THE RANK METHOD AND APPLICATIONS TO QUANTUM LOWER BOUNDS

Mark Zhandry

Joint work with Dan Boneh
This Talk

Highlight technique from very recent paper:

*Quantum-Secure Message Authentication Codes*

Specifically:

- Quantum Oracle Interrogation
- The Rank Method
- Quantum Polynomial Interpolation
Quantum Oracle Interrogation

Adversary wins if:

\[ H(x_i) = y_i \forall i \]
\[ x_i \neq x_j \forall i \neq j \]
Previously Known

If $q \geq k$, can win (efficiently) with probability 1
   $\rightarrow$ Can always resort to classical queries

What if $q < k$?
   Adversary sees superposition of all input/output pairs
   $\rightarrow$ No value is perfectly hidden from adversary

Only non-trivial result: if $|Y|=2$ and $q \geq k/2$, can win efficiently with probability close to 1 [vD98]

Existing lower-bound techniques fail
   $\rightarrow$ Need new lower bound technique
Quantum Computation

Quantum system: N-dimensional complex Hilbert space
Quantum state: unit vector $|\psi\rangle$

Measurement:
- Relative to some orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$
- Probability outcome is $i$: $|\langle i | \psi \rangle|^2$
  - Same as length squared of projection of $|\psi\rangle$ onto $|i\rangle$
The Setup

Value $z$ drawn from distribution $D$ on set $Z$

Quantum adversary $A$:
- Given “access” to $z$
- Produces final state $|\psi_z\rangle$
- State is measured to obtain $w$

$A$ tries to achieve some goal $G$
Example: Oracle Interrogation

“Access” means \( q \) quantum queries, \( H \) random oracle

Goal: produce \( (x_1, \ldots, x_k, y_1, \ldots, y_k, s) \) such that \( x_i \) are distinct and \( y_i = H(x_i) \) for all \( i \)

\[
|\psi_H\rangle
\]
The Rank

Let $\Psi_{A,Z}$ be the matrix whose row vectors are the different $|\psi_z\rangle$ vectors.

The **Rank** of $A$ is the rank of the matrix $\Psi_{A,Z}$

- Same* as the rank of the density matrix

\[
\rho = \sum_{\tilde{z}} \Pr[z \leftarrow D]|\psi_{\tilde{z}}\rangle\langle\psi_{\tilde{z}}|
\]

- Same as dimension of subspace spanned by the $|\psi_z\rangle$
The Rank Method

Knowing nothing but the rank of A, get good bounds on success probability

Toy example:
- Z is the set {0,1,2}
- D is the uniform distribution on Z
- Goal: output z
- Rank = 1, 2, 3
Rank = 1

$|\psi_z\rangle$ independent* of $z$

No matter what, win with probability $1/3$
Rank = 2

$|\psi_z\rangle$ depends on $z$, but still far from basis

Can show that in best case, win with probability is $2/3$
Rank = 3

No constraints on $|\psi_z\rangle$

If $|\psi_z\rangle = |z\rangle$, then win with probability 1
The Rank Method

**Theorem:** For any distribution $D$, goal $G$, the probability that a rank $r$ algorithm achieves $G$ is at most $r$ times the probability of achieving $G$ for the best rank 1 algorithm
Rank for Oracle Algorithms

**Theorem:** The rank of any algorithm making q queries to H: X→Y is at most

\[
C_{|X|, q, |Y|} = \sum_{t=0}^{q} \binom{|X|}{r} (|Y| - 1)^r \leq \binom{|X|}{q} |Y|^q
\]
Interrogating Random Functions

Say $q = k-1$

Best rank 1 algorithm:
- Arbitrarily pick $x$
- Randomly guess $y$
- Success probability: $1/|Y|^k$

Best $q$ query algorithm can do:

$$\frac{C_{|X|,q,|Y|}}{|Y|^k} \leq \frac{\binom{|X|}{q}|Y|^q}{|Y|^k} = \frac{\binom{|X|}{q}}{|Y|}$$

Can we do better?
Theorem: Let $|X| = m$, $|Y| = n$. Let $A$ be a quantum algorithm making $q$ queries to a random oracle $H$: $X \rightarrow Y$. The probability that $A$ can produce $k$ distinct input/output pairs is at most

$$\frac{C_{k,q,|Y|}}{|Y|^k} \leq \frac{\binom{k}{q}}{|Y|^{k-q}}$$

Moreover, there is an efficient* quantum algorithm that exactly achieves this bound.
The $q = k-1$ case

Best any quantum algorithm can do:

$$\frac{C_{k, k-1, |Y|}}{|Y|^k} \leq \frac{k}{|Y|}$$

For exponentially-large $|Y|$, impossible to save even one query

What about small (constant) $|Y|$?
Constant $|Y|$ (e.g. $|Y|=2$)

Using Chernoff bound, if $q/k > (1-1/|Y|)$,

$$
\frac{C_{k,q,|Y|}}{|Y|^k} > 1 - e^{-\frac{k}{2|Y|} \left(|Y| \frac{q}{k} - (|Y| - 1)\right)^2}
$$

Pick constant $c > 1-1/|Y|$. For $q = ck$, success probability is

$$
\frac{C_{k,q,|Y|}}{|Y|^k} > 1 - e^{-\frac{k|Y|}{2} \left(c - (1 - 1/|Y|)\right)^2}
$$

Which is exponentially close to 1, in $k$
Quantum Oracle Interrogation Summary

Exact characterization of success probability

For exponential $|Y|$, poly $k$, sharp threshold

For constant $|Y|$, constant-factor improvement in number of queries over classical case
Quantum Polynomial Interpolation

Adversary

\[ \sum_x \alpha_x |x\rangle \]

\[ \sum_x \alpha_x |x, f(x)\rangle \]

\[ f \leftarrow \text{Poly}(\mathbb{F}_n, d) \]

Goal: reconstruct f
Previously Known

If \( q \geq d+1 \), can interpolate \( f \) with probability 1
   \[ \rightarrow \] Just use classical queries

Existing lower bounds: If \( q \leq d/2 \), degree \( d \) coefficient completely hidden
   \[ \rightarrow \] need \( q \geq (d+1)/2 \) queries to interpolate

Large gap in knowledge
Using the Rank Method

Knowing polynomial same as knowing d+1 points
Best any rank 1 algorithm can do: $1/n^{d+1}$
Best any q query algorithm can do:

$$C_{n,q,n} \frac{n^{2q}}{q!n^{d+1}} = \frac{n^{2q-d-1}}{q!}$$

- $q=(d+1)/2$:

$$\frac{1}{[((d + 1)/2)!} \ll 1$$
Quantum Polynomial Interpolation

Summary

If \( q \geq d+1 \), can interpolate \( f \) with probability 1

\[ \rightarrow \] Just use classical queries

Rank method: need \( q > \frac{(d+1)}{2} \) for \( d > 1 \)
Quantum Polynomial Interpolation

Summary

If $q \geq d$, can interpolate $f$ with probability almost 1

- Using a single quantum query, a few QFTs
- Don’t know how to extend

Rank method: need $q > (d+1)/2$ for $d > 1$
Quantum Polynomial Interpolation

Summary

If $q \geq d$, can interpolate $f$ with probability almost 1

- Using a single quantum query, a few QFTs
- Don’t know how to extend

Rank method: need $q > (d+1)/2$ for $d > 1$

Open Questions:

- Closing the gap
- Is there a sharp threshold?