QUERY COMPLEXITY LOWER BOUNDS FOR LOCAL LIST-DECODING AND HARD-CORE PREDICATES

Noga Ron-Zewi  Ronen Shaltiel  Nithin Varma
Talk outline

- List decoding and local list decoding
Talk outline

■ List decoding and local list decoding
■ Our results and applications to blackbox proofs for hardcore predicates
Talk outline

- List decoding and local list decoding
- Our results and applications to blackbox proofs for hardcore predicates
- Lower bound argument based on a coin problem
Talk outline

- List decoding and local list decoding
- Our results and applications to blackbox proofs for hardcore predicates
- Lower bound argument based on a coin problem
- Open problems
List decodable and local list decodable codes

- Binary code $\text{Enc}: \{0,1\}^k \to \{0,1\}^n$ is $(\frac{1}{2} - \varepsilon, L)$-list decodable if  

$$\left(\frac{1}{2} - \varepsilon, L\right)$$ -list decodable

[Elias, Wozencraft 60's]
List decodable and local list decodable codes

- Binary code $\text{Enc}: \{0,1\}^k \rightarrow \{0,1\}^n$ is $(\frac{1}{2} - \varepsilon, L)$-list decodable if

  $\forall w \in \{0,1\}^n,$

  $\exists j \in [L]$ such that

  $m = m(j),$ and

  $\text{Decoder, on input } i \in k, j \in [L],$ makes $q$ queries to $w$ and outputs, with probability at least $1 - \delta,$

  $m_i(j),$ the $i$-th bit of message $m(j).$
List decodable and local list decodable codes

- Binary code $Enc: \{0,1\}^k \rightarrow \{0,1\}^n$ is $(\frac{1}{2} - \varepsilon, L)$-list decodable if $[Elias, Wozencraft 60's] \forall w \in \{0,1\}^n$, there are $\leq L$ messages $m$ such that $dist(Enc(m), w) \leq \left(\frac{1}{2} - \varepsilon\right) \cdot n$

$dist(x, y)$: Hamming distance between $x$ and $y$
List decodable and local list decodable codes

- Binary code $\text{Enc}: \{0,1\}^k \to \{0,1\}^n$ is $(\frac{1}{2} - \varepsilon, L)$-list decodable if $\forall w \in \{0,1\}^n$, there are $\leq L$ messages $m$ such that $\text{dist}(\text{Enc}(m), w) \leq \left(\frac{1}{2} - \varepsilon\right) \cdot n$

$\text{dist}(x, y)$: Hamming distance between $x$ and $y$

List of $\leq L$ messages whose encodings differ from $w$ in at most $\left(\frac{1}{2} - \varepsilon\right) n$ locations
List decodable and local list decodable codes

- Binary code $Enc: \{0,1\}^k \rightarrow \{0,1\}^n$ is $(\frac{1}{2} - \varepsilon, L)$-list decodable if

  \[ \forall w \in \{0,1\}^n, \text{there are } \leq L \text{ messages } m \]

  such that

  \[ \text{dist}(Enc(m), w) \leq \left(\frac{1}{2} - \varepsilon\right) \cdot n \]

$(\frac{1}{2} - \varepsilon, q, L)$-Locally List Decodable Code

- [Elias, Wozencraft 60's]
  - [Sudan, Trevisan, Vadhan 99]
List decodable and local list decodable codes

- Binary code $Enc: \{0,1\}^k \to \{0,1\}^n$ is $(\frac{1}{2} - \epsilon, L)$-list decodable if $\forall w \in \{0,1\}^n$, there are $\leq L$ messages $m$ such that $dist(Enc(m), w) \leq (\frac{1}{2} - \epsilon) \cdot n$

$(\frac{1}{2} - \epsilon, q, L)$-Locally List Decodable Code $[\text{Sudan, Trevisan, Vadhan 99}]$

- For every word $w$, and every message $m$, such that $dist(Enc(m), w) \leq (\frac{1}{2} - \epsilon) \cdot n$,
List decodable and local list decodable codes

- Binary code $\text{Enc}: \{0,1\}^k \rightarrow \{0,1\}^n$ is $(\frac{1}{2} - \varepsilon, L)$-list decodable if [Elias, Wozencraft 60’s]
  \[\forall w \in \{0,1\}^n, \text{there are } \leq L \text{ messages } m\]
  such that $\text{dist}(\text{Enc}(m), w) \leq \left(\frac{1}{2} - \varepsilon\right) \cdot n$

$(\frac{1}{2} - \varepsilon, q, L)$-Locally List Decodable Code [Sudan, Trevisan, Vadhan 99]

- For every word $w$, and every message $m$, such that $\text{dist}(\text{Enc}(m), w) \leq \left(\frac{1}{2} - \varepsilon\right) \cdot n$, with probability at least $2/3$
  \[\exists j \in [L] \text{ such that for all } i \in [k] \]
  $\Pr[\text{Dec}^w(i,j) = m_i] \geq 2/3$
What we study

\[ \text{Enc}: \{0,1\}^k \rightarrow \{0,1\}^n; \ n = 2^k \] (low rate)

- Example: Hadamard Code

\[ \langle m, r \rangle \]

With probability at least \( \frac{2}{3} \),
\[ \exists \ j \in [L] \text{ such that for all } i \in [k] \]
\[ \Pr[\text{Dec}^w(i,j) = m_i] \geq \frac{2}{3} \]
What we study

\[ \text{Enc}: \{0,1\}^k \rightarrow \{0,1\}^n; \quad n = 2^k \quad \text{(low rate)} \]

- Example: Hadamard Code

\[
\begin{align*}
\langle m, r \rangle & \quad \text{Enc}(m) \\
& \quad \text{Decoder Parameters:} \\
& \quad \text{[Goldreich Levin 89]} \\
& \quad r \in \{0,1\}^k
\end{align*}
\]

\[ w \in \{0,1\}^n \]

With probability at least \( 2/3 \),
\[ \exists \ j \in [L] \text{ such that for all } i \in [k] \]
\[ \Pr[ \text{Dec}^w(i,j) = m_i ] \geq 2/3 \]
What we study

\[ \text{Enc}: \{0,1\}^k \rightarrow \{0,1\}^n; \ n = 2^k \] (low rate)

- Example: Hadamard Code

**Example: Hadamard Code**

\[ \langle m, r \rangle \]

**Decoder Parameters:**

[Goldreich Levin 89]

For all \( \varepsilon \in [0, \frac{1}{2}) \), fraction of errors \( \frac{1}{2} - \varepsilon \),

- With probability at least \( \frac{2}{3} \),
  - \( \exists j \in [L] \) such that for all \( i \in [k] \)
    - \( \Pr[ \text{Dec}^w(i, j) = m_i ] \geq \frac{2}{3} \)
What we study

$\text{Enc}: \{0,1\}^k \rightarrow \{0,1\}^n; \ n = 2^k$ (low rate)

- Example: Hadamard Code

Decoder Parameters:
[Goldreich Levin 89]
For all $\varepsilon \in [0, \frac{1}{2})$, fraction of errors $\frac{1}{2} - \varepsilon$,
list size $O\left(\frac{1}{\varepsilon^2}\right)$
query complexity $O\left(\frac{1}{\varepsilon^2}\right)$

With probability at least $\frac{2}{3}$,
$\exists \ j \in [L]$ such that for all $i \in [k]
\Pr[\text{Dec}^w(i,j) = m_i] \geq \frac{2}{3}$
What we study

\[ Enc: \{0,1\}^k \rightarrow \{0,1\}^n; \quad n = 2^k \text{ (low rate)} \]

- Example: Hadamard Code

Decoder Parameters:

- [Goldreich Levin 89]
- For all \( \varepsilon \in [0, \frac{1}{2}) \), fraction of errors \( \frac{1}{2} - \varepsilon \),
- list size \( O\left(\frac{1}{\varepsilon^2}\right) \) (small list)
- query complexity \( O\left(\frac{1}{\varepsilon^2}\right) \)

Question: Can the number of queries be smaller, say \( \left(\frac{1}{\varepsilon}\right)^{o(1)} \) if we allow for large lists, say \( L = 2^{\frac{k}{100}} \) ?
Motivation

- Improvement in query complexity has the potential to provide “better” hardcore predicates from one-way functions (OWF) that are hard to invert

What we study

*Example: Hadamard Code*

\[
\text{Had} : \{0,1\}^k \rightarrow \{0,1\}^n; \quad n = 2^k \quad \text{(low rate)}
\]

\[
\text{Had}(m)
\]

- LLDC Parameters:

  - [Goldreich Levin 89]
  - For all \( \varepsilon \in [0, \frac{1}{2}) \), fraction of errors \( \frac{1}{2} - \varepsilon \),
  - list size \( O\left(\frac{1}{\varepsilon^2}\right) \) (small list)
  - query complexity \( O\left(\frac{1}{\varepsilon^2}\right) \)

**Question:** Can the number of queries be smaller, say \( \left(\frac{1}{\varepsilon}\right)^{o(1)} \) if we allow for large lists, say \( L = 2^{\frac{k}{100}} \)?
What we study

- Example: Hadamard Code

\[ \text{Had}: \{0,1\}^k \rightarrow \{0,1\}^n; \ n = 2^k \] (low rate) 
\( m, r \)

Our results

- For large \( \varepsilon > \frac{1}{k^{0.01}} \),

**Question**: Can the number of queries be smaller, say \( \left( \frac{1}{\varepsilon} \right)^{o(1)} \) if we allow for large lists, say \( L = 2^{\frac{k}{100}} \)?
What we study

\[ \text{Had}: \{0,1\}^k \rightarrow \{0,1\}^n; \ n = 2^k \ (\text{low rate}) \]

- Example: Hadamard Code

\[ \text{Had}(m) \]

LLDC Parameters:

[Goldreich Levin 89]

For all \( \varepsilon \in [0, \frac{1}{2}) \), fraction of errors \( \frac{1}{2} - \varepsilon \),

- list size \( O\left(\frac{1}{\varepsilon^2}\right) \) (small list)
- query complexity \( O\left(\frac{1}{\varepsilon^2}\right) \)

Question: Can the number of queries be smaller, say \( \left(\frac{1}{\varepsilon}\right)^{o(1)} \) if we allow for large lists, say \( L = 2^{\frac{k}{100}} \)?

Our results

- For large \( \varepsilon > \frac{1}{k^{0.01}} \), query complexity of local list decoding is \( \Omega\left(\frac{1}{\varepsilon^2}\right) \)

- Example: Hadamard Code

\[ \text{Had}(m) \]

- For large \( \varepsilon > \frac{1}{k^{0.01}} \), query complexity of local list decoding is \( \Omega\left(\frac{1}{\varepsilon^2}\right) \)
- Tight lower bound
- Holds even for large lists and low rate \( (n \geq 2^{k^{0.01}}) \)
- Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate \( (n \leq 2^{k^{0.01}}) \)

- For smaller \( \varepsilon \), query complexity is \( \Omega\left(\frac{1}{\varepsilon}\right) \)
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega\left(\frac{1}{\varepsilon^2}\right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^{k^{0.01}}$)

What we study

- Example: Hadamard Code
  \[ \text{Had}(\ast) \]

LLDC Parameters:
- [Goldreich Levin 89]
- For all $\varepsilon \in [0, \frac{1}{2})$, fraction of errors $\frac{1}{2} - \varepsilon$,
  list size $O\left(\frac{1}{\varepsilon^2}\right)$ (small list)
  query complexity $O\left(\frac{1}{\varepsilon^2}\right)$

Question: Can the number of queries be smaller, say $\left(\frac{1}{\varepsilon}\right)^{o(1)}$ if we allow for large lists, say $L = 2^{\frac{k}{100}}$?
What we study

- Example: Hadamard Code

\[ \text{Had}: \{0,1\}^k \rightarrow \{0,1\}^n; \quad n = 2^k \]
(low rate)

- LLDC Parameters:

**Goldreich Levin 89**

For all \( \varepsilon \in [0, \frac{1}{2}) \), fraction of errors \( \frac{1}{2} - \varepsilon \),
list size \( O\left(\frac{1}{\varepsilon^2}\right) \) (small list)
query complexity \( O\left(\frac{1}{\varepsilon^2}\right) \)

Our results

- For large \( \varepsilon > \frac{1}{k^{0.01}} \), query complexity of local list decoding is \( \Omega\left(\frac{1}{\varepsilon^2}\right) \)
  - Tight lower bound
  - Holds even for large lists and low rate \( (n \geq 2^k) \)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate \( (n \leq 2^{k^{0.01}}) \)

- For smaller \( \varepsilon \), query complexity is \( \Omega\left(\frac{1}{\sqrt{\varepsilon}}\right) \)
  - Rules out upper bound \( \left(\frac{1}{\varepsilon}\right)^{o(1)} \)

**Question:** Can the number of queries be smaller, say \( \left(\frac{1}{\varepsilon}\right)^{o(1)} \) if we allow for large lists, say \( L = 2^{\frac{k}{100}} \)?
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega\left(\frac{1}{\varepsilon^2}\right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^{k^{0.01}}$)

- For smaller $\varepsilon$, query complexity is $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$
  - Rules out upper bound $\left(\frac{1}{\varepsilon}\right)^{o(1)}$

Consequence of our result

Restatement of [Goldreich Levin 89]
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega \left( \frac{1}{\varepsilon^2} \right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^{k^{0.01}}$)

- For smaller $\varepsilon$, query complexity is $\Omega \left( \frac{1}{\sqrt{\varepsilon}} \right)$
  - Rules out upper bound $\left( \frac{1}{\varepsilon} \right)^{o(1)}$

Consequence of our result

Restatement of [Goldreich Levin 89]

- Given $f: \{0,1\}^k \rightarrow \{0,1\}^k$ such that for all circuits $C$ of size $s$,
  \[ \Pr_{x \sim R}\left[ C(f(x)) \in f^{-1}(f(x)) \right] \leq \rho \]
Our results

- For large \( \varepsilon > \frac{1}{k^{0.01}} \), query complexity of local list decoding is \( \Omega \left( \frac{1}{\varepsilon^2} \right) \)
  - Tight lower bound
  - Holds even for large lists and low rate \( n \geq 2^k \)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate \( n \leq 2^{k^{0.01}} \)

- For smaller \( \varepsilon \), query complexity is \( \Omega \left( \frac{1}{\sqrt{\varepsilon}} \right) \)
  - Rules out upper bound \( \left( \frac{1}{\varepsilon} \right)^{o(1)} \)

Consequence of our result

Restatement of [Goldreich Levin 89]

- Given \( f: \{0,1\}^k \rightarrow \{0,1\}^k \) such that for all circuits \( C \) of size \( s \),
  \[ \Pr_{x \sim_R \{0,1\}^k} \left[ C(f(x)) \in f^{-1}(f(x)) \right] \leq \rho \]
- Define \( f_{new}(x,r) = (f(x),r) \) for \( x,r \in \{0,1\}^k \)
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega\left(\frac{1}{\varepsilon^2}\right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^{k^{0.01}}$)

- For smaller $\varepsilon$, query complexity is $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$
  - Rules out upper bound $\left(\frac{1}{\varepsilon}\right)^{o(1)}$

Consequence of our result

Restatement of [Goldreich Levin 89]

- Given $f: \{0,1\}^k \rightarrow \{0,1\}^k$ such that for all circuits $C$ of size $s$,
  \[
  \Pr_{x \sim R\{0,1\}^k} [C(f(x)) \in f^{-1}(f(x))] \leq \rho
  \]

- Define
  \[
  f^{\text{new}}(x, r) = (f(x), r) \quad \text{for } x, r \in \{0,1\}^k \\
  f^{\text{pred}}(x, r) = r^{\text{th}} \text{ bit of } Had(x)
  \]
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega\left(\frac{1}{\varepsilon^2}\right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^{k^{0.01}}$)

- For smaller $\varepsilon$, query complexity is $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$
  - Rules out upper bound $\left(\frac{1}{\varepsilon}\right)^{o(1)}$

Consequence of our result

**Restatement of [Goldreich Levin 89]**

- Given $f: \{0,1\}^k \rightarrow \{0,1\}^k$ such that for all circuits $C$ of size $s$,
  $$\Pr_{x \sim R}\left[C(f(x)) \in f^{-1}(f(x))\right] \leq \rho$$

- Define
  $$f^{\text{new}}(x,r) = (f(x),r) \text{ for } x,r \in \{0,1\}^k \text{ and } f^{\text{pred}}(x,r) = r\text{th bit of } Had(x)$$

- For all circuits $C'$ of size $s' = \frac{s}{q \cdot \text{poly}(k)}$,
  $$\Pr_{(x,r) \sim R^{2^k}}\left[C'(f^{\text{new}}(x,r)) = f^{\text{pred}}(x,r)\right] \leq \frac{1}{2} + \varepsilon$$
Our results

- For large $\epsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega\left(\frac{1}{\epsilon^2}\right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^{k^{0.01}}$)

- For smaller $\epsilon$, query complexity is $\Omega\left(\frac{1}{\sqrt{\epsilon}}\right)$
  - Rules out upper bound $\left(\frac{1}{\epsilon}\right)^{o(1)}$

Consequence of our result

Restatement of [Goldreich Levin 89]

- Given $f : \{0,1\}^k \to \{0,1\}^k$ such that for all circuits $C$ of size $s$, $\text{poly}(k)$
  $$\Pr_{x \sim_R \{0,1\}^k} [C(f(x)) \in f^{-1}(f(x))] \leq \rho$$

- Define
  $$f^{\text{new}}(x, r) = (f(x), r) \text{ for } x, r \in \{0,1\}^k \text{ and } f^{\text{pred}}(x, r) = r \text{th bit of } \text{Had}(x)$$

- For all circuits $C'$ of size $s' = \frac{s}{q \cdot \text{poly}(k)}$
  $$\Pr_{(x,r) \sim_R \{0,1\}^{2k}} [C'(f^{\text{new}}(x,r)) = f^{\text{pred}}(x,r)] \leq \frac{1}{2} + \epsilon$$
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega\left(\frac{1}{\varepsilon^2}\right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^{k^{0.01}}$)

- For smaller $\varepsilon$, query complexity is $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$
  - Rules out upper bound $\left(\frac{1}{\varepsilon}\right)^{o(1)}$

Consequence of our result

Restatement of [Goldreich Levin 89]

- Given $f: \{0,1\}^k \to \{0,1\}^k$ such that for all circuits $C$ of size $s$, $\Pr_{x \sim R\{0,1\}^k}[C(f(x)) \in f^{-1}(f(x))] \leq \rho$

- Define $f^{\text{new}}(x,r) = (f(x),r)$ for $x,r \in \{0,1\}^k$ and $f^{\text{pred}}(x,r) = r$th bit of $\text{Had}(x)$

- For all circuits $C'$ of size $s' = \frac{s}{q \cdot \text{poly}(k)}$

  $\Pr_{(x,r) \sim R\{0,1\}^{2k}}[C'(f^{\text{new}}(x,r)) = f^{\text{pred}}(x,r)] \leq \frac{1}{2} + \varepsilon$
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega\left(\frac{1}{\varepsilon^2}\right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^{k^{0.01}}$)

- For smaller $\varepsilon$, query complexity is $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$
  - Rules out upper bound $\left(\frac{1}{\varepsilon}\right)^{o(1)}$

Consequence of our result

Restatement of [Goldreich Levin 89]

- Given $f: \{0,1\}^k \rightarrow \{0,1\}^k$ such that for all circuits $C$ of size $s$, $\Pr_{x \sim R_{\{0,1\}^k}}[C(f(x)) \in f^{-1}(f(x))] \leq \rho$

- Define
  $f^{\text{new}}(x,r) = (f(x),r)$ for $x,r \in \{0,1\}^k$ and
  $f^{\text{pred}}(x,r) = r$th bit of $Had(x)$

- For all circuits $C'$ of size $s' = \frac{s}{q \cdot \text{poly}(k)}$, $\Pr_{(x,r) \sim R_{\{0,1\}^{2k}}}[C'(f^{\text{new}}(x,r)) = f^{\text{pred}}(x,r)] \leq \frac{1}{2} + \varepsilon$

\[\varepsilon = \frac{1}{\text{poly}(k)}\]
Our results

- For large \( \varepsilon > \frac{1}{k^{0.01}} \), query complexity of local list decoding is \( \Omega\left(\frac{1}{\varepsilon^2}\right) \)
  - Tight lower bound
  - Holds even for large lists and low rate \((n \geq 2^k)\)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate \((n \leq 2^{k^{0.01}})\)

- For smaller \( \varepsilon \), query complexity is \( \Omega\left(\frac{1}{\sqrt{\varepsilon}}\right) \)
  - Rules out upper bound \(\left(\frac{1}{\varepsilon}\right)^{o(1)}\)

Consequence of our result

Restatement of [Goldreich Levin 89]

- Given \( f: \{0,1\}^k \to \{0,1\}^k \) such that for all circuits \( C \) of size \( s, \) \( \Pr_{x \sim R_0 \{0,1\}^k} \left[ C(f(x)) \in f^{-1}(f(x)) \right] \leq \rho \frac{1}{2^{\sqrt{k}}} \)

- Define \( f^{new}(x, r) = (f(x), r) \) for \( x, r \in \{0,1\}^k \) and \( f^{pred}(x, r) = r \)th bit of Had(x)

- For all circuits \( C' \) of size \( s' = \frac{s}{q \cdot poly(k)} \)
  \( \Pr_{x, r \sim_R \{0,1\}^{2k}} \left[ C'(f^{new}(x, r)) = f^{pred}(x, r) \right] \leq \frac{1}{2} + \varepsilon \)
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega\left(\frac{1}{\varepsilon^2}\right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^{k^{0.01}}$)

- For smaller $\varepsilon$, query complexity is $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$
  - Rules out upper bound $\left(\frac{1}{\varepsilon}\right)^{o(1)}$

Consequence of our result

Restatement of [Goldreich Levin 89]

- Given $f : \{0,1\}^k \to \{0,1\}^k$ such that for all circuits $C$ of size $s$, $\Pr_{x \sim R\{0,1\}^k}[C(f(x)) \in f^{-1}(f(x))] \leq \rho \frac{1}{2^{\sqrt{k}}}$

- Define $f^{new}(x, r) = (f(x), r)$ for $x, r \in \{0,1\}^k$ and $f^{pred}(x, r) = r^{th}$ bit of $Had(x)$

- For all circuits $C'$ of size $s' = \frac{s}{q \cdot poly(k)}$, $\Pr_{(x, r) \sim R\{0,1\}^{2k}}[C'(f^{new}(x, r)) = f^{pred}(x, r)] \leq \frac{1}{2} + \varepsilon$

Even if we start with a harder function, possible to obtain only $\varepsilon = \frac{1}{poly(k)}$ via this approach
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega \left( \frac{1}{\varepsilon^2} \right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^{k^{0.01}}$)

- For smaller $\varepsilon$, query complexity is $\Omega \left( \frac{1}{\sqrt{\varepsilon}} \right)$
  - Rules out upper bound $\left(\frac{1}{\varepsilon}\right)^{o(1)}$

Consequence of our result

Restatement of [Goldreich Levin 89]

- Given $f: \{0,1\}^k \rightarrow \{0,1\}^k$ such that for all circuits $C$ of size $s$, $\text{poly}(k)$
  \[ \Pr_{x \sim_R \{0,1\}^k} \left[ C(f(x)) \in f^{-1}(f(x)) \right] \leq \rho \left( \frac{1}{2} \right) + \varepsilon \]

- Define
  \[ f^{\text{new}}(x,r) = (f(x),r) \text{ for } x,r \in \{0,1\}^k \text{ and } f^{\text{pred}}(x,r) = r \text{th bit of Had}(x) \]

- For all circuits $C'$ of size $s' = \frac{s}{q \cdot \text{poly}(k)}$
  \[ \Pr_{(x,r) \sim_R \{0,1\}^{2k}} \left[ C'(f^{\text{new}}(x,r)) = f^{\text{pred}}(x,r) \right] \leq \frac{1}{2} + \varepsilon \]

Is it possible to obtain $\varepsilon \ll 1/\text{poly}(k)$ with replacing Hadamard with another list decodable code?
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega\left(\frac{1}{\varepsilon^2}\right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^{k^{0.01}}$)

- For smaller $\varepsilon$, query complexity is $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$
  - Rules out upper bound $\left(\frac{1}{\varepsilon}\right)^{o(1)}$

Consequence of our result

Restatement of [Goldreich Levin 89]

- Given $f: \{0,1\}^k \to \{0,1\}^k$ such that for all circuits $C$ of size $s$, $\Pr_{x \sim R_1 \{0,1\}^k} [C(f(x)) \in f^{-1}(f(x))] \leq \rho \frac{1}{2^{\sqrt{k}}}$

- Define $f^{\text{new}}(x,r) = (f(x),r)$ for $x,r \in \{0,1\}^k$ and $f^{\text{pred}}(x,r) = r$th bit of Had($x$)

- For all circuits $C'$ of size $s' = \frac{s}{q \cdot \text{poly}(k)}$, $\Pr_{(x,r) \sim R_1 \{0,1\}^{2k}} [C'(f^{\text{new}}(x,r)) = f^{\text{pred}}(x,r)] \leq \frac{1}{2} + \varepsilon$

Is it possible to obtain $\varepsilon \ll 1/\text{poly}(k)$ with replacing Hadamard with another list decodable code? No!
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega\left(\frac{1}{\varepsilon^2}\right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^{k^{0.01}}$)

- For smaller $\varepsilon$, query complexity is $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$
  - Rules out upper bound $\frac{1}{\varepsilon^{o(1)}}$

Consequence of our result

**Restatement of** [Goldreich Levin 89]

- Given $f : \{0,1\}^k \to \{0,1\}^k$ such that for all circuits $C$ of size $s$, $\Pr_{x \sim R\{0,1\}^k} [C(f(x)) \in f^{-1}(f(x))] \leq \rho$ $1/2^{\sqrt{k}}$

- Define $f^{new}(x,r) = (f(x), r)$ for $x,r \in \{0,1\}^k$ and $f^{pred}(x,r) = r$th bit of $Had(x)$

- For all circuits $C'$ of size $s' = \frac{s}{q \cdot poly(k)}$,
  $\Pr_{(x,r) \sim R\{0,1\}^{2k}} [C'(f^{new}(x,r)) = f^{pred}(x,r)] \leq \frac{1}{2} + \varepsilon$

Is it possible obtain a hardcore predicate with $\varepsilon = \frac{1}{k^{\omega(1)}}$ via a different "black-box method"?
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega\left(\frac{1}{\varepsilon^2}\right)$
  - Tight lower bound
  - Holds even for large lists and low rate ($n \geq 2^k$)
  - Extends the result of [Grinberg Shaltiel Viola 18] that worked for codes with larger rate ($n \leq 2^k^{0.01}$)

- For smaller $\varepsilon$, query complexity is $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$
  - Rules out upper bound $\left(\frac{1}{\varepsilon}\right)^{o(1)}$

Consequence of our result

Restatement of [Goldreich Levin 89]

- Given $f: \{0,1\}^k \to \{0,1\}^k$ such that for all circuits $C$ of size $s$, $\Pr_{x \sim_R \{0,1\}^k}[C(f(x)) \in f^{-1}(f(x))] \leq \rho 1/2^{\sqrt{k}}$

- Define $f^{new}(x,r) = (f(x),r)$ for $x,r \in \{0,1\}^k$ and $f^{pred}(x,r) = r$th bit of $Had(x)$

- For all circuits $C'$ of size $s' = \frac{s}{q \cdot \text{poly}(k)}$, $\Pr_{(x,r) \sim_R \{0,1\}^{2k}}[C'(f^{new}(x,r)) = f^{pred}(x,r)] \leq \frac{1}{2} + \varepsilon$

Is it possible obtain a hardcore predicate with $\varepsilon = \frac{1}{k^{\omega(1)}}$ via a different “black-box method”? No!
What we will show

- Local list decoding of $Enc: \{0,1\}^k \rightarrow \{0,1\}^n$ from $\frac{1}{2} - \varepsilon$ fraction errors needs $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$ queries for small $\varepsilon < \frac{1}{k^{0.01}}$. 
What we will show

- Local list decoding of $\text{Enc} : \{0,1\}^k \to \{0,1\}^n$ from $\frac{1}{2} - \varepsilon$ fraction errors needs $\Omega \left( \frac{1}{\sqrt{\varepsilon}} \right)$ queries for small $\varepsilon < \frac{1}{k^{0.01}}$

even for codes with $n \geq 2^k$ and even by allowing large list sizes $L \leq \beta 2^k$

for some constant $\beta > 0$

Proof idea inspired from Applebaum, Artemenko, Shaltiel, Yang 16
Reducing to a different problem

\[ m \in \{0,1\}^k \]

\[ \text{Enc}(m) \in \{0,1\}^n \]

\[ w \in \{0,1\}^n \]

\[ \frac{1}{2} - \varepsilon \text{ fraction errors} \]

\[ q \text{ queries} \]

\[ i \in [k] \]

\[ j \in [L] \]

\[ m_i, \text{ with probability } \geq \frac{2}{3} \]

\[ m_i: \text{i}^{th} \text{ bit of message } m \]
Reducing to a different problem

- Decode from word $w \in \{0,1\}^n$

- $m \sim_R \{0,1\}^k$

- $z \sim BSC_{\frac{n}{2} - 2\epsilon}^n$

- $m_i$: $i$th bit of message $m$

- $i \in [k]$ with probability $\geq \frac{2}{3}$

- $j \in [L]$:

- $1/2 - \epsilon$ fraction errors

- $w \in \{0,1\}^n$

- $Enc(m) \in \{0,1\}^n$

- $Dec(m) \in \{0,1\}^n$

- $q$ queries

$BSC_p^n$: Distribution over $\{0,1\}^n$; each bit $1$ independently with probability $p$
Reducing to a different problem

- Decode from word $w \in \{0,1\}^n$

- Decode at least $1 - 1/2k$ fraction of message bits correctly

$BSC_p^n$: Distribution over $\{0,1\}^n$; each bit 1 independently with probability $p$
Reducing to a different problem

- Decode from word \( w \in \{0,1\}^n \)

\[
m \sim_R \{0,1\}^k
\]

\[
Enc(m) \oplus z \sim BSC_{\frac{1}{2} - 2\varepsilon}^n
\]

- Decode at least \( 1 - \frac{1}{2k} \) fraction of message bits correctly
- Deterministic decoder

\( m \in \{0,1\}^k \)

\( w \in \{0,1\}^n \)

\( \frac{1}{2} - \varepsilon \) fraction errors

\( i \in [k] \)

\( j \in [L] \)

\( m_i \): \( i \)th bit of message \( m \)

\( BSC_p^n \): Distribution over \( \{0,1\}^n \); each bit 1 independently with probability \( p \)
\( m \in \{0,1\}^k \)

\( \text{Enc}(m) \in \{0,1\}^n \)

\( w \in \{0,1\}^n \)

\( \frac{1}{2} - \varepsilon \) fraction errors

\( q \) queries

\( i \in [k] \)

\( j \in [L] \)

\( \text{Decoder} \)

\( m_i, \text{ with probability } \geq 1 - \delta \)

\( m_i: \text{i}^{\text{th}} \text{ bit of message } m \)

\( BSC_p^n: \text{Distribution over } \{0,1\}^n; \text{ each bit } 1 \text{ independently with probability } p \)

Reducing to a different problem

- Decode from word \( w \in \{0,1\}^n \)

\( m \sim_R \{0,1\}^k \)

\( \text{Enc}(m) \oplus z \sim BSC_{1/2 - 2\varepsilon}^n \)

- Decode at least \( 1 - 1/2k \) fraction of message bits correctly

- Deterministic decoder

Local list decoding implies above decoding task (up to \( O(\log k) \) factor in queries)
\( m \sim_R \{0,1\}^k \)

\[ \text{Dec}(m) \]

\( w \in \{0,1\}^n \)

\( q \) queries

\( i \in [k] \)

\( j \in [L] \)

With probability at least \( \frac{1}{3} \) over the choice of \((m, z, w)\), \( \exists j \in [L] \)

\[ \Pr_{i \sim [k]} [\text{Dec}^w(i, j) = m_i] \geq 1 - 1/2k \]

Reducing to a different problem

- Decode from word \( w \in \{0,1\}^n \)

- Decode at least \( 1 - 1/2k \) fraction of message bits correctly

- Deterministic decoder

Local list decoding implies above decoding task (up to \( O(\log k) \) factor in queries)
Lower bounds on circuit sizes for coin problem

- Circuits of AND, OR, NOT gates of unbounded fan-in

\[ m \sim_R \{0,1\}^k \]

\[ \text{Enc}(m) \]

\[ w \in \{0,1\}^n \]

\[ z \sim BSC_{\frac{1}{2}-2\varepsilon}^n \]

\[ m \oplus z \]

\[ q \text{ queries} \]

\[ i \in [k] \]

\[ j \in [L] \]

With probability at least \( \frac{1}{3} \) over the choice of \((m, z, w)\), \( \exists j \in [L] \)

\[ \Pr_{i \sim [k]} [\text{Dec}^w(i, j) = m_i] \geq 1 - 1/2k \]
Lower bounds on circuit sizes for coin problem

- Circuits of AND, OR, NOT gates of unbounded fan-in
- **Theorem**: If $C : \{0,1\}^n \rightarrow \{0,1\}$ has depth $d$, and:
  1. $\Pr_{z \sim \text{BSC}_{\frac{1}{2}-2\epsilon}} [C(z) = 1] \geq 0.99$
  2. $\Pr_{z \sim \text{BSC}_{\frac{1}{2}-2\epsilon}} [C(z) = 1] \leq 0.01$

With probability at least $\frac{1}{3}$ over the choice of $(m, z, w)$, $\exists j \in [L]$

$$\Pr_{i \sim [k]} [\text{Dec}^w(i, j) = m_i] \geq 1 - 1/2k$$
Lower bounds on circuit sizes for coin problem

- Circuits of AND, OR, NOT gates of unbounded fan-in

- **Theorem:** If $C : \{0,1\}^n \rightarrow \{0,1\}$ has depth $d$, and:
  
  1. \( \Pr_{z \sim \text{BSC}_{\frac{1}{2}}^{-2\varepsilon}} [C(z) = 1] \geq 0.99 \)
  2. \( \Pr_{z \sim \text{BSC}_{\frac{1}{2}}^{-2\varepsilon}} [C(z) = 1] \leq 0.01 \)

Then $C$ has size at least

\[
\exp \left( \Omega \left( d \cdot \left( \frac{1}{\varepsilon} \right)^{d-1} \right) \right)
\]
Lower bounds on circuit sizes for coin problem

- Circuits of AND, OR, NOT gates of unbounded fan-in

- **Theorem:** If $C: \{0,1\}^n \rightarrow \{0,1\}$ has depth $d$, and:
  1. $\Pr_{z \sim BSC^1_{\frac{1}{2}-2\varepsilon}}[C(z) = 1] \geq 0.99$
  2. $\Pr_{z \sim BSC^1_{\frac{1}{2}-2\varepsilon}}[C(z) = 1] \leq 0.01$

  Then $C$ has size at least

  $$\exp\left(\Omega\left(d \cdot \left(\frac{1}{\varepsilon}\right)^{d-1}\right)\right)$$

With probability at least $\frac{1}{3}$ over the choice of $(m, z, w)$, $\exists j \in [L]$

$$\Pr_{i \sim [k]}[\text{Dec}^w(i, j) = m_i] \geq 1 - 1/2k$$

---

Shaltiel Viola 10, Aaronson 10, Cohen Ganor Raz 14, Limaye Sreenivasaiah Srinivasan Tripathi Venkitesh 19
Circuit based on decoder

- For $m \in \{0,1\}^k$ define a circuit $C_m$ that on input $z \in \{0,1\}^n$:

Lower bounds on circuit sizes for coin problem

- Circuits of AND, OR, NOT gates of unbounded fan-in

- **Theorem**: If $C: \{0,1\}^n \to \{0,1\}$ has depth $d$, and:
  1. $\Pr_{z \sim \text{BSC}_1^n_{\frac{1}{2} - 2\epsilon}} [C(z) = 1] \geq 0.99$
  2. $\Pr_{z \sim \text{BSC}_1^n_{\frac{1}{2} - 2\epsilon}} [C(z) = 1] \leq 0.01$

  Then $C$ has size at least

$$\exp \left( \Omega \left( d \cdot \left( \frac{1}{\epsilon} \right)^{d-1} \right) \right)$$
Circuit based on decoder

- For \( m \in \{0,1\}^k \) define a circuit \( C_m \) that on input \( z \in \{0,1\}^n \):
  - Evaluate \( w = Enc(m) \oplus z \)

Lower bounds on circuit sizes for coin problem

- Circuits of AND, OR, NOT gates of unbounded fan-in

- **Theorem:** If \( C: \{0,1\}^n \to \{0,1\} \) has depth \( d \), and:
  1. \( \Pr_{z \sim BSC^n_{1/2}} \left[ C(z) = 1 \right] \geq 0.99 - 2\varepsilon \)
  2. \( \Pr_{z \sim BSC^n_{1/2}} \left[ C(z) = 1 \right] \leq 0.01 + 2\varepsilon \)

Then \( C \) has size at least

\[
\exp \left( \Omega \left( d \cdot \left( \frac{1}{\varepsilon} \right)^{d-1} \right) \right)
\]
Circuit based on decoder

- For $m \in \{0,1\}^k$ define a circuit $C_m$ that on input $z \in \{0,1\}^n$:
  - Evaluate $w = Enc(m) \oplus z$
  - For $i \in [k], j \in [L]$, evaluate a bit $b_{i,j}$ for whether $Dec^w(i,j) = m_i$

Lower bounds on circuit sizes for coin problem

- Circuits of AND, OR, NOT gates of unbounded fan-in

- Theorem: If $C: \{0,1\}^n \rightarrow \{0,1\}$ has depth $d$, and:
  1. $\Pr_{z \sim BSC_1^n/2} [C(z) = 1] \geq 0.99$
  2. $\Pr_{z \sim BSC_1^n/2} [C(z) = 1] \leq 0.01$

Then $C$ has size at least

$$\exp\left(\Omega \left( d \cdot \left(\frac{1}{\varepsilon}\right)^{d-1}\right)\right)$$
Circuit based on decoder

- For $m \in \{0,1\}^k$ define a circuit $C_m$ that on input $z \in \{0,1\}^n$:
  - Evaluate $w = Enc(m) \oplus z$
  - For $i \in [k], j \in [L]$, evaluate a bit $b_{i,j}$ for whether $Dec^w(i, j) = m_i$
  - Output $\land_{i \in [k]} b_{i,j}$

Lower bounds on circuit sizes for coin problem

- Circuits of AND, OR, NOT gates of unbounded fan-in

- **Theorem:** If $C: \{0,1\}^n \to \{0,1\}$ has depth $d$, and:
  1. $\Pr_{z \sim BSC_1^n_{\frac{1}{2} - 2\epsilon}} [C(z) = 1] \geq 0.99$
  2. $\Pr_{z \sim BSC_1^n_{\frac{1}{2} + \epsilon}} [C(z) = 1] \leq 0.01$

Then $C$ has size at least

$$\exp \left( \Omega \left( d \cdot \left( \frac{1}{\epsilon} \right)^{d-1} \right) \right)$$
Circuit based on decoder

For $m \in \{0,1\}^k$ define a circuit $C_m$ that on input $z \in \{0,1\}^n$: 
- Evaluate $w = Enc(m) \oplus z$
- For $i \in [k], j \in [L]$, evaluate a bit $b_{i,j}$ for whether $Dec^w(i, j) = m_i$
- Output $\forall j \in [L] \land \forall i \in [k] \ b_{i,j}$

Lower bounds on circuit sizes for coin problem

- Circuits of AND, OR, NOT gates of unbounded fan-in
- **Theorem:** If $C : \{0,1\}^n \to \{0,1\}$ has depth $d$, and:
  1. $\Pr_{z \sim BSC_{\frac{1}{2}}^n} [C(z) = 1] \geq 0.99$ 
  2. $\Pr_{z \sim BSC_{\frac{1}{2}}^n} [C(z) = 1] \leq 0.01$

Then $C$ has size at least

$$\exp \left( \Omega \left( d \cdot \left( \frac{1}{\varepsilon} \right)^{d-1} \right) \right)$$
Circuit based on decoder

- For $m \in \{0,1\}^k$ define a circuit $C_m$ that on input $z \in \{0,1\}^n$:
  - Evaluate $w = Enc(m) \oplus z$
  - For $i \in [k], j \in [L]$, evaluate a bit $b_{i,j}$ for whether $Dec^w(i,j) = m_i$
  - Output $\lor_{j \in [L]} \land_{i \in [k]} b_{i,j}$
- Can do this with a circuit of depth 3 and size $O(k \cdot L \cdot q2^q)$

Lower bounds on circuit sizes for coin problem

- Circuits of AND, OR, NOT gates of unbounded fan-in
- **Theorem:** If $C: \{0,1\}^n \to \{0,1\}$ has depth $d$, and:
  1. $\Pr_{z \sim BSC^n_{1/2}}[C(z) = 1] \geq 0.99$
  2. $\Pr_{z \sim BSC^n_{1/2}}[C(z) = 1] \leq 0.01$

  Then $C$ has size at least

  $\exp\left(\Omega\left(d \cdot \left(\frac{1}{\varepsilon}\right)^{d-1}\right)\right)$
Circuit based on decoder

- For $m \in \{0,1\}^k$ define a circuit $C_m$ that on input $z \in \{0,1\}^n$:
  - Evaluate $w = Enc(m) \oplus z$
  - For $i \in [k], j \in [L]$, evaluate a bit $b_{i,j}$ for whether $Dec^w(i, j) = m_i$
  - Output $\lor_{j \in [L]} \land_{i \in [k]} b_{i,j}$

- Can do this with a circuit of depth $3$ and size $O(k \cdot L \cdot q2^q)$

- Main Idea: $q$-query deterministic decoder can be represented with $O(q \cdot 2^q)$ size and only $O(k \cdot L \cdot q2^q)$ “useful bits” in $Enc(m)$

Lower bounds on circuit sizes for coin problem

- Circuits of AND, OR, NOT gates of unbounded fan-in

- Theorem: If $C: \{0,1\}^n \rightarrow \{0,1\}$ has depth $d$, and:
  1. $\Pr_{z \sim BSC_\frac{1}{2}-2\epsilon} [C(z) = 1] \geq 0.99$
  2. $\Pr_{z \sim BSC_\frac{1}{2}} [C(z) = 1] \leq 0.01$

  Then $C$ has size at least

$$\exp \left( \Omega \left( d \cdot \left( \frac{1}{\epsilon} \right)^{d-1} \right) \right)$$
Circuit based on decoder

- For $m \in \{0,1\}^k$ define a circuit $C_m$ that on input $z \in \{0,1\}^n$:
  - Evaluate $w = Enc(m) \oplus z$
  - For $i \in [k], j \in [L]$, evaluate a bit $b_{i,j}$ for whether $Dec^w(i,j) = m_i$
  - Output $\lor_{j \in [L]} \land_{i \in [k]} b_{i,j}$

- Can do this with a circuit of depth 3 and size $O(k \cdot L \cdot q2^q)$
Circuit based on decoder

- For $m \in \{0,1\}^k$ define a circuit $C_m$ that on input $z \in \{0,1\}^n$:
  - Evaluate $w = Enc(m) \oplus z$
  - For $i \in [k], j \in [L]$, evaluate a bit $b_{i,j}$ for whether $Dec^w(i,j) = m_i$
  - Output $\vee_{j \in [L]} \wedge_{i \in [k]} b_{i,j}$

- Can do this with a circuit of depth 3 and size $O(k \cdot L \cdot q2^q)$

- From definition of decoder:
  $$\Pr_{m \sim \{0,1\}^k, z \sim BSC_1^n} [C_m(z) = 1] \geq \frac{1}{6}$$
For $m \in \{0,1\}^k$ define a circuit $C_m$ that on input $z \in \{0,1\}^n$:
- Evaluate $w = Enc(m) \oplus z$
- For $i \in [k], j \in [L]$, evaluate a bit $b_{i,j}$ for whether $Dec^w(i, j) = m_i$
- Output $\bigvee_{j \in [L]} \bigwedge_{i \in [k]} b_{i,j}$

Can do this with a circuit of depth $3$ and size $O(k \cdot L \cdot q2^q)$

From definition of decoder:
$$\Pr_{m \sim \{0,1\}^k, z \sim BSC_1^n_{\frac{1}{2}-2\varepsilon}} [C_m(z) = 1] \geq \frac{1}{6}$$

Since $Enc(m) \oplus z$ is uniformly random for $z \sim BSC_1^n_{\frac{1}{2}}$:
$$\Pr_{m \sim \{0,1\}^k, z \sim BSC_1^n_{\frac{1}{2}}} [C_m(z) = 1] \leq \frac{L}{2^k}$$
Circuit based on decoder

- For $m \in \{0,1\}^k$ define a circuit $C_m$ that on input $z \in \{0,1\}^n$:
  - Evaluate $w = Enc(m) \oplus z$
  - For $i \in [k], j \in [L]$, evaluate a bit $b_{i,j}$ for whether $Dec^w(i,j) = m_i$
  - Output $\lor_{j \in [L]} \land_{i \in [k]} b_{i,j}$
- Can do this with a circuit of depth 3 and size $O(k \cdot L \cdot q^2)$

- From definition of decoder:
  $$Pr_{m \sim \{0,1\}^k, z \sim BSC_1^n} [C_m(z) = 1] \geq \frac{1}{6}$$

- Since $Enc(m) \oplus z$ is uniformly random for $z \sim BSC_1^n$:
  $$Pr_{m \sim \{0,1\}^k, z \sim BSC_1^n} [C_m(z) = 1] \leq \frac{L}{2^k}$$

- By averaging and using $L \leq \beta 2^k$ for some $\beta > 0$, there exists $m \in \{0,1\}^k$ such that
  $$Pr_{z \sim BSC_1^n} [C_m(z) = 1] \geq 0.99 \text{ and}$$
  $$Pr_{z \sim BSC_1^n} [C_m(z) = 1] \leq 0.01$$
From definition of decoder:

\[ \Pr_{m \sim \{0,1\}^k, z \sim BSC_{1/2}^n} [C_m(z) = 1] \geq \frac{1}{6} \]

Since \( Enc(m) \oplus z \) is uniformly random for \( z \sim BSC_{1/2}^n \):

\[ \Pr_{m \sim \{0,1\}^k, z \sim BSC_{1/2}^n} [C_m(z) = 1] \leq \frac{L}{2^k} \]

By averaging and using \( L \leq \beta 2^k \) for some \( \beta > 0 \), there exists \( m \in \{0,1\}^k \) such that

\[ \Pr_{z \sim BSC_{1/2}^n} [C_m(z) = 1] \geq 0.99 \text{ and } \Pr_{z \sim BSC_{1/2}^n} [C_m(z) = 1] \leq 0.01 \]

Circuit based on decoder

- For \( m \in \{0,1\}^k \) define a circuit \( C_m \) that on input \( z \in \{0,1\}^n \):
  - Evaluate \( w = Enc(m) \oplus z \)
  - For \( i \in [k], j \in [L] \), evaluate a bit \( b_{i,j} \) for whether \( Dec^w(i,j) = m_i \)
  - Output \( \lor_{j \in [L]} \land_{i \in [k]} b_{i,j} \)

- Can do this with a circuit of depth 3 and size \( O(k \cdot L \cdot q 2^q) \)

\[
kL2^{2q} \geq \exp \left( \Omega \left( \frac{1}{\sqrt{\varepsilon}} \right) \right)
\]

\[
\Rightarrow q \geq \frac{1}{\log k \sqrt{\varepsilon}} - \log L = \Omega \left( \frac{1}{\varepsilon^{0.5-o(1)}} \right)
\]
What we saw

- Local list decoding of $Enc: \{0,1\}^k \rightarrow \{0,1\}^n$ from $\frac{1}{2} - \varepsilon$ fraction errors needs $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$ queries for small $\varepsilon < \frac{1}{k^{0.01}}$, even for codes with $n \geq 2^k$ and even by allowing large list sizes $L \leq \beta 2^k$ for some constant $\beta > 0$. 
Open problems

- Improving the lower bound for the small $\varepsilon$ case from $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$
Open problems

- Improving the lower bound for the small $\varepsilon$ case from $\Omega \left( \frac{1}{\sqrt{\varepsilon}} \right)$
- Our lower bound for the case of large $\varepsilon$ can be extended to decode from $1 - \varepsilon$ fraction erasures to get a bound $\Omega \left( \frac{1}{\varepsilon} \right)$
  - Is it possible to do a similar extension for the small $\varepsilon$ case?
Open problems

- Improving the lower bound for the small $\varepsilon$ case from $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$

- Our lower bound for the case of large $\varepsilon$ can be extended to decode from $1 - \varepsilon$ fraction erasures to get a bound $\Omega\left(\frac{1}{\varepsilon}\right)$
  - Is it possible to do a similar extension for the small $\varepsilon$ case?

- Non-black-box techniques that help obtain better hardcore predicates from hard functions?

Thank You!