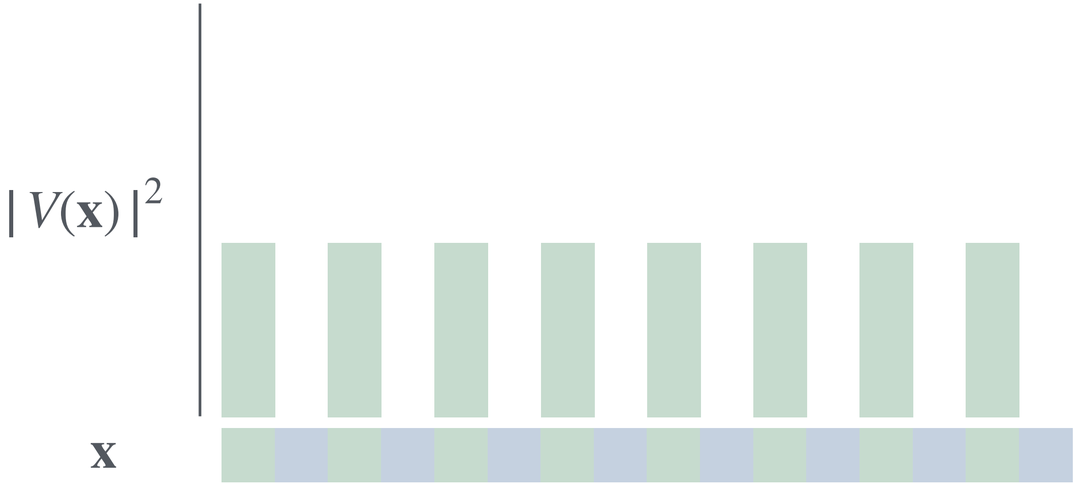
Their tensor contains undesired cross-terms:

$$|\phi\rangle|\psi\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} V(\mathbf{x})W(\mathbf{y}) \cdot |\mathbf{x}\rangle|\mathbf{y}\rangle.$$

The Coordinate-wise Product

- Let $|\phi\rangle$ be a uniform superposition over all codewords of the Generalized Reed-Solomon Code, so measuring this state results in a uniform random codeword, i.e.

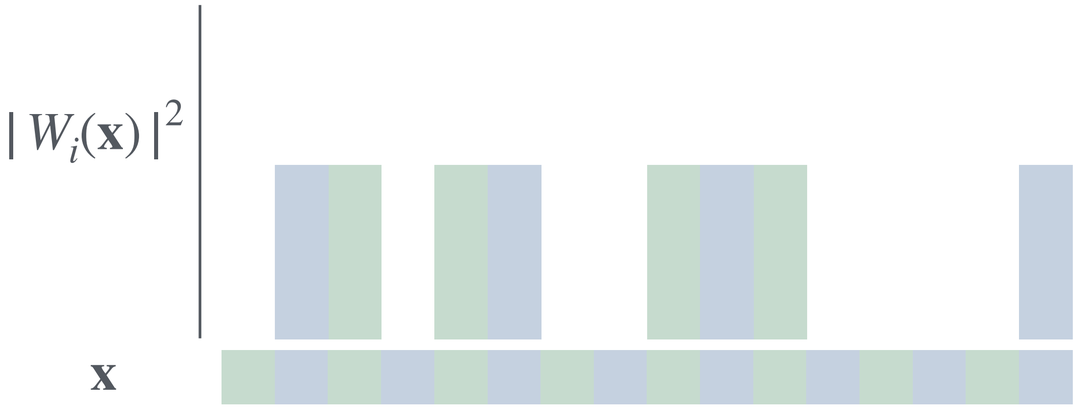
$$|\phi\rangle = \sum_{\mathbf{x}\in\mathbb{F}^N} V(\mathbf{x}) \cdot |\mathbf{x}\rangle, \text{ where } V(\mathbf{x}) = \begin{cases} 1/\sqrt{|C|} & \mathbf{x} \in C \\ 0 & \mathbf{x} \notin C \end{cases}.$$



The Coordinate-wise Product

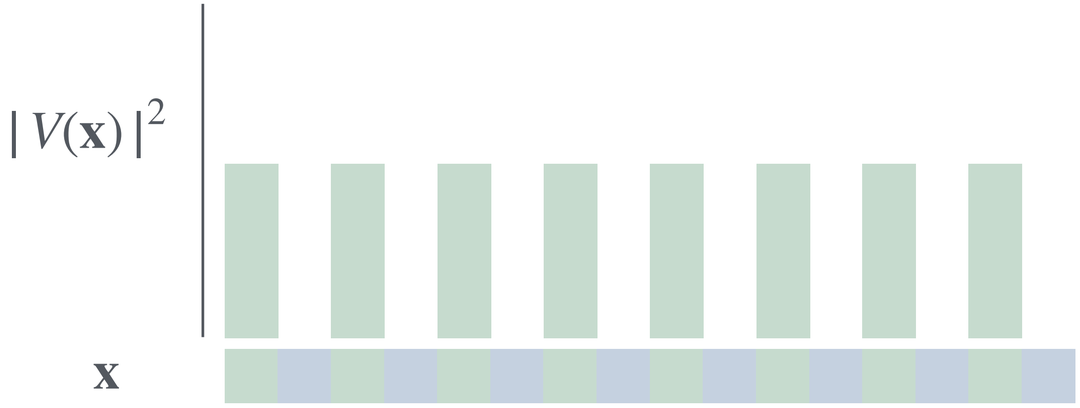
- Let $|\psi\rangle$ be a uniform superposition over all the roots of the degree d constraints, so measuring this state results in a uniform solution to the n^2 many polynomials p_i defined on disjoint variables. i.e. $|\psi\rangle = \bigotimes_{i=1}^{n^2} |\psi_i\rangle$ where for $i \in [n^2]$

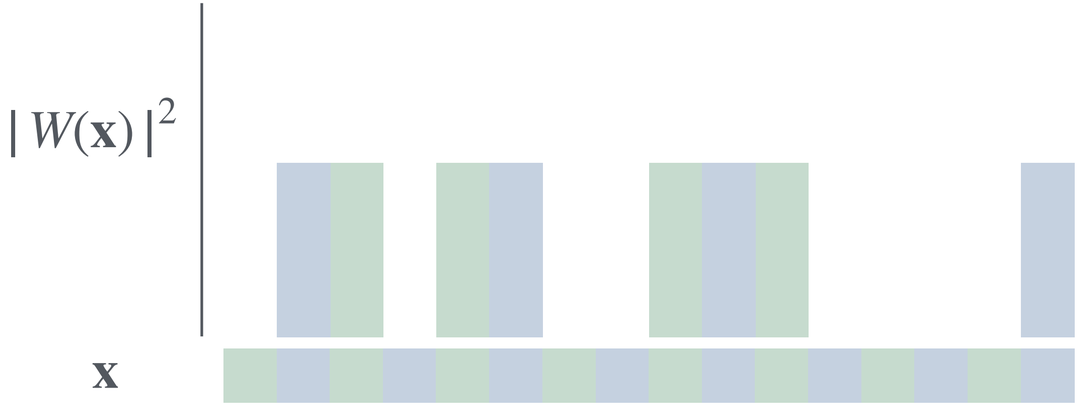
$$|\psi_i\rangle = \sum_{\mathbf{y} \in \mathbb{F}_2^n} W_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } W_i(\mathbf{y}) = \begin{cases} 1/\sqrt{|R_i|} & p_i(\mathbf{y}) = 0 \\ 0 & \text{o.w.} \end{cases}.$$



The Coordinate-wise Product

- Solving the polynomial system defined by the code constraint $\overline{\mathbf{H}} \cdot \mathbf{x} = \mathbf{0}$ and the random degree d polynomial system on disjoint variable blocks, $\{p_i\}_{i \in [n]}$, is exactly finding an $\mathbf{x}$ such that $V(\mathbf{x}) \neq 0$ AND $W(\mathbf{x}) \neq 0$.
- Therefore, **measuring the coordinate-wise product always gives us a solution to the polynomial system.**

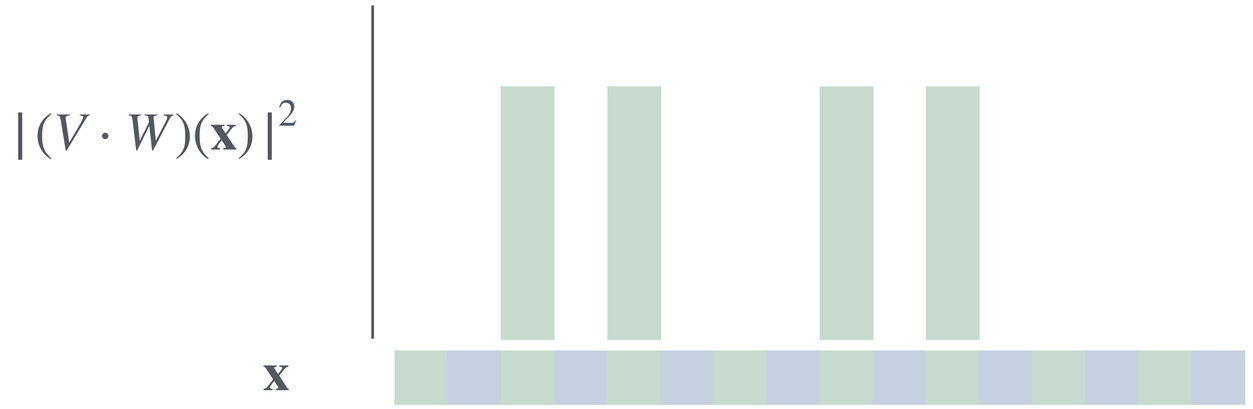




The Coordinate-wise Product

- Solving the polynomial system defined by the code constraint $\overline{\mathbf{H}} \cdot \mathbf{x} = \mathbf{0}$ and the random degree d polynomial system on disjoint variable blocks, $\{p_i\}_{i \in [n]}$, is exactly finding an $\mathbf{x}$ such that $V(\mathbf{x}) \neq 0$ AND $W(\mathbf{x}) \neq 0$.

- Therefore, **measuring the coordinate-wise product always gives us a solution to the polynomial system.**



The Prior Algorithmic Framework

Coordinate-wise Product <—> Convolution [Yamakawa-Zhandry '22, Regev '05]

$$\sum_{\mathbf{z}\in\mathbb{F}^N} (\hat{V} * \hat{W})(\mathbf{z}) \,|\, \mathbf{z}\rangle = \mathsf{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z}) \,|\, \mathbf{z}\rangle$$

The Prior Algorithmic Framework

Coordinate-wise Product <—> Convolution [Yamakawa-Zhandry '22, Regev '05]

- Define $|\hat{\phi}\rangle = \mathsf{QFT}\,|\phi\rangle, |\hat{\psi}\rangle = \mathsf{QFT}\,|\psi\rangle,$ so that

$$|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x}\rangle\,|\mathbf{y}\rangle.$$

The Prior Algorithmic Framework

Coordinate-wise Product <—> Convolution [Yamakawa-Zhandry '22, Regev '05]

- Define $|\hat{\phi}\rangle = \mathsf{QFT}\,|\phi\rangle, |\hat{\psi}\rangle = \mathsf{QFT}\,|\psi\rangle,$ so that

$$|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x}\rangle\,|\mathbf{y}\rangle.$$

- Apply a unitary addition to add the first register into the second register.

$$\mathbf{U}_{\mathsf{add}}\,|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x}\rangle\,|\mathbf{x}+\mathbf{y}\rangle$$

The Prior Algorithmic Framework

Coordinate-wise Product <—> Convolution [Yamakawa-Zhandry '22, Regev '05]

- Define $|\hat{\phi}\rangle = \mathsf{QFT}\,|\phi\rangle, |\hat{\psi}\rangle = \mathsf{QFT}\,|\psi\rangle,$ so that

$$|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x}\rangle\,|\mathbf{y}\rangle.$$

- Apply a unitary addition to add the first register into the second register.

$$\mathbf{U}_{\mathsf{add}}\,|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x}\rangle\,|\mathbf{x}+\mathbf{y}\rangle$$

- **Wishful thinking:** If we could *uncompute* the first register, the resulting state would be

$$\sum_{\mathbf{z}\in\mathbb{F}^N} (\hat{V} * \hat{W})(\mathbf{z})\,|\mathbf{z}\rangle = \mathsf{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z})\,|\mathbf{z}\rangle$$

from which we could obtain our desired coordinate-wise product state by inverting the QFT.

The Prior Algorithmic Framework

Coordinate-wise Product <—> Convolution [Yamakawa-Zhandry '22, Regev '05]

- Define $|\hat{\phi}\rangle = \mathsf{QFT}\,|\phi\rangle, |\hat{\psi}\rangle = \mathsf{QFT}\,|\psi\rangle,$ so that

$$|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x}\rangle\,|\mathbf{y}\rangle.$$

- Apply a unitary addition to add the first register into the second register.

$$\mathbf{U}_{\mathsf{add}}\,|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y})\,|\mathbf{x}\rangle\,|\mathbf{x}+\mathbf{y}\rangle \to |\mathbf{0}\rangle$$

- **Wishful thinking:** If we could *uncompute* the first register, the resulting state would be

$$\sum_{\mathbf{z}\in\mathbb{F}^N} (\hat{V} * \hat{W})(\mathbf{z})\,|\mathbf{z}\rangle = \mathsf{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z})\,|\mathbf{z}\rangle$$

from which we could obtain our desired coordinate-wise product state by inverting the QFT.

Main Question:
How do you *uncompute* the first register?

The Prior Algorithmic Framework

Coordinate-wise Product <—> Convolution [Yamakawa-Zhandry '22, Regev '05]

- Define $|\hat{\phi}\rangle = \mathsf{QFT}\,|\phi\rangle, |\hat{\psi}\rangle = \mathsf{QFT}\,|\psi\rangle,$ so that

$$|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x}\rangle\,|\mathbf{y}\rangle.$$

- Apply a unitary addition to add the first register into the second register.

$$\mathbf{U}_{\mathsf{add}}\,|\hat{\phi}\rangle\,|\hat{\psi}\rangle = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y})\,|\mathbf{x}\rangle\,|\mathbf{x}+\mathbf{y}\rangle \to |\mathbf{0}\rangle$$

- **Wishful thinking:** If we could *uncompute* the first register, the resulting state would be

$$\sum_{\mathbf{z}\in\mathbb{F}^N} (\hat{V} * \hat{W})(\mathbf{z})\,|\mathbf{z}\rangle = \mathsf{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z})\,|\mathbf{z}\rangle$$

from which we could obtain our desired coordinate-wise product state by inverting the QFT.

Main Question:
How do you *uncompute* the first register?

YZ'22: Treat $\mathbf{y}$ as noise and decode a noisy codeword $\mathbf{x}+\mathbf{y}$.

The Quantum Algorithm

1. Prepare uniform superposition over codewords $|\phi\rangle = \sum_{\mathbf{x}\in\mathbb{F}^N} V(\mathbf{x}) \cdot |\mathbf{x}\rangle$ and over roots of each polynomial $|\psi_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} W_i(\mathbf{y}) \cdot |\mathbf{y}\rangle$ for $i \in [n^2]$. Let $|\psi\rangle = \otimes_i |\psi_i\rangle$.

2. Compute $\left(\left(I \otimes \mathrm{QFT}^{-1}\right) \circ \mathbf{U}_{\mathsf{Decode}} \circ \mathbf{U}_{\mathsf{add}}\right)(\mathrm{QFT}|\phi\rangle \otimes \mathrm{QFT}|\psi\rangle)$.

3. Output measurement of the second register.

The Quantum Algorithm

1. Prepare uniform superposition over codewords $|\phi\rangle = \sum_{\mathbf{x}\in\mathbb{F}^N} V(\mathbf{x}) \cdot |\mathbf{x}\rangle$ and over roots of each polynomial $|\psi_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} W_i(\mathbf{y}) \cdot |\mathbf{y}\rangle$ for $i \in [n^2]$. Let $|\psi\rangle = \otimes_i |\psi_i\rangle$.
2. Compute $\left(\left(I \otimes \mathrm{QFT}^{-1}\right) \circ \mathbf{U}_{\mathrm{Decode}} \circ \mathbf{U}_{\mathrm{add}}\right)(\mathrm{QFT}|\phi\rangle \otimes \mathrm{QFT}|\psi\rangle)$. Let's look at this!
3. Output measurement of the second register.

Two Technical Challenges

We have that

$$\left(\mathbf{U}_{\mathsf{Decode}} \circ \mathbf{U}_{\mathsf{add}}\right)(\mathsf{QFT}\,|\phi\rangle \otimes \mathsf{QFT}\,|\psi\rangle) = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x} - \mathsf{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle\,|\mathbf{x}+\mathbf{y}\rangle$$

Crux: We want to show decoding almost always succeeds!

1. For what average-case error distributions can we *uniquely* decode?

2. What error distribution is induced by a uniform distribution over the root set of multivariate polynomials over disjoint variables?

Two Technical Challenges

We have that

$$\left(\mathbf{U}_{\mathsf{Decode}} \circ \mathbf{U}_{\mathsf{add}}\right)(\mathsf{QFT}\,|\phi\rangle \otimes \mathsf{QFT}\,|\psi\rangle) = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x} - \mathsf{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle\,|\mathbf{x}+\mathbf{y}\rangle$$

Crux: We want to show decoding almost always succeeds!

1. For what average-case error distributions can we *uniquely* decode?

Generic coding question.

2. What error distribution is induced by a uniform distribution over the root set of multivariate polynomials over disjoint variables?

Specific to our polynomial system.

$$\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x} - \mathrm{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle |\mathbf{x}+\mathbf{y}\rangle \approx \sum_{\mathbf{x},\mathbf{y},\ \text{decodable}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{0}\rangle |\mathbf{x}+\mathbf{y}\rangle$$

$$\approx |\mathbf{0}\rangle \otimes \mathrm{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z}) |\mathbf{z}\rangle$$

$$\mathscr{B} \triangleq \{\mathbf{e} \in \mathbb{F}_{2^n}^{n^3} : \exists \mathbf{x} \in C^\perp,\ \mathrm{Decode}_{C^\perp}(\mathbf{x}+\mathbf{e}) \neq \mathbf{x}\}$$

$$\sum_{\mathbf{e}\in\mathscr{B}} \left|\hat{W}(\mathbf{e})\right|^2 \leq \mathrm{negl}(n)$$

$$\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x} - \mathrm{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle |\mathbf{x}+\mathbf{y}\rangle \approx \sum_{\mathbf{x},\mathbf{y},\ \text{decodable}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{0}\rangle |\mathbf{x}+\mathbf{y}\rangle$$

$$\approx |\mathbf{0}\rangle \otimes \mathrm{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z}) |\mathbf{z}\rangle$$

$$\mathscr{B} \triangleq \{\mathbf{e} \in \mathbb{F}_{2^n}^{n^3} : \exists \mathbf{x} \in C^\perp,\ \mathrm{Decode}_{C^\perp}(\mathbf{x}+\mathbf{e}) \neq \mathbf{x}\}$$

$$\sum_{\mathbf{e}\in\mathscr{B}} \left|\hat{W}(\mathbf{e})\right|^2 \leq \mathrm{negl}(n)$$

probability mass on a bad error e.

$$\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\,\mathbf{x} - \mathsf{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle\,|\,\mathbf{x}+\mathbf{y}\rangle \overset{1}{\approx} \sum_{\mathbf{x},\mathbf{y},\ \text{decodable}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\,\mathbf{0}\rangle\,|\,\mathbf{x}+\mathbf{y}\rangle$$

$$\overset{2}{\approx} |\,\mathbf{0}\rangle \otimes \mathsf{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V\cdot W)(\mathbf{z})\,|\,\mathbf{z}\rangle$$

$$\mathscr{B} \triangleq \{\mathbf{e} \in \mathbb{F}_{2^n}^{n^3} : \exists \mathbf{x} \in C^\perp,\ \mathsf{Decode}_{C^\perp}(\mathbf{x}+\mathbf{e}) \neq \mathbf{x}\}$$

1. $$\sum_{\mathbf{e}\in\mathscr{B}} \left|\hat{W}(\mathbf{e})\right|^2 \leq \mathsf{negl}(n)$$

2. $$\sum_{\mathbf{z}\in\mathbb{F}_2^n} \left| \sum_{(\mathbf{x},\mathbf{z}-\mathbf{x})\in\mathsf{BAD}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{z}-\mathbf{x}) \right|^2 \leq \mathsf{negl}(n)$$

$$\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x} - \mathsf{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle |\mathbf{x}+\mathbf{y}\rangle \overset{1}{\approx} \sum_{\mathbf{x},\mathbf{y},\ \text{decodable}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{0}\rangle |\mathbf{x}+\mathbf{y}\rangle$$

$$\overset{2}{\approx} |\mathbf{0}\rangle \otimes \mathsf{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z}) |\mathbf{z}\rangle$$

$$\mathscr{B} \triangleq \{\mathbf{e} \in \mathbb{F}_{2^n}^{n^3} : \exists \mathbf{x} \in C^\perp,\ \mathsf{Decode}_{C^\perp}(\mathbf{x}+\mathbf{e}) \neq \mathbf{x}\}$$

(1) $$\sum_{\mathbf{e}\in\mathscr{B}} \left|\hat{W}(\mathbf{e})\right|^2 \leq \mathsf{negl}(n)$$

(2) ? $$\sum_{\mathbf{z}\in\mathbb{F}_2^n} \left| \sum_{(\mathbf{x},\mathbf{z}-\mathbf{x})\in\mathsf{BAD}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{z}-\mathbf{x}) \right|^2 \leq \mathsf{negl}(n)$$

$$= \begin{cases} |C^\perp|^{-1/2} & \text{if } \mathbf{x} \in C \\ 0 & \text{o.w.} \end{cases}$$

$$\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x} - \mathsf{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle |\mathbf{x}+\mathbf{y}\rangle \overset{(1)}{\approx} \sum_{\mathbf{x},\mathbf{y},\ \text{decodable}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{0}\rangle |\mathbf{x}+\mathbf{y}\rangle$$

$$\overset{(2)}{\approx} |\mathbf{0}\rangle \otimes \mathrm{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V\cdot W)(\mathbf{z}) |\mathbf{z}\rangle$$

$$\mathscr{B} \triangleq \{\mathbf{e} \in \mathbb{F}_{2^n}^{n^3} : \exists \mathbf{x} \in C^\perp,\ \mathsf{Decode}_{C^\perp}(\mathbf{x}+\mathbf{e}) \neq \mathbf{x}\}$$

(1) $\sum_{\mathbf{e}\in\mathscr{B}} \left|\hat{W}(\mathbf{e})\right|^2 \leq \mathrm{negl}(n)$ $\overset{?}{\Longrightarrow}$ (2) $\sum_{\mathbf{z}\in\mathbb{F}_2^n} \left| \sum_{(\mathbf{x},\mathbf{z}-\mathbf{x})\in\mathsf{BAD}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{z}-\mathbf{x}) \right|^2 \leq \mathrm{negl}(n)$

? Δ-inequality ?

$= \begin{cases} |C^\perp|^{-1/2} & \text{if } \mathbf{x}\in C \\ 0 & \text{o.w.} \end{cases}$

$$\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x} - \mathsf{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle |\mathbf{x}+\mathbf{y}\rangle \overset{(1)}{\approx} \sum_{\mathbf{x},\mathbf{y},\ \text{decodable}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{0}\rangle |\mathbf{x}+\mathbf{y}\rangle$$

$$\overset{(2)}{\approx} |\mathbf{0}\rangle \otimes \mathrm{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V\cdot W)(\mathbf{z}) |\mathbf{z}\rangle$$

$$\mathscr{B} \triangleq \{\mathbf{e} \in \mathbb{F}_{2^n}^{n^3} : \exists \mathbf{x} \in C^\perp,\ \mathsf{Decode}_{C^\perp}(\mathbf{x}+\mathbf{e}) \neq \mathbf{x}\}$$

(1) $\sum_{\mathbf{e}\in\mathscr{B}} \left|\hat{W}(\mathbf{e})\right|^2 \leq \mathrm{negl}(n)$ $\overset{?}{\Longrightarrow}$ (2) $\sum_{\mathbf{z}\in\mathbb{F}_2^n} \left| \sum_{(\mathbf{x},\mathbf{z}-\mathbf{x})\in\mathsf{BAD}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{z}-\mathbf{x}) \right|^2 \leq \mathrm{negl}(n)$

? Δ-inequality ?

$= \begin{cases} |C^\perp|^{-1/2} & \text{if } \mathbf{x}\in C \\ 0 & \text{o.w.} \end{cases}$

$$\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x} - \mathsf{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle |\mathbf{x}+\mathbf{y}\rangle \overset{(1)}{\approx} \sum_{\mathbf{x},\mathbf{y},\ \text{decodable}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{0}\rangle |\mathbf{x}+\mathbf{y}\rangle$$

$$\overset{(2)}{\approx} |\mathbf{0}\rangle \otimes \mathsf{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V\cdot W)(\mathbf{z}) |\mathbf{z}\rangle$$

$$\mathscr{B} \triangleq \{\mathbf{e} \in \mathbb{F}_{2^n}^{n^3} : \exists \mathbf{x} \in C^\perp,\ \mathsf{Decode}_{C^\perp}(\mathbf{x}+\mathbf{e}) \neq \mathbf{x}\}$$

(1) $$\sum_{\mathbf{e}\in\mathscr{B}} \left|\hat{W}(\mathbf{e})\right|^2 \leq \mathsf{negl}(n)$$

$\not\Rightarrow$ (Δ-ineq.)

(2) $$\sum_{\mathbf{z}\in\mathbb{F}_2^n} \left| \sum_{(\mathbf{x},\mathbf{z}-\mathbf{x})\in\mathsf{BAD}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{z}-\mathbf{x}) \right|^2 \leq \mathsf{negl}(n)$$

e.g. $|a|^2 + |b|^2 \lesssim |a+b|^2$

$$\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\,\mathbf{x} - \mathsf{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle\,|\,\mathbf{x}+\mathbf{y}\rangle \overset{(1)}{\approx} \sum_{\mathbf{x},\mathbf{y},\ \text{decodable}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\,\mathbf{0}\rangle\,|\,\mathbf{x}+\mathbf{y}\rangle$$

$$\overset{(2)}{\approx} |\,\mathbf{0}\rangle \otimes \mathsf{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V\cdot W)(\mathbf{z})\,|\,\mathbf{z}\rangle$$

$$\mathscr{B} \triangleq \{\mathbf{e} \in \mathbb{F}_{2^n}^{n^3} : \exists \mathbf{x} \in C^\perp,\ \mathsf{Decode}_{C^\perp}(\mathbf{x}+\mathbf{e}) \neq \mathbf{x}\}$$

(1) $$\sum_{\mathbf{e}\in\mathscr{B}} \left|\hat{W}(\mathbf{e})\right|^2 \leq \mathsf{negl}(n)$$

$\Longrightarrow$ + shift-invariance

(2) $$\sum_{\mathbf{z}\in\mathbb{F}_2^n} \left| \sum_{(\mathbf{x},\mathbf{z}-\mathbf{x})\in\mathsf{BAD}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{z}-\mathbf{x}) \right|^2 \leq \mathsf{negl}(n)$$

$$\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\,\mathbf{x} - \mathsf{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle\,|\,\mathbf{x}+\mathbf{y}\rangle \approx \sum_{\mathbf{x},\mathbf{y},\ \text{decodable}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\,\mathbf{0}\rangle\,|\,\mathbf{x}+\mathbf{y}\rangle$$

$$\approx |\,\mathbf{0}\rangle \otimes \mathsf{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V\cdot W)(\mathbf{z})\,|\,\mathbf{z}\rangle$$

$$\mathscr{B} \triangleq \{\mathbf{e} \in \mathbb{F}_{2^n}^{n^3} : \exists \mathbf{x} \in C^\perp,\ \mathsf{Decode}_{C^\perp}(\mathbf{x}+\mathbf{e}) \neq \mathbf{x}\}$$

$$\sum_{\mathbf{e}\in\mathscr{B}} \left|\hat{W}(\mathbf{e})\right|^2 \leq \mathsf{negl}(n)$$

$$\sum_{\mathbf{z}\in\mathbb{F}_2^n} \left| \sum_{(\mathbf{x},\mathbf{z}-\mathbf{x})\in\mathsf{BAD}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{z}-\mathbf{x}) \right|^2 \leq \mathsf{negl}(n)$$

Current focus. Proof in two step process...

1. Uniquely Decodable Error Distributions

Folded Reed-Solomon Codes

YZ'22: Burst error distributions with the following property are uniquely decodable:

$$\text{for all } i \in [n^2],\ \mathbf{e}_i = \begin{cases} \mathbf{0} & \text{w.p. } 1/2 \\ \mathsf{Unif}(\mathbb{F}_2^n \backslash \mathbf{0}) & \text{w.p. } 1/2 \end{cases}.$$

No reason that a root set of uniform random degree d polynomials would induce such an error distribution.

1. Uniquely Decodable Error Distributions

Folded Reed-Solomon Codes

YZ'22: Burst error distributions with the following property are uniquely decodable:

$$\text{for all } i \in [n^2],\ \mathbf{e}_i = \begin{cases} \mathbf{0} & \text{w.p. } 1/2 \\ \mathsf{Unif}(\mathbb{F}_2^n \backslash \mathbf{0}) & \text{w.p. } 1/2 \end{cases}.$$

Our work: observes the YZ proof of the above extends to *any* burst error distributions where blocks are $\mathbf{0}$ w.p. $1/2$, and takes on any point in $\mathbb{F}_2^n \backslash \{\mathbf{0}\}$ w.p. $2^{-\Omega(n)}$ i.e. high min-entropy.

1. Uniquely Decodable Error Distributions

Folded Reed-Solomon Codes

YZ'22: Burst error distributions with the following property are uniquely decodable:

$$\text{for all } i \in [n^2],\ \mathbf{e}_i = \begin{cases} \mathbf{0} & \text{w.p. } 1/2 \\ \mathsf{Unif}(\mathbb{F}_2^n \backslash \mathbf{0}) & \text{w.p. } 1/2 \end{cases}.$$

Our work: observes the YZ proof of the above extends to *any* burst error distributions where blocks are $\mathbf{0}$ w.p. $1/2$, and takes on any point in $\mathbb{F}_2^n \backslash \{\mathbf{0}\}$ w.p. $2^{-\Omega(n)}$ i.e. high min-entropy.

The question remains: does our uniform random polynomial distribution induce such a distribution?

1. Uniquely Decodable Error Distributions

Folded Reed-Solomon Codes

YZ'22: Burst error distributions with the following property are uniquely decodable:

$$\text{for all } i \in [n^2],\ \mathbf{e}_i = \begin{cases} \mathbf{0} & \text{w.p. } 1/2 \\ \mathsf{Unif}(\mathbb{F}_2^n \backslash \mathbf{0}) & \text{w.p. } 1/2 \end{cases}.$$

Our work: observes the YZ proof of the above extends to *any* burst error distributions where blocks $\mathbf{0}$ are probability $1/2$, and have probability mass $2^{-\Omega(n)}$ on any point in $\mathbb{F}_2^n \backslash \{\mathbf{0}\}$, i.e. high min-entropy.

Yes! In fact, holds for any 2-wise indep. distribution on polynomials.

2. Distribution Induced by Root Sets are Uniquely Decodable

$$|\psi_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} W_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } W_i(\mathbf{y}) = \begin{cases} 1/\sqrt{|R_i|} & p_i(\mathbf{y}) = 0 \\ 0 & \text{o.w.} \end{cases}.$$

2. Distribution Induced by Root Sets are Uniquely Decodable

$$|\psi_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} W_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } W_i(\mathbf{y}) = \begin{cases} 1/\sqrt{|R_i|} & p_i(\mathbf{y}) = 0 \\ 0 & \text{o.w.} \end{cases}.$$

$$|\hat{\psi}_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} \hat{W}_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } \hat{W}_i(\mathbf{y}) = 2^{-n/2} \cdot \sum_{\mathbf{z}\in\mathbb{F}_2^n} W_i(\mathbf{z}) \cdot (-1)^{\mathbf{y}\cdot\mathbf{z}}.$$

2. Distribution Induced by Root Sets are Uniquely Decodable

$$|\psi_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} W_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } W_i(\mathbf{y}) = \begin{cases} 1/\sqrt{|R_i|} & p_i(\mathbf{y}) = 0 \\ 0 & \text{o.w.} \end{cases}.$$

$$|\hat{\psi}_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} \hat{W}_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } \hat{W}_i(\mathbf{y}) = 2^{-n/2} \cdot \sum_{\mathbf{z}\in\mathbb{F}_2^n} W_i(\mathbf{z}) \cdot (-1)^{\mathbf{y}\cdot\mathbf{z}}.$$

What is the distribution over $\mathbb{F}_2^n$ defined by the probability mass function: $\mathbb{E}_{p_i}\left[\|\hat{W}_i(\,\cdot\,)\|^2\right]$?

(why? By Markov, with all but negl. prob. over p_i, almost all mass on GOOD)

2. Distribution Induced by Root Sets are Uniquely Decodable

$$|\hat{\psi}_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} \hat{W}_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } \hat{W}_i(\mathbf{y}) = 2^{-n/2} \cdot \sum_{\mathbf{z}\in\mathbb{F}_2^n} W_i(\mathbf{z}) \cdot (-1)^{\mathbf{y}\cdot\mathbf{z}}.$$

Easy observation: $\mathbb{E}_{p_i}\left[\|\hat{W}_i(\mathbf{0})\|^2\right] = 2^{-n} \cdot \mathbb{E}_{p_i}\left[|R_i|\right] = \frac{1}{2}.$

Due to the 1-wise independence of random inhomogeneous degree d polynomials:

$$\forall \mathbf{y} \in \mathbb{F}_2^n, \text{ we have } \mathbb{E}_{p_i}[\mathbb{I}_{\mathbf{y}}(p_i)] = 1/2.$$

2. Distribution Induced by Root Sets are Uniquely Decodable

$$|\hat{\psi}_i\rangle = \sum_{\mathbf{y}\in\mathbb{F}_2^n} \hat{W}_i(\mathbf{y}) \cdot |\mathbf{y}\rangle \text{ where } \hat{W}_i(\mathbf{y}) = 2^{-n/2} \cdot \sum_{\mathbf{z}\in\mathbb{F}_2^n} W_i(\mathbf{z}) \cdot (-1)^{\mathbf{y}\cdot\mathbf{z}}.$$

Easy observation: $\mathbb{E}_{p_i}\left[\|\hat{W}_i(\mathbf{0})\|^2\right] = 2^{-n} \cdot \mathbb{E}_{p_i}\left[|R_i|\right] = \frac{1}{2}$.

Due to the 1-wise independence of random inhomogeneous degree d polynomials:

$$\forall \mathbf{y} \in \mathbb{F}_2^n, \text{ we have } \mathbb{E}_{p_i}[\mathbb{I}_{\mathbf{y}}(p_i)] = 1/2.$$

2. Distribution Induced by Root Sets are Uniquely Decodable

For all $\mathbf{y} \in \mathbb{F}_2^n \backslash \{\mathbf{0}\}, n \geq 10$, we can show that

$$\mathbb{E}_p \left[\|\hat{W}_i(\mathbf{y})\|^2 \right] \leq 2^{-n/2} \text{ (Property 2) .}$$

2-wise independence of random inhomogeneous degree d polynomials => Property 2.

$\forall \mathbf{x} \neq \mathbf{y} \in \mathbb{F}_2^n$, we have $\mathbb{E}_{p_i}[\mathbb{I}_{\mathbf{x}}(p_i) \cdot \mathbb{I}_{\mathbf{y}}(p_i)] = 1/4$.

2. Distribution Induced by Root Sets are Uniquely Decodable

For all $\mathbf{y} \in \mathbb{F}_2^n \backslash \{\mathbf{0}\}, n \geq 10$, we can show that

$$\mathbb{E}_p \left[\|\hat{W}_i(\mathbf{y})\|^2 \right] \leq 2^{-n/2} \text{ (Property 2) .}$$

To do so, we can express the Fourier coefficient for all $\mathbf{y} \neq \mathbf{0}$ as

$$\hat{W}_i(\mathbf{y}) = 2^{-n/2} |R_i|^{-1/2} \cdot \sum_{\mathbf{z} \in \mathbb{F}_2^n} (-1)^{p_i(\mathbf{z}) + \langle \mathbf{y}', \mathbf{z} \rangle_2}$$

Effectively, need to consider the behavior of the root set of p_i shifted by linear polynomials.

2. Distribution Induced by Root Sets are Uniquely Decodable

$$\mathbb{E}_p\left[\|\hat{W}_i(\mathbf{0})\|^2\right] = \frac{1}{2} \text{ (Property 1)}$$

For all $\mathbf{y} \in \mathbb{F}_2^n \backslash \{\mathbf{0}\}, n \geq 10$, we have $\mathbb{E}_p\left[\|\hat{W}_i(\mathbf{y})\|^2\right] \leq 2^{-n/2}$ (Property 2).

Together, satisfy unique decodability from step 1.

$\therefore$ **Any** 2-wise independent distribution on $\mathbb{F}_2[x_1, \ldots, x_n]$ gives the above distribution.

Using Shift-invariance

$$\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}^N} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{x} - \mathsf{Decode}_{\mathbf{C}^\perp}(\mathbf{x}+\mathbf{y})\rangle |\mathbf{x}+\mathbf{y}\rangle \overset{(1)}{\approx} \sum_{\mathbf{x},\mathbf{y},\ \text{decodable}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{y}) \cdot |\mathbf{0}\rangle |\mathbf{x}+\mathbf{y}\rangle$$

$$\overset{(2)}{\approx} |\mathbf{0}\rangle \otimes \mathsf{QFT} \sum_{\mathbf{z}\in\mathbb{F}^N} (V \cdot W)(\mathbf{z}) |\mathbf{z}\rangle$$

$$\mathscr{B} \triangleq \{\mathbf{e} \in \mathbb{F}_{2^n}^{n^3} : \exists \mathbf{x} \in C^\perp,\ \mathsf{Decode}_{C^\perp}(\mathbf{x}+\mathbf{e}) \neq \mathbf{x}\}$$

(1) $\sum_{\mathbf{e}\in\mathscr{B}} \left|\hat{W}(\mathbf{e})\right|^2 \leq \mathsf{negl}(n)$ $\Longrightarrow$ (+ shift-invariance) (2) $\sum_{\mathbf{z}\in\mathbb{F}_2^n} \left| \sum_{(\mathbf{x},\mathbf{z}-\mathbf{x})\in\mathsf{BAD}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{z}-\mathbf{x}) \right|^2 \leq \mathsf{negl}(n)$

Using Shift-invariance

Exploiting symmetry!

Want to show: $$\sum_{\mathbf{z}\in\mathbb{F}_2^n} \left| \sum_{(\mathbf{x},\mathbf{z}-\mathbf{x})\in \mathsf{BAD}} \hat{V}(\mathbf{x})\hat{W}(\mathbf{z}-\mathbf{x}) \right|^2 \leq \mathsf{negl}(n)$$

Yamakawa-Zhandry: Uses some permutation-invariant property of random oracles.

Using Shift-invariance

Exploiting symmetry!

Want to show: $$\sum_{\mathbf{z}\in\mathbb{F}_2^n}\left|\sum_{(\mathbf{x},\mathbf{z}-\mathbf{x})\in\mathsf{BAD}}\hat{V}(\mathbf{x})\hat{W}(\mathbf{z}-\mathbf{x})\right|^2 \leq \mathsf{negl}(n)$$

Yamakawa-Zhandry: Uses some permutation-invariant property of random oracles.

We use **shift-invariance**:

A distribution $\mathscr{D}$ is **shift-invariant** if for all $\mathbf{s}\in\mathbb{F}_2^n$, the distribution $\mathscr{D}_{\mathbf{s}}$ where you sample a random $p\sim\mathscr{D}$ and then output $p_{\mathbf{s}}$ where $p_{\mathbf{s}}(\mathbf{x})=p(\mathbf{x}+\mathbf{s})$ is distributed identically to $\mathscr{D}$.

Concluding thoughts

- The quantum algorithm works for any shift-invariant, and 2-wise independent distribution over polynomials. Two examples:
  - Uniform random degree bounded polynomials for any $d \geq 2$.
  - Random high (poly in n) degree d, sparse (nonzero w.p. $1/n^{d-1}$) polynomials.
- **Recap:** First evidence of an efficiently quantumly invertible yet plausibly classically hard-to-invert polynomial system, and a non-oracle low-degree instantiation of YZ.

Further Thoughts

- Connections to complement sampling: Thanks to an anonymous SODA '26 reviewer who pointed out a simpler proof for correctness in the case of $\mathbb{F}_2$ using complement sampling [Benedetti-Buhrman-Weggemans '25].
  - Our results extend to larger finite fields, whereas this argument does not immediately extend (complement set of $H^{-1}(1)$ would no longer be $H^{-1}(0)$).
- Further classical cryptanalysis on this polynomial system.
- **Main question for future work:** Can we find other interesting instantiations of the R.O.?

Thank you!