Quantum Computing

and

Locally Decodable Codes

Iordanis Kerenidis (UC Berkeley)

Ronald de Wolf (CWI Amsterdam)

Error-Correcting Codes

- Encoding $C : \{0,1\}^n \to \{0,1\}^m$, $m \geq n$
- Even if $C(x)$ is corrupted in δm positions, we can still recover the whole x
- We can achieve this with $m = O(n)$, linear-time encoding and decoding. $O(1)$ time per bit!
- Disadvantage: if you only want one bit x_i, you still need to decode the whole $C(x)$

Locally Decodable Codes

- Recover x_i with high probability, looking only at a few positions in the codeword

- $C : \{0,1\}^n \to \{0,1\}^m$ is a
  (q, δ, ε)-*locally decodable code* (LDC)
  if there exists a randomized decoder A
  such that for every $y \in \{0,1\}^m$ and $i \in [n]$

  1. $A^y(i)$ makes $\leq q$ queries to bits of y

  2. $d(y, C(x)) \leq \delta m \Rightarrow \Pr[A^y(i) = x_i] \geq 1/2 + \varepsilon$

- LQDCs: classical code, quantum queries

Example: Hadamard Code

- Define $C(x)_j = j \cdot x \bmod 2$ for all $j \in \{0,1\}^n$, so $m = 2^n$
- Example: $C(11) = 0110$
- Decode: pick random $j \in \{0,1\}^n$, query j and $j \oplus e_i$, output $y_j \oplus y_{j \oplus e_i}$
- Works perfectly if $y = C(x)$ (no noise)
- δ-corruption hits $C(x)_j$ or $C(x)_{j \oplus e_i}$ with probability $\leq 2\delta$, so

$$\Pr[A^y(i) = x_i] \geq 1 - 2\delta$$

What's Known About LDCs

Main question: tradeoff between q and m

- Upper bounds:

  $q = m$ $\Rightarrow$ $m \leq O(n)$ (standard ECC)
  $q = (\log n)^2$ $\Rightarrow$ $m \leq poly(n)$ (Babai et al)
  constant q $\Rightarrow$ $m \leq 2^{n^{c(q)}}$ (from PIR)

- Lower bounds:

  Katz-Trevisan 99:
  $q = 1$ $\Rightarrow$ LDCs don't exist
  $q > 1$ $\Rightarrow$ $m \geq n^{1+1/(q-1)}$

  GKST 02:
  $q = 2$, linear C $\Rightarrow$ $m \geq 2^{cn}, c = \delta\varepsilon/8$

- Our result:

  $q = 2 \Rightarrow m \geq 2^{cn}$ also for non-linear LDCs

Proof Uses Quantum!

- Step 1:

  2-query LDCs can be decoded
  with 1 quantum query:

  $(2, \delta, \varepsilon)$-LDC is $(1, \delta, 4\varepsilon/7)$-LQDC

- Step 2:

  $(1, \delta, \varepsilon)$-LQDC needs length $m \geq 2^{cn}$,

  for $c = 1 - H(1/2 + \delta\varepsilon/4) \approx (\delta\varepsilon)^2$

Step 1: From 2-LDC to 1-LQDC

Lemma: Any $f : \{0,1\}^2 \to \{0,1\}$ can be computed with 1 quantum query, with success probability exactly 11/14

- Query $\frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$
  $\Rightarrow |\phi\rangle = \frac{1}{\sqrt{3}}(|0\rangle + (-1)^{a_1}|1\rangle + (-1)^{a_2}|2\rangle)$

- Measure in 4-element basis $|\psi_{b_1 b_2}\rangle =$

$$\frac{1}{2}\Big(|0\rangle + (-1)^{b_1}|1\rangle + (-1)^{b_2}|2\rangle + (-1)^{b_1+b_2}|3\rangle\Big)$$

- Outcome $b_1 b_2$ equals $a_1 a_2$ with probability $|\langle\phi|\psi_{a_1 a_2}\rangle|^2 = 3/4$

- Base output on $b_1 b_2$ and truth table of f

Step 1 (cntd)

- Take 2-query classical decoder.
  Fix randomness $R \Rightarrow$ this fixes j, k, f s.t.

$$\Pr_R[f(y_j, y_k) = x_i] = p \geq 1/2 + \varepsilon$$

- Lemma: 1 quantum query gives success

$$\frac{11}{14}p + \frac{3}{14}(1-p) = \frac{3}{14} + \frac{4p}{7} \geq \frac{1}{2} + \frac{4\varepsilon}{7}$$

  Note: *exactly* 11/14 matters!

- This works for any x, y, i, hence
  a $(2, \delta, \varepsilon)$-LDC is a $(1, \delta, 4\varepsilon/7)$-LQDC

Step 2: Lower Bound for 1-LQDC

- Most general 1-query quantum decoder:
  - Apply query to $\sum_{j=1}^{m} \alpha_j |j\rangle$,
    α_j non-negative (depend on i)
  - Apply POVM with elements D and $I - D$,
    Pr[output 1 on $|\phi\rangle$] $= p(\phi) = \langle\phi|D|\phi\rangle$

- $A = \{j : \alpha_j \leq 1/\sqrt{\delta m}\}$ (small amplitudes)
  $a = \sqrt{\sum_{j \in A} \alpha_j^2}$
  $B = \{j : \alpha_j > 1/\sqrt{\delta m}\}$ (large amplitudes)
  Note $|B| \leq \delta m$

Step 2: small amplitude-part predicts x_i

- $|A(x)\rangle = \sum_{j \in A} \alpha_j (-1)^{C(x)_j} |j\rangle, \;\; |B\rangle = \sum_{j \in B} \alpha_j |j\rangle$

- States $|A(x)\rangle + |B\rangle$ and $|A(x)\rangle - |B\rangle$ are corrupted only in B ($\leq \delta m$ positions)

- If $x_i = 1$: $p(A(x) + B), p(A(x) - B) \geq \frac{1}{2} + \varepsilon$, hence $p(A(x)) + p(B) \geq 1/2 + \varepsilon$.

  If $x'_i = 0$: $p(A(x')) + p(B) \leq 1/2 - \varepsilon$

  $\Rightarrow \quad p(A(x)/a) - p(A(x')/a) \geq 2\varepsilon/a^2$

- Given $|A(x)\rangle/a$ we can determine x_i with probability $1/2 + \varepsilon/2a^2$

Step 2: get $|A(x)\rangle/a$ from uniform state

- $|U(x)\rangle = \frac{1}{\sqrt{m}} \sum_{j=1}^{m} (-1)^{C(x)_j} |j\rangle$, indep. of i

- Measure this with POVM M^*M, $I - M^*M$, where $M = \sqrt{\delta m} \sum_{j \in A} \alpha_j |j\rangle\langle j|$

- With prob $\delta a^2/2$: M turns $|U(x)\rangle$ into $|A(x)\rangle/a$
  Else: output a coin flip

  $\Pr[\text{output} = x_i] =$

  $$\underbrace{\frac{\delta a^2}{2}\left(\frac{1}{2} + \frac{\varepsilon}{2a^2}\right)}_{M \text{ succeeds}} + \underbrace{\left(1 - \frac{\delta a^2}{2}\right)\frac{1}{2}}_{M \text{ fails}} = \frac{1}{2} + \frac{\delta\varepsilon}{4} = p$$

- $|U(x)\rangle$ is a quantum random access code!

  $$\underbrace{\log m}_{\#\text{qubits of } U(x)} \geq \underbrace{(1 - H(p))n}_{\text{RAC bound (Nayak 99)}}$$

LQDCs are shorter than LDCs

- Best known $2q$-query LDCs (BIKR 02) output the XOR of the $2q$ bits

- Can do this with q quantum queries!

Queries	Length of LDC	Length of LQDC
$q = 1$	don't exist	$2^{\Theta(n)}$
$q = 2$	$2^{\Theta(n)}$	$2^{n^{3/10}}$
$q = 3$	$2^{n^{1/2}}$	$2^{n^{1/7}}$
$q = 4$	$2^{n^{3/10}}$	$2^{n^{1/11}}$

Private Information Retrieval

- User retrieves x_i from database x that is replicated over k non-communicating servers; individual server learns nothing about i

- How much communication is needed?

- 1-server PIR scheme needs $\Omega(n)$ bits, even quantum (Nayak 99)

- There is a 2-server PIR with $O(n^{1/3})$ bits (CGKS 95)

Lower Bound for Classical Binary PIR

- Binary PIR: servers send back only 1 bit
- Can reduce 2 binary classical servers to 1 quantum server (treat servers as queries)
- $\Omega(n)$ lower bound for 1-server quantum PIR
  $\Rightarrow$
  $\Omega(n)$ lower bound for 2-server binary PIR
- Previously known only for *linear* PIR

Upper Bound for Quantum PIR

- Best known $2k$-server binary PIRs (BIKR 02) output XOR of the $2k$ bits
- Can do this with k quantum servers
- Better than best known k-server PIRs!

Servers	PIR complexity	QPIR complexity
$k = 1$	n	n
$k = 2$	$n^{1/3}$	$n^{3/10}$
$k = 3$	$n^{1/5.25}$	$n^{1/7}$
$k = 4$	$n^{1/7.87}$	$n^{1/11}$

Summary

- Exponential lower bound for 2-query LDCs via a quantum proof
- q-query LQDCs are shorter than LDCs
- Linear lower bound for 2-server binary PIR
- Upper bound $O(n^{3/10})$ for 2-server QPIR

Future Work

- Extend lower bound to more than 2 queries
- Extend to $C(x)$ over non-binary alphabet