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

Noga Ron-Zewi Ronen Shaltiel Nithin Varma

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

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 $Enc: \{0,1\}^k \to \{0,1\}^n$ is $\left(\frac{1}{2} - \varepsilon, L\right)$-list decodable if [Elias, Wozencraft 60's]

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

List decodable and local list decodable codes

- Binary code $Enc: \{0,1\}^k \to \{0,1\}^n$ is $\left(\frac{1}{2} - \varepsilon, L\right)$-list decodable if [Elias, Wozencraft 60's]
  $\forall\, w \in \{0,1\}^n$,

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

List decodable and local list decodable codes

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

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

List decodable and local list decodable codes

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

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

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

$m^{(2)} \in \{0,1\}^k$

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

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

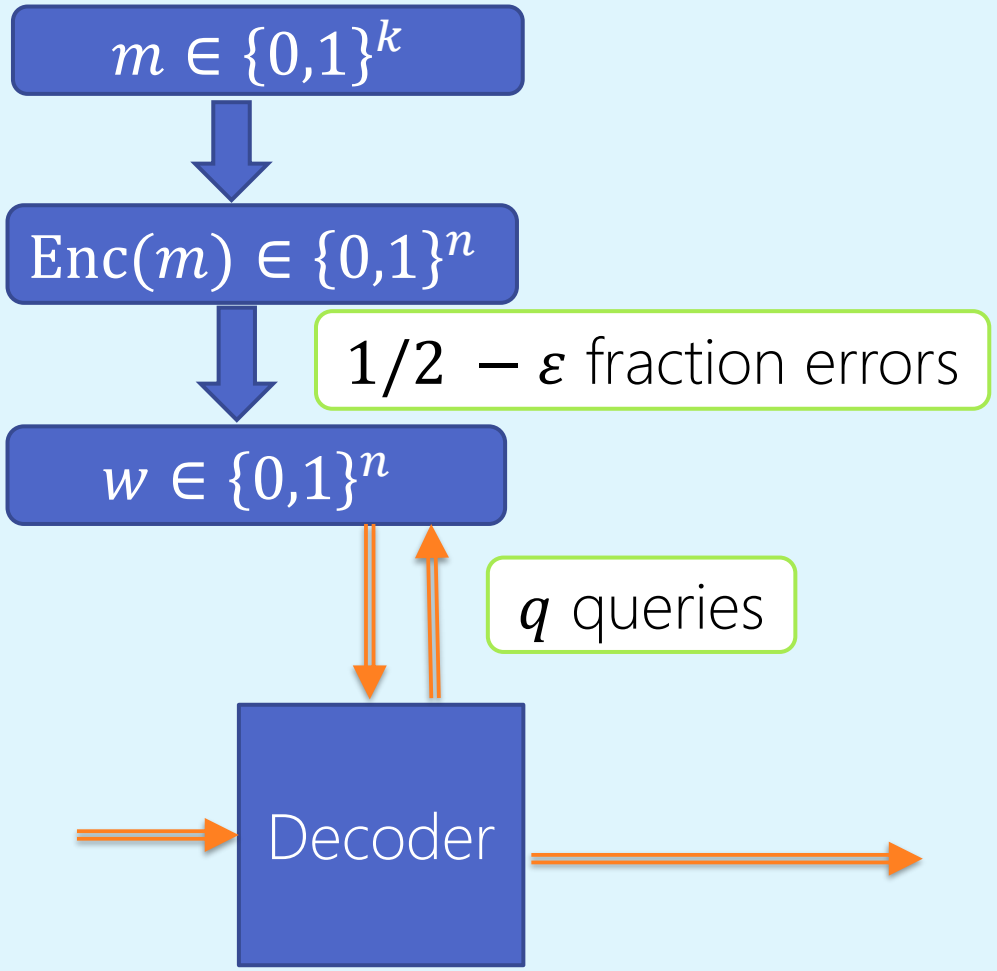
List of $\leq L$ messages whose encodings differ from w in at most $\left(\frac{1}{2} - \varepsilon\right) n$ locations

List decodable and local list decodable codes

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

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

[Sudan, Trevisan, Vadhan 99]



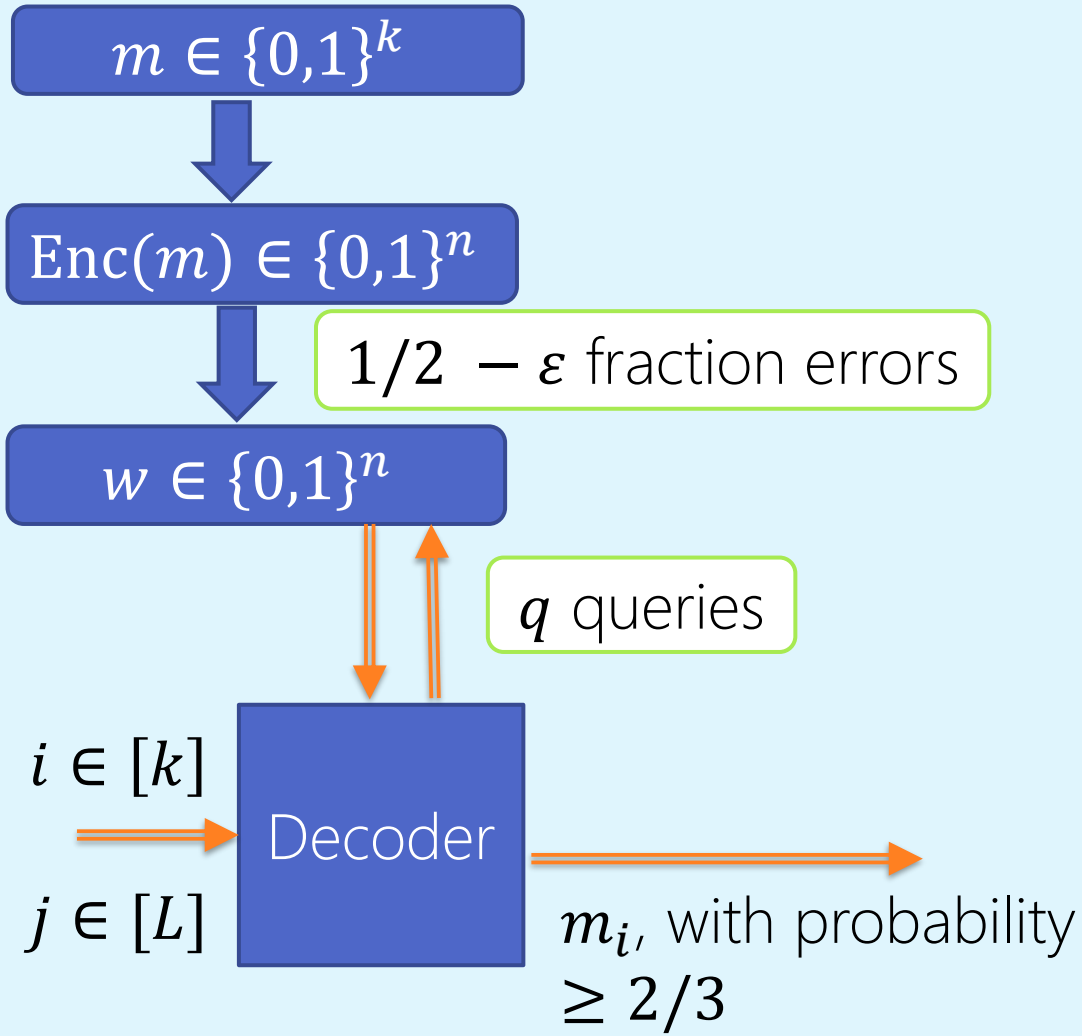
List decodable and local list decodable codes

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

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

[Sudan, Trevisan, Vadhan 99]

- For every word w, and every message m, such that $\mathbf{dist}(Enc(m), w) \leq \left(\frac{1}{2} - \varepsilon\right) \cdot n$,



m_i: ith bit of message m

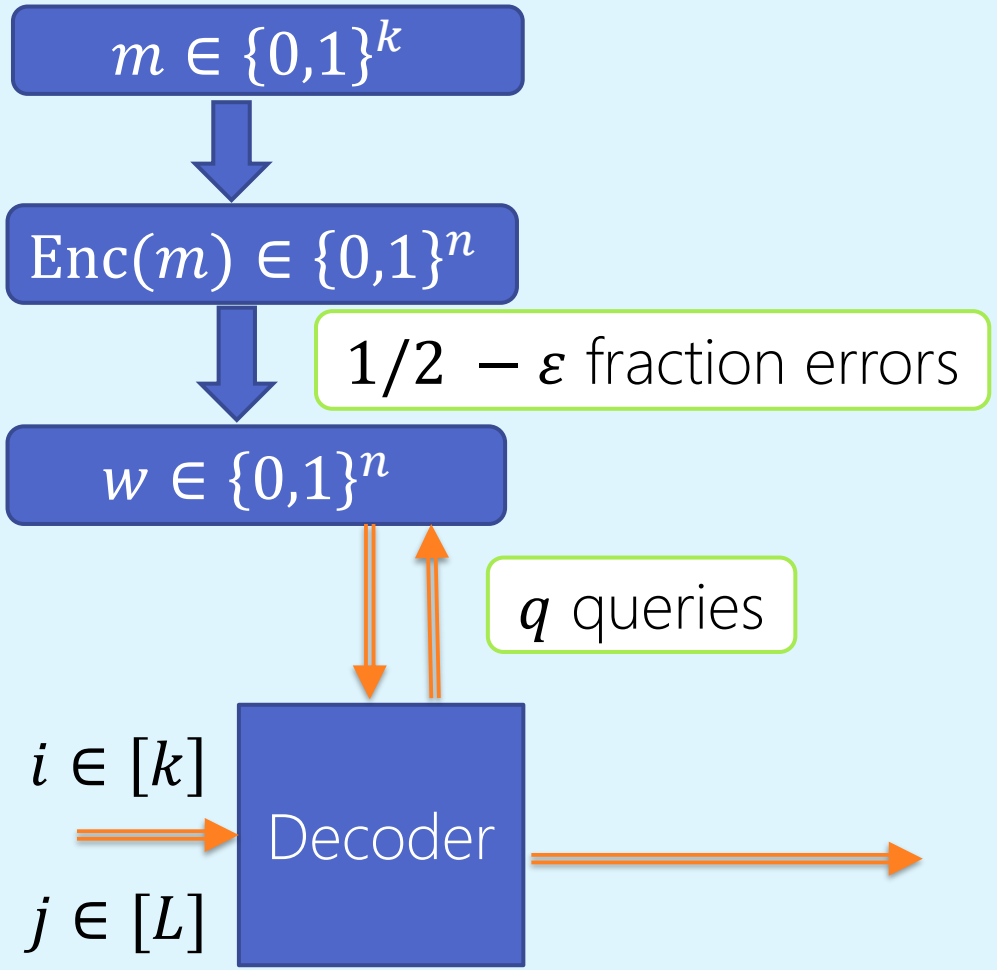
List decodable and local list decodable codes

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

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

[Sudan, Trevisan, Vadhan 99]

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



With probability at least $2/3$,

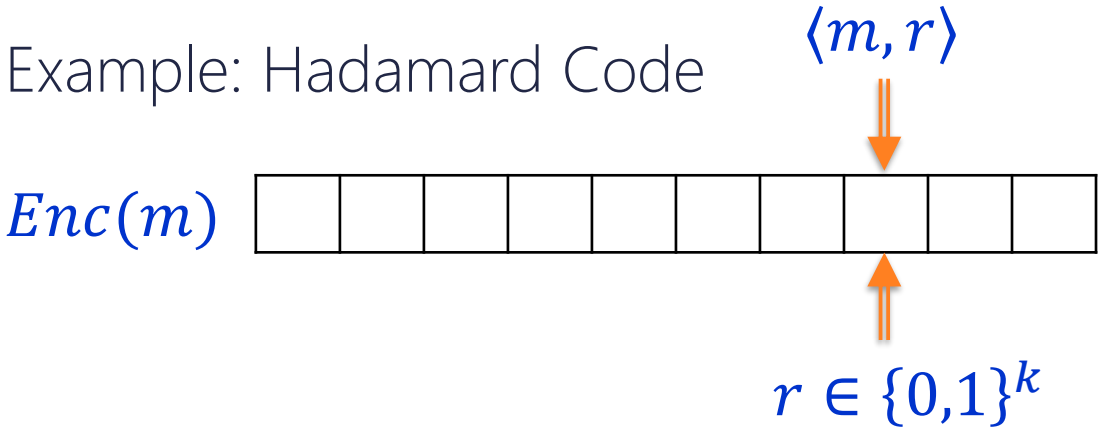
$\exists\ j \in [L]$ such that for all $i \in [k]$

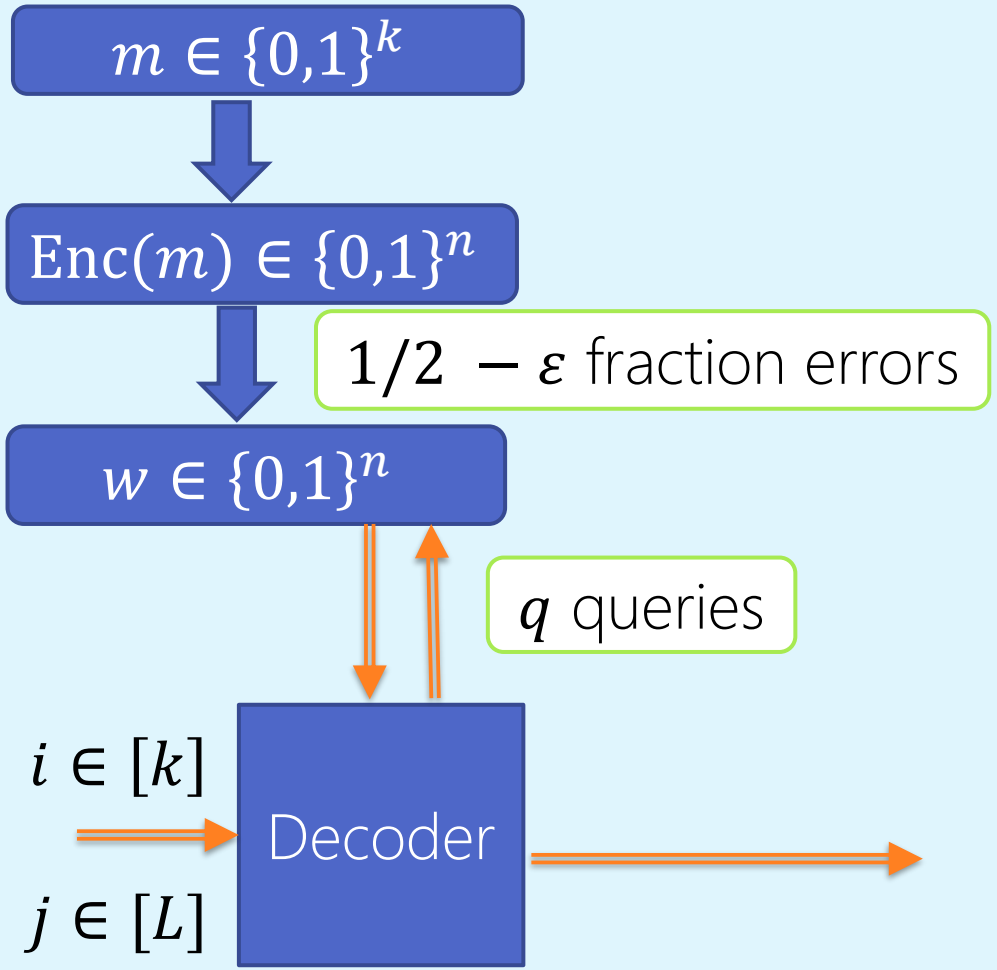
$$\Pr[\mathrm{Dec}^w(i,j) = m_i] \geq 2/3$$

What we study

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

- Example: Hadamard Code





With probability at least $2/3$,

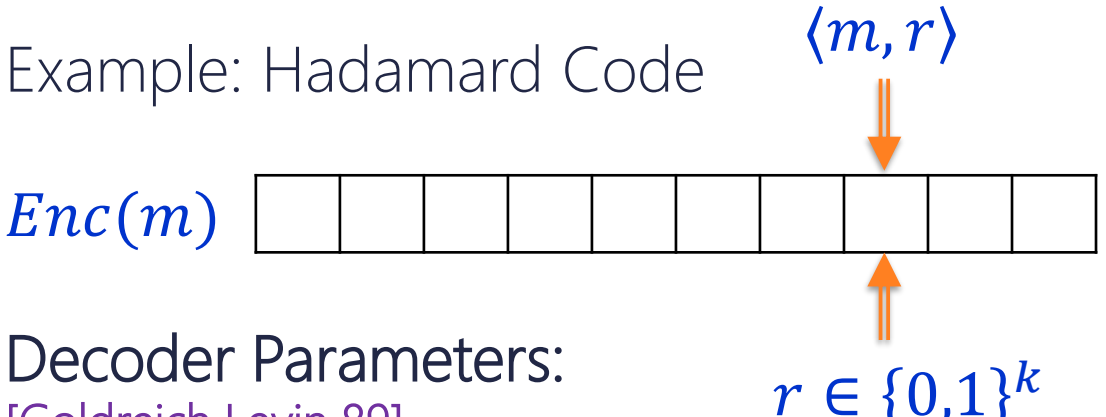
$\exists\ j \in [L]$ such that for all $i \in [k]$

$$\Pr[\mathrm{Dec}^w(i,j) = m_i] \geq 2/3$$

What we study

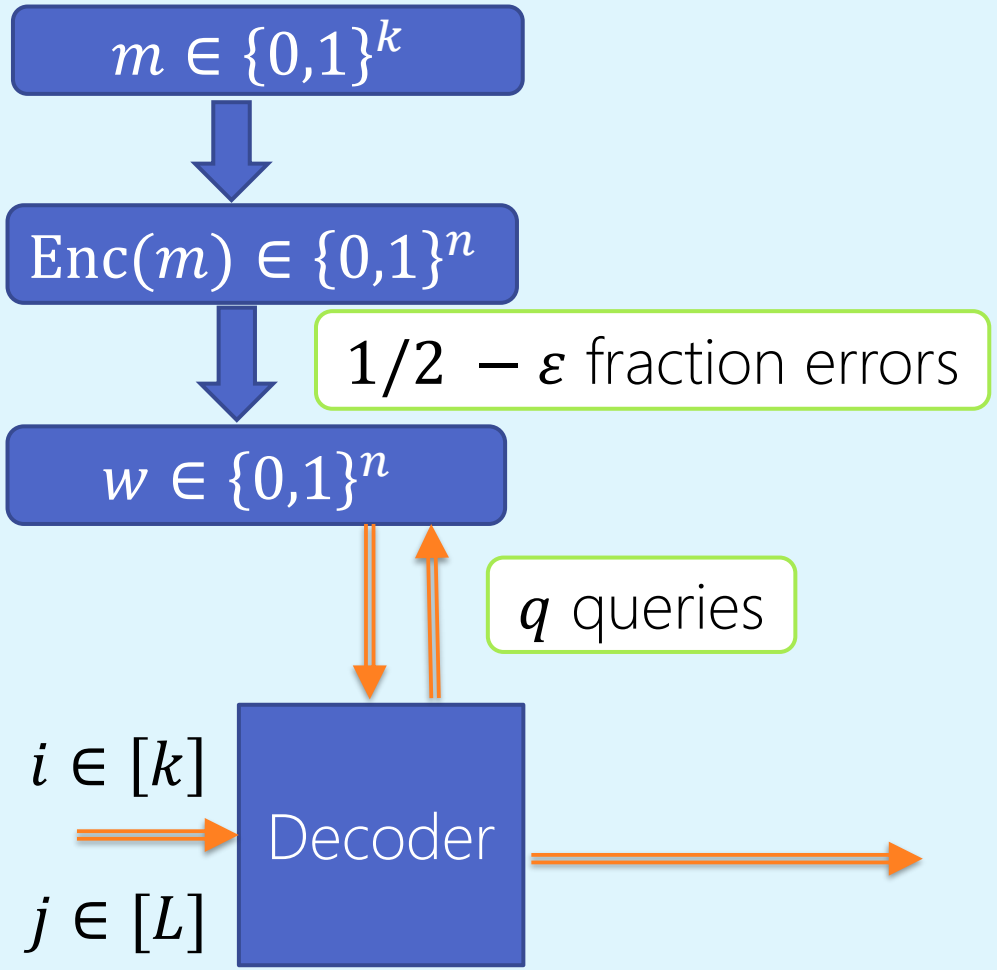
$Enc: \{0,1\}^k \to \{0,1\}^n;\ n = 2^k$ (low rate)

- Example: Hadamard Code



Decoder Parameters:

[Goldreich Levin 89]



With probability at least $2/3$,

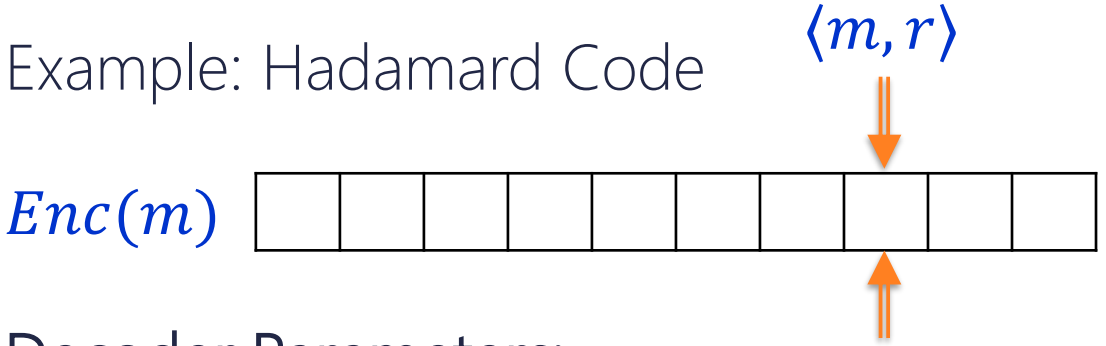
$\exists\ j \in [L]$ such that for all $i \in [k]$

$$\Pr[\mathrm{Dec}^w(i,j) = m_i] \geq 2/3$$

What we study

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

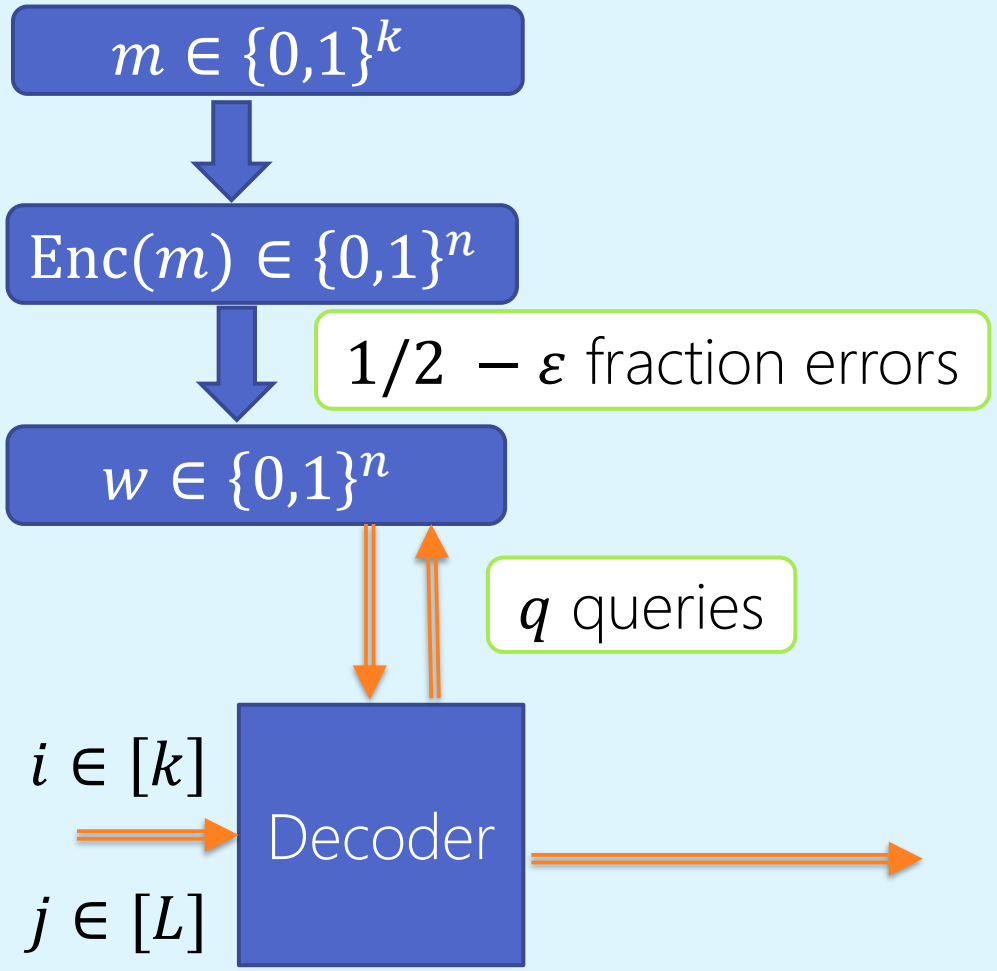
- Example: Hadamard Code



Decoder Parameters:

[Goldreich Levin 89]

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



With probability at least $2/3$,

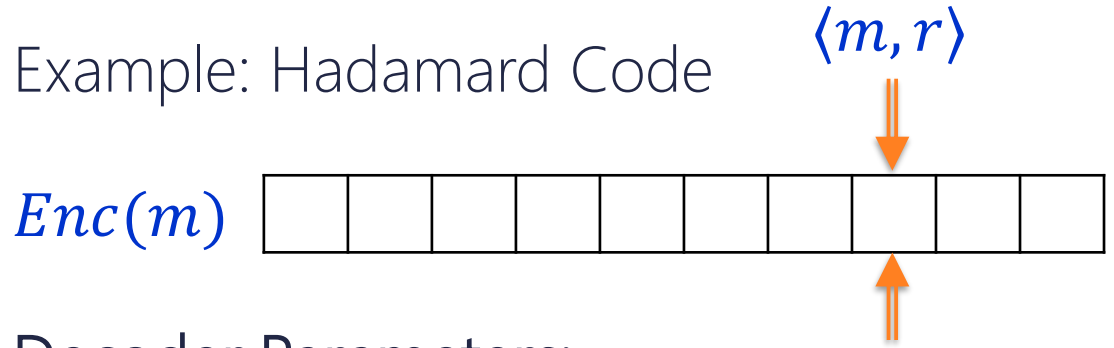
$\exists\ j \in [L]$ such that for all $i \in [k]$

$$\Pr[\mathrm{Dec}^w(i,j) = m_i] \geq 2/3$$

What we study

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

- Example: Hadamard Code

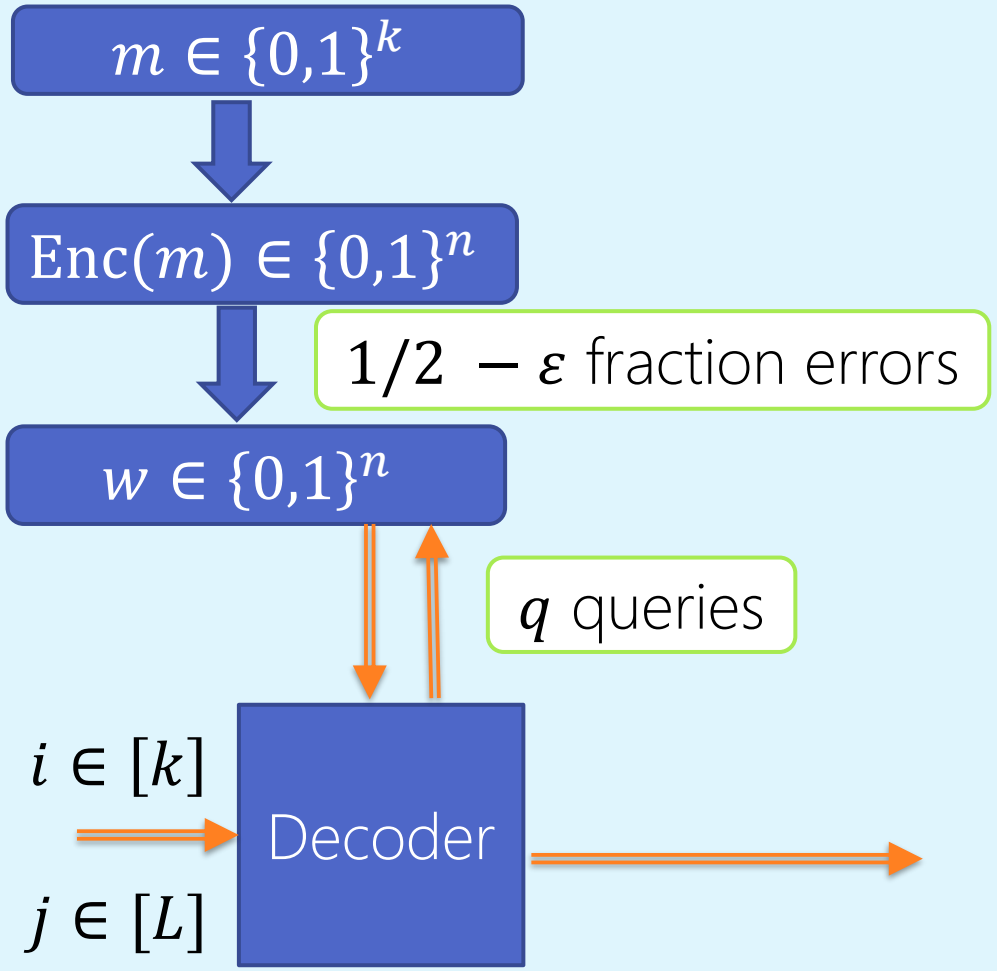


Decoder Parameters:
[Goldreich Levin 89]

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

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

query complexity $O\left(\frac{1}{\varepsilon^2}\right)$



With probability at least $2/3$,

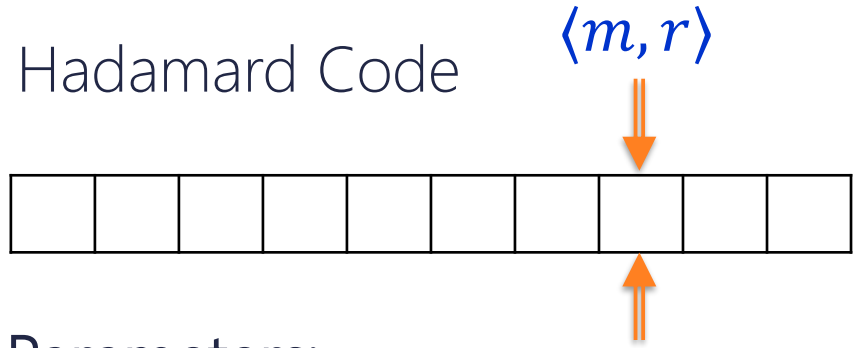
$\exists\ j \in [L]$ such that for all $i \in [k]$

$$\Pr[\,\mathrm{Dec}^w(i,j) = m_i] \geq 2/3$$

What we study

$Enc: \{0,1\}^k \to \{0,1\}^n$; $n = 2^k$ (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 $O\left(\frac{1}{\varepsilon^2}\right)$ (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 $L = 2^{\frac{k}{100}}$?

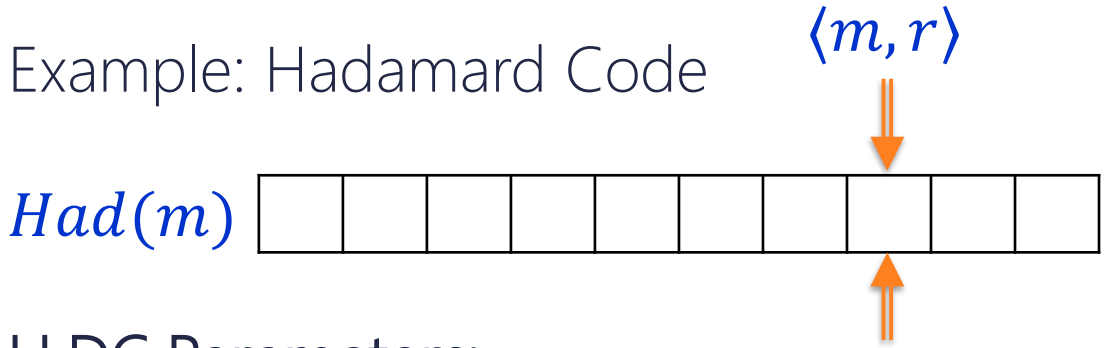
Motivation

- 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

$Had: \{0,1\}^k \to \{0,1\}^n;\ n = 2^k$ (low rate)

- Example: Hadamard Code



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 $L = 2^{\frac{k}{100}}$?

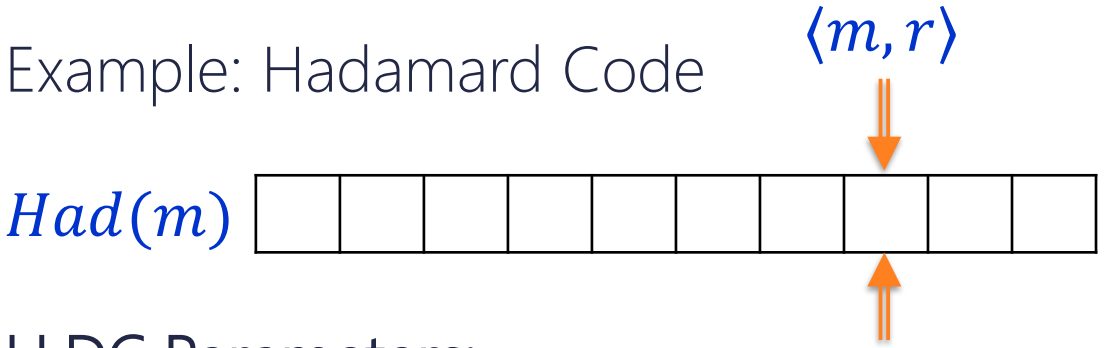
Our results

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

What we study

$Had: \{0,1\}^k \to \{0,1\}^n$; $n = 2^k$ (low rate)

- Example: Hadamard Code



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 $L = 2^{\frac{k}{100}}$?

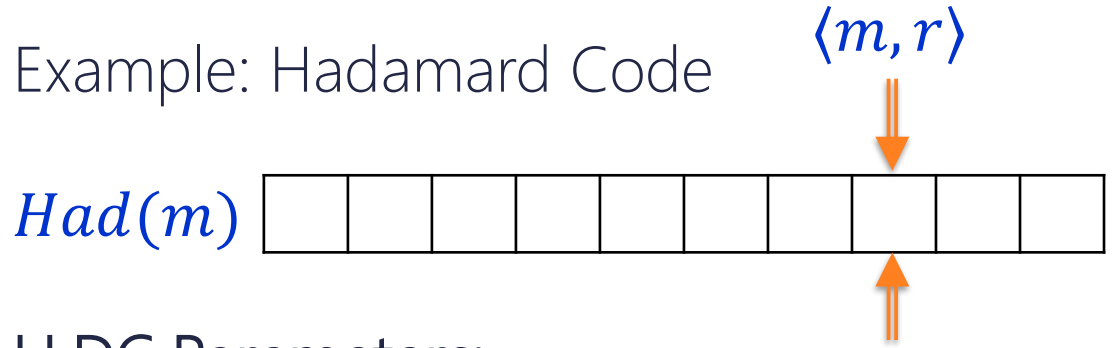
Our results

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

What we study

$Had: \{0,1\}^k \to \{0,1\}^n$; $n = 2^k$ (low rate)

- Example: Hadamard Code



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 $L = 2^{\frac{k}{100}}$?

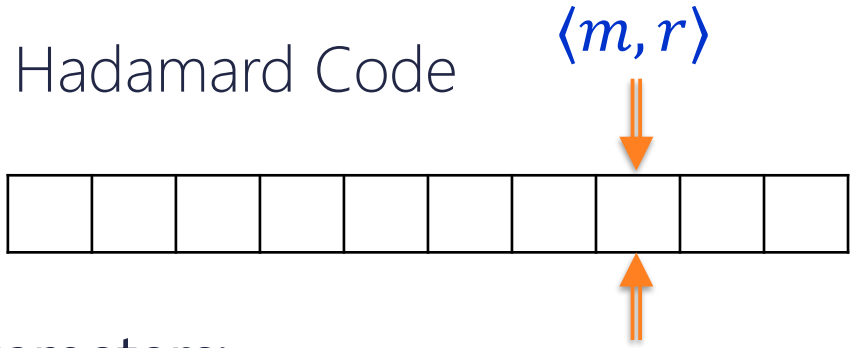
Our results

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

$Had: \{0,1\}^k \to \{0,1\}^n$; $n = 2^k$ (low rate)

- Example: Hadamard Code



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 $L = 2^{\frac{k}{100}}$?

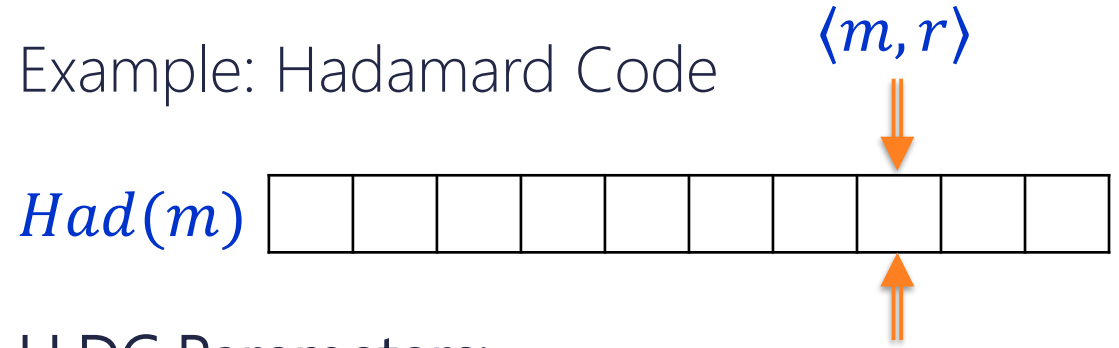
Our results

- For large $\varepsilon > \frac{1}{k^{0.01}}$, query complexity of local list decoding is $\Omega\left(\frac{1}{\varepsilon^2}\right)$
  - 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 ε, query complexity is $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$
  - Rules out upper bound $\left(\frac{1}{\varepsilon}\right)^{o(1)}$

What we study

$Had: \{0,1\}^k \to \{0,1\}^n$; $n = 2^k$ (low rate)

- Example: Hadamard Code



LLDC Parameters:
[Goldreich Levin 89]

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

list size $O\left(\frac{1}{\varepsilon^2}\right)$

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 $\Omega\left(\frac{1}{\varepsilon^2}\right)$
  - 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 ε, 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 ε, 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,
$$\Pr_{x \sim_R \{0,1\}^k}\left[C\left(f(x)\right) \in f^{-1}\left(f(x)\right)\right] \leq \rho$$

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

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

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 ε, 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, poly(k)
$$\Pr_{x \sim_R \{0,1\}^k}\left[C\left(f(x)\right) \in f^{-1}\left(f(x)\right)\right] \leq \rho$$
1/poly(k)
- Define $f^{new}(x,r) = (f(x),r)$ for $x,r \in \{0,1\}^k$ and $f^{pred}(x,r) =$ rth bit of $Had(x)$
- For all circuits C' of size $s' = \frac{s}{q \cdot poly(k)}$,
$$\Pr_{(x,r) \sim_R \{0,1\}^{2k}}\left[C'\left(f^{new}(x,r)\right) = f^{pred}(x,r)\right] \leq \frac{1}{2} + \varepsilon$$

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 ε, 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, poly(k)

$$\Pr_{x \sim_R \{0,1\}^k}\left[C\left(f(x)\right) \in f^{-1}\left(f(x)\right)\right] \leq \rho$$

1/poly(k)

- Define $f^{new}(x,r) = (f(x),r)$ for $x,r \in \{0,1\}^k$ and $f^{pred}(x,r) =$ rth bit of $Had(x)$
- For all circuits C' of size $s' = \frac{s}{q \cdot poly(k)}$,

$$\Pr_{(x,r) \sim_R \{0,1\}^{2k}}\left[C'\left(f^{new}(x,r)\right) = f^{pred}(x,r)\right] \leq \frac{1}{2} + \varepsilon$$

$\varepsilon = 1/\text{poly}(k)$

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 ε, 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, poly(k) $\Pr_{x\sim_R\{0,1\}^k}\left[C\left(f(x)\right) \in f^{-1}\left(f(x)\right)\right] \leq \rho$ $1/2^{\sqrt{k}}$
- Define $f^{new}(x,r) = (f(x),r)$ for $x,r \in \{0,1\}^k$ and $f^{pred}(x,r) =$ rth bit of $Had(x)$
- For all circuits C' of size $s' = \frac{s}{q\cdot poly(k)}$, $\Pr_{(x,r)\sim_R\{0,1\}^{2k}}\left[C'\left(f^{new}(x,r)\right) = f^{pred}(x,r)\right] \leq \frac{1}{2} + \varepsilon$

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 ε, 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, poly(k) $\Pr_{x \sim_R \{0,1\}^k}\left[C\left(f(x)\right) \in f^{-1}\left(f(x)\right)\right] \leq \rho$ $1/2^{\sqrt{k}}$
- Define $f^{new}(x,r) = (f(x),r)$ for $x,r \in \{0,1\}^k$ and $f^{pred}(x,r) =$ rth bit of $Had(x)$
- For all circuits C' of size $s' = \frac{s}{q \cdot poly(k)}$, $\Pr_{(x,r) \sim_R \{0,1\}^{2k}}\left[C'\left(f^{new}(x,r)\right) = f^{pred}(x,r)\right] \leq \frac{1}{2} + \varepsilon$

Even if we start with a harder function, possible to obtain only $\varepsilon = 1/poly(k)$ 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 ε, 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, poly(k) $\Pr_{x\sim_R\{0,1\}^k}\left[C\left(f(x)\right) \in f^{-1}\left(f(x)\right)\right] \leq \rho$ $1/2^{\sqrt{k}}$
- Define $f^{new}(x,r) = (f(x),r)$ for $x,r \in \{0,1\}^k$ and $f^{pred}(x,r) =$ rth bit of $Had(x)$
- For all circuits C' of size $s' = \frac{s}{q\cdot poly(k)}$, $\Pr_{(x,r)\sim_R\{0,1\}^{2k}}\left[C'\left(f^{new}(x,r)\right) = f^{pred}(x,r)\right] \leq \frac{1}{2} + \varepsilon$

Is it possible to obtain $\varepsilon \ll 1/poly(k)$ 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 ε, 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, poly(k) $\Pr_{x\sim_R\{0,1\}^k}\left[C\left(f(x)\right) \in f^{-1}\left(f(x)\right)\right] \leq \rho$ $1/2^{\sqrt{k}}$
- Define $f^{new}(x,r) = (f(x),r)$ for $x,r \in \{0,1\}^k$ and $f^{pred}(x,r) =$ rth bit of $Had(x)$
- For all circuits C' of size $s' = \frac{s}{q\cdot poly(k)}$, $\Pr_{(x,r)\sim_R\{0,1\}^{2k}}\left[C'\left(f^{new}(x,r)\right) = f^{pred}(x,r)\right] \leq \frac{1}{2} + \varepsilon$

Is it possible to obtain $\varepsilon \ll 1/poly(k)$ 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 ε, 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, poly(k) $\Pr_{x\sim_R\{0,1\}^k}\left[C\left(f(x)\right) \in f^{-1}\left(f(x)\right)\right] \leq \rho$ $1/2^{\sqrt{k}}$
- Define $f^{new}(x,r) = (f(x),r)$ for $x,r \in \{0,1\}^k$ and $f^{pred}(x,r) =$ rth bit of $Had(x)$
- For all circuits C' of size $s' = \frac{s}{q\cdot poly(k)}$, $\Pr_{(x,r)\sim_R\{0,1\}^{2k}}\left[C'\left(f^{new}(x,r)\right) = f^{pred}(x,r)\right] \leq \frac{1}{2} + \varepsilon$

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 ε, 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, poly(k) $\Pr_{x\sim_R\{0,1\}^k}\left[C\left(f(x)\right) \in f^{-1}\left(f(x)\right)\right] \leq \rho$ $1/2^{\sqrt{k}}$
- Define $f^{new}(x,r) = (f(x),r)$ for $x,r \in \{0,1\}^k$ and $f^{pred}(x,r) =$ rth bit of $Had(x)$
- For all circuits C' of size $s' = \frac{s}{q\cdot poly(k)}$, $\Pr_{(x,r)\sim_R\{0,1\}^{2k}}\left[C'\left(f^{new}(x,r)\right) = f^{pred}(x,r)\right] \leq \frac{1}{2} + \varepsilon$

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

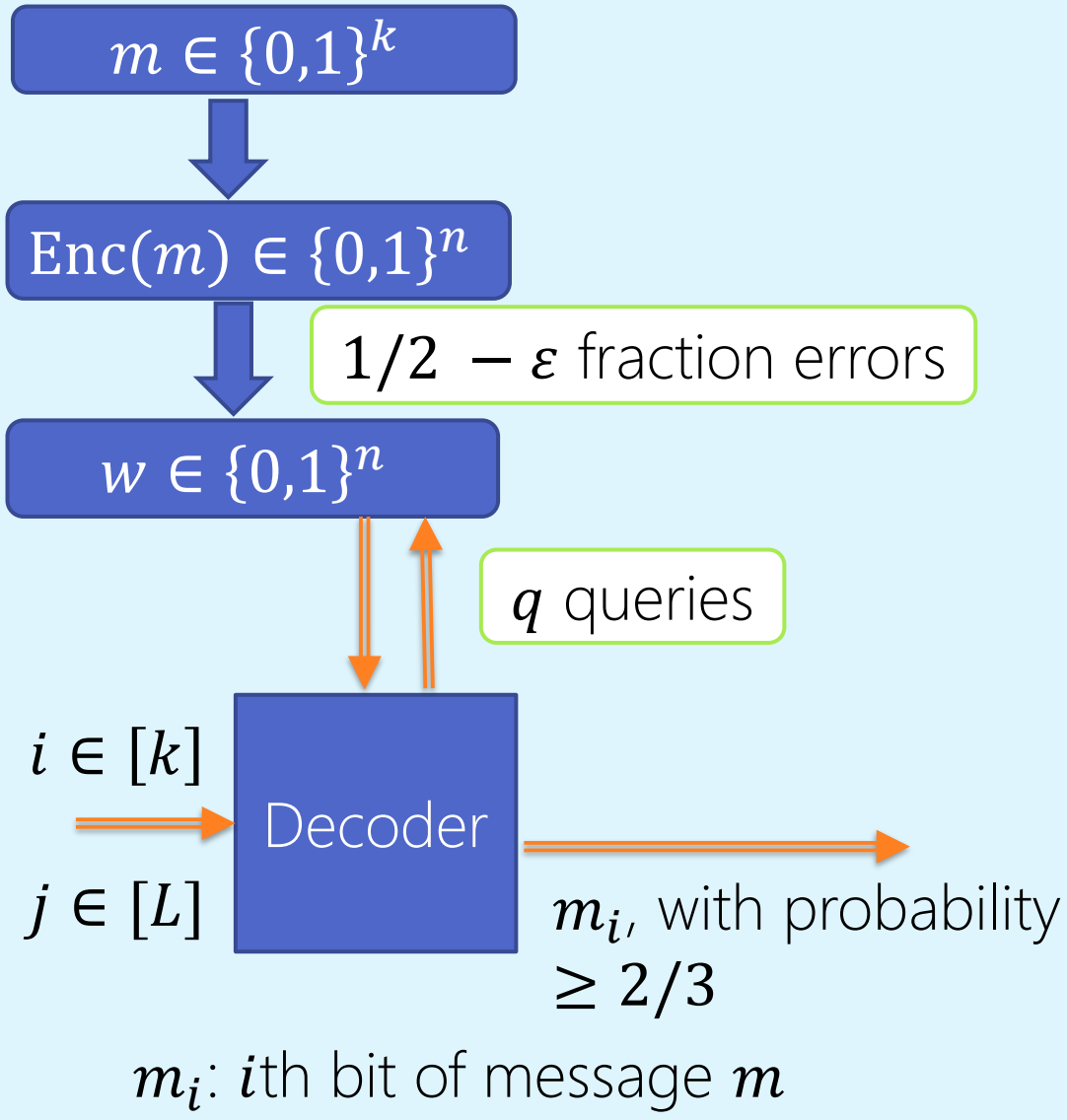
- Local list decoding of $Enc: \{0,1\}^k \to \{0,1\}^n$ from $\frac{1}{2} - \varepsilon$ fraction errors needs $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$ queries for small $\varepsilon < \frac{1}{k^{0.01'}}$

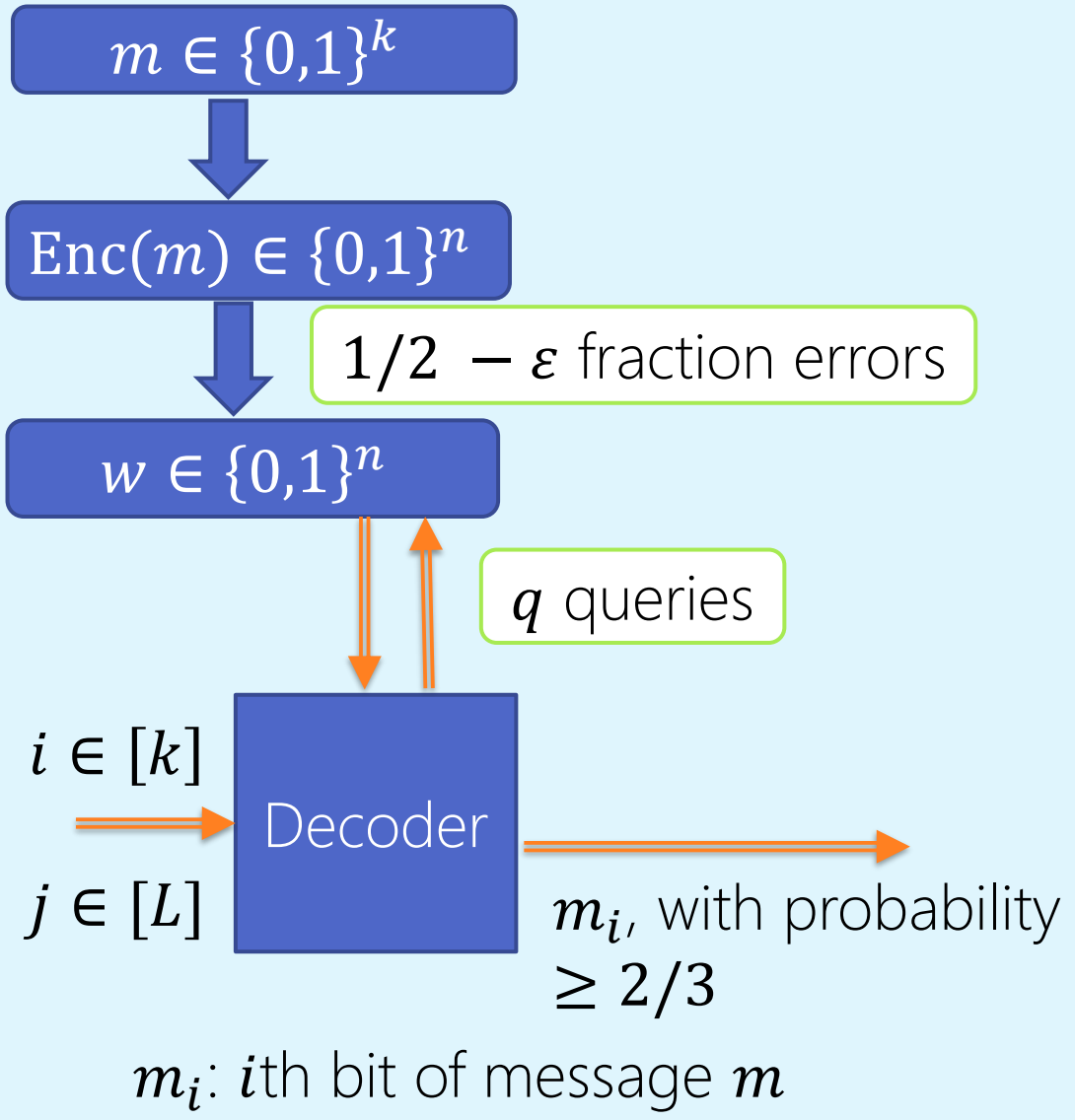
What we will show

- Local list decoding of $Enc: \{0,1\}^k \to \{0,1\}^n$ 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



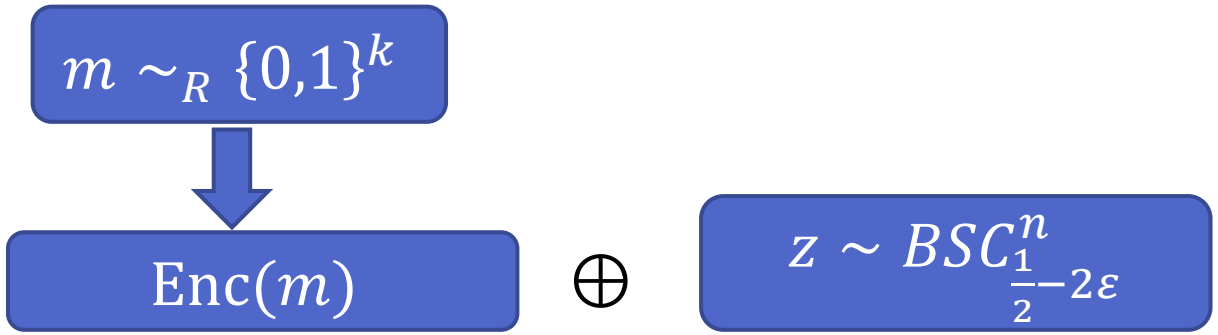


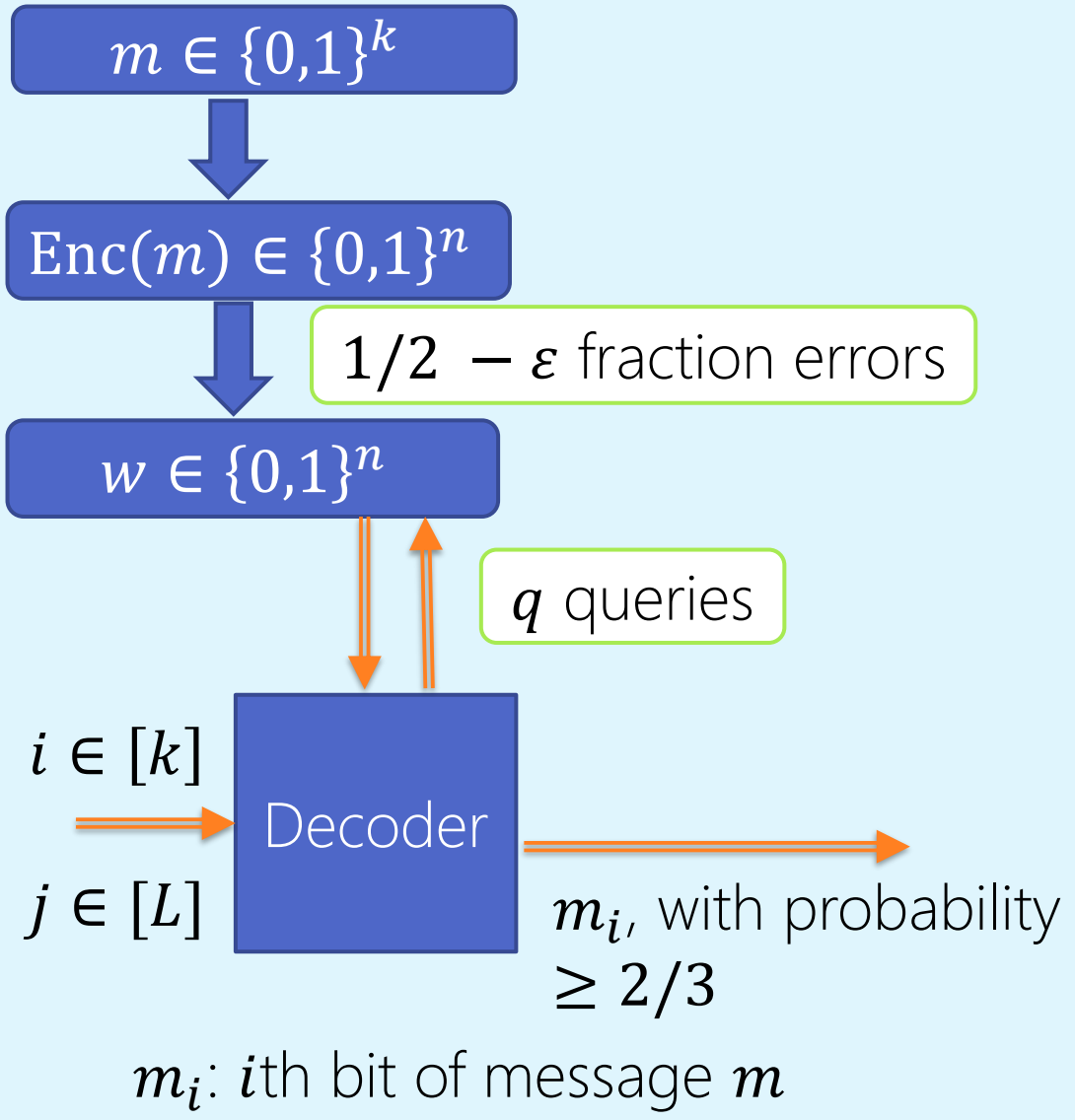
m_i: ith bit of message m

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

Reducing to a different problem

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

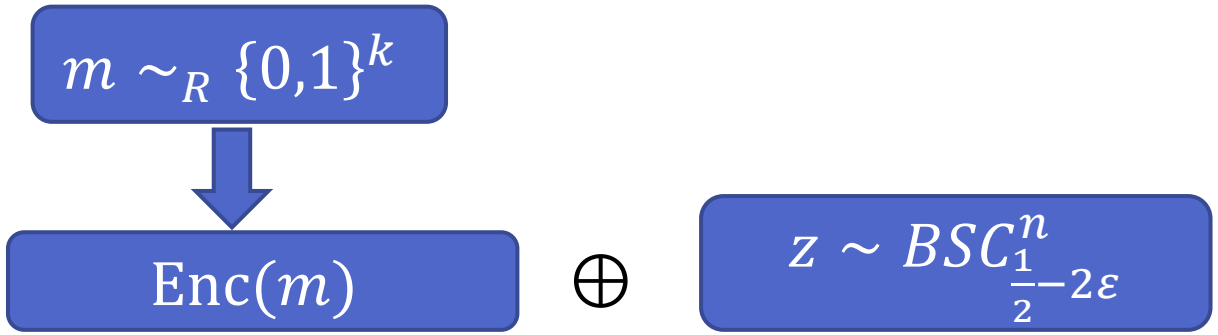




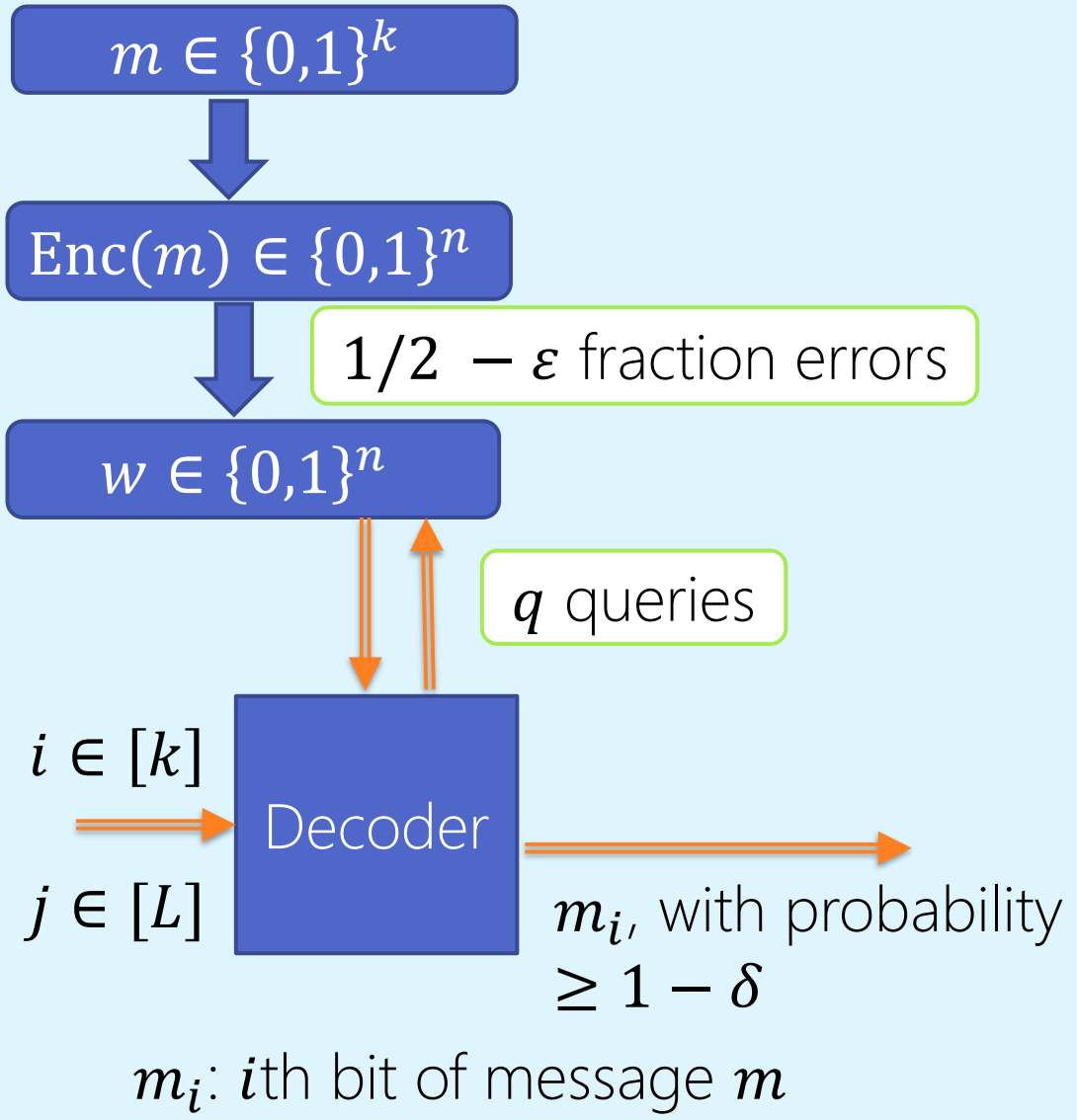
BSC_p^n: Distribution over $\{0,1\}^n$; each bit 1 independently with probability p

Reducing to a different problem

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



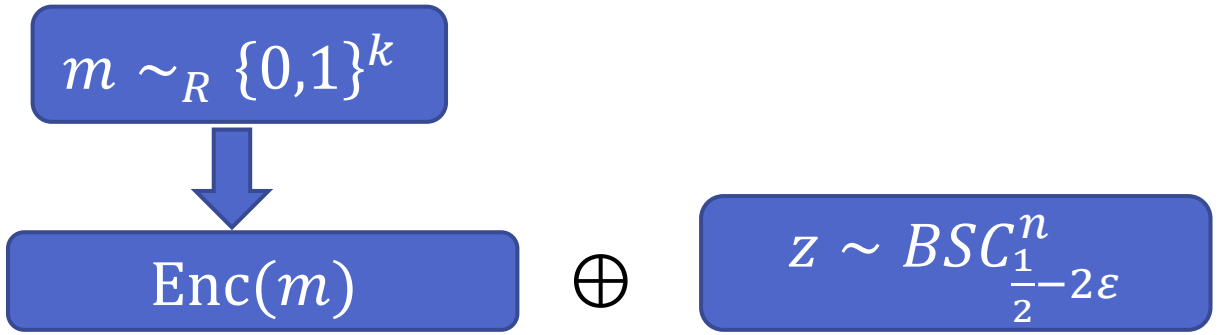
- Decode at least $1 - 1/2k$ fraction of message bits correctly



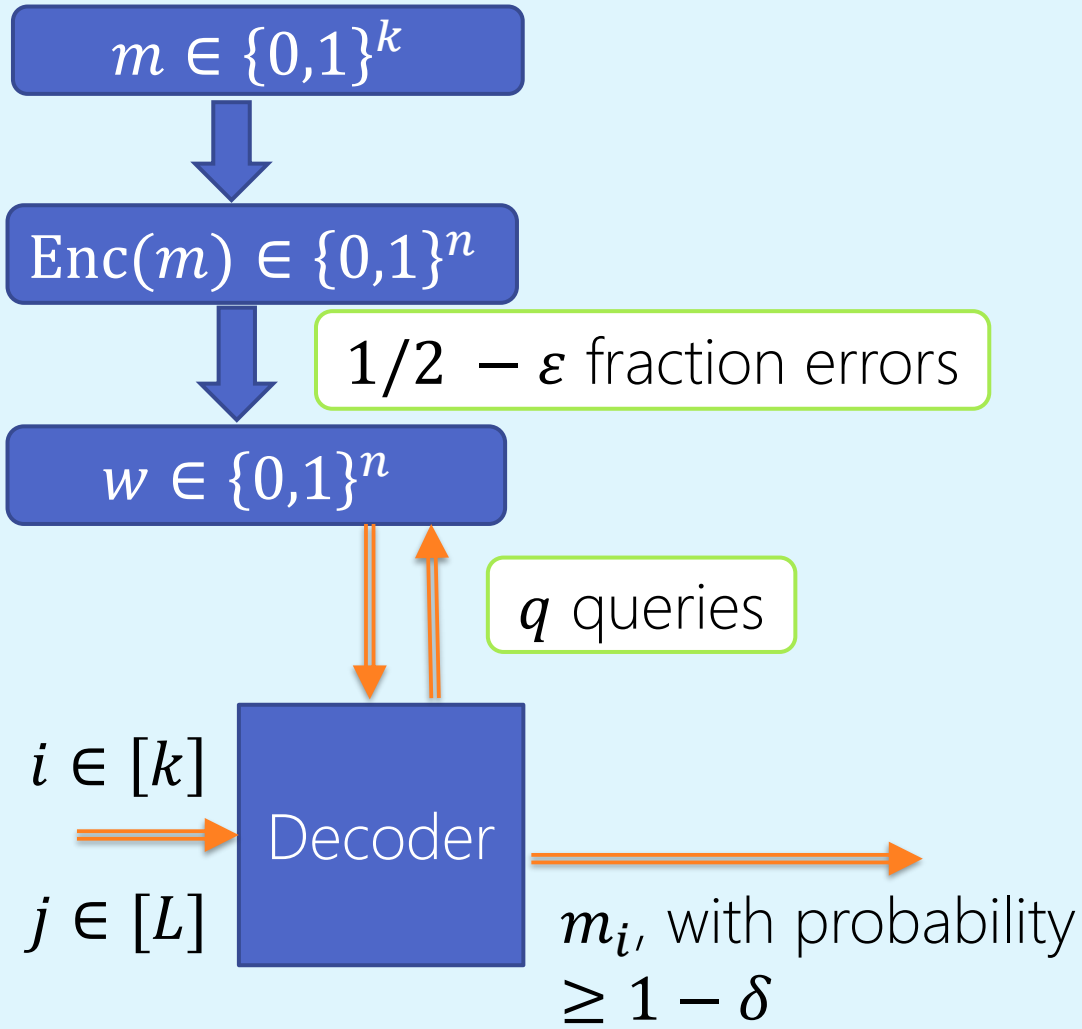
BSC_p^n: Distribution over $\{0,1\}^n$; each bit 1 independently with probability p

Reducing to a different problem

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



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

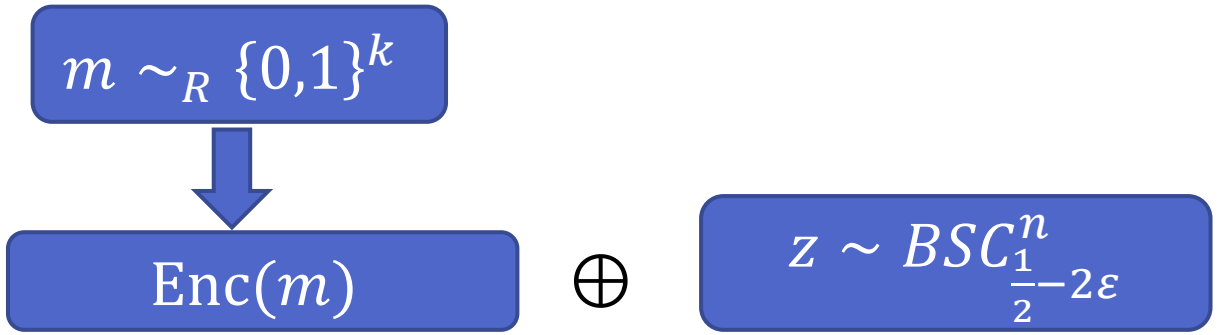


m_i: ith bit of message m

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

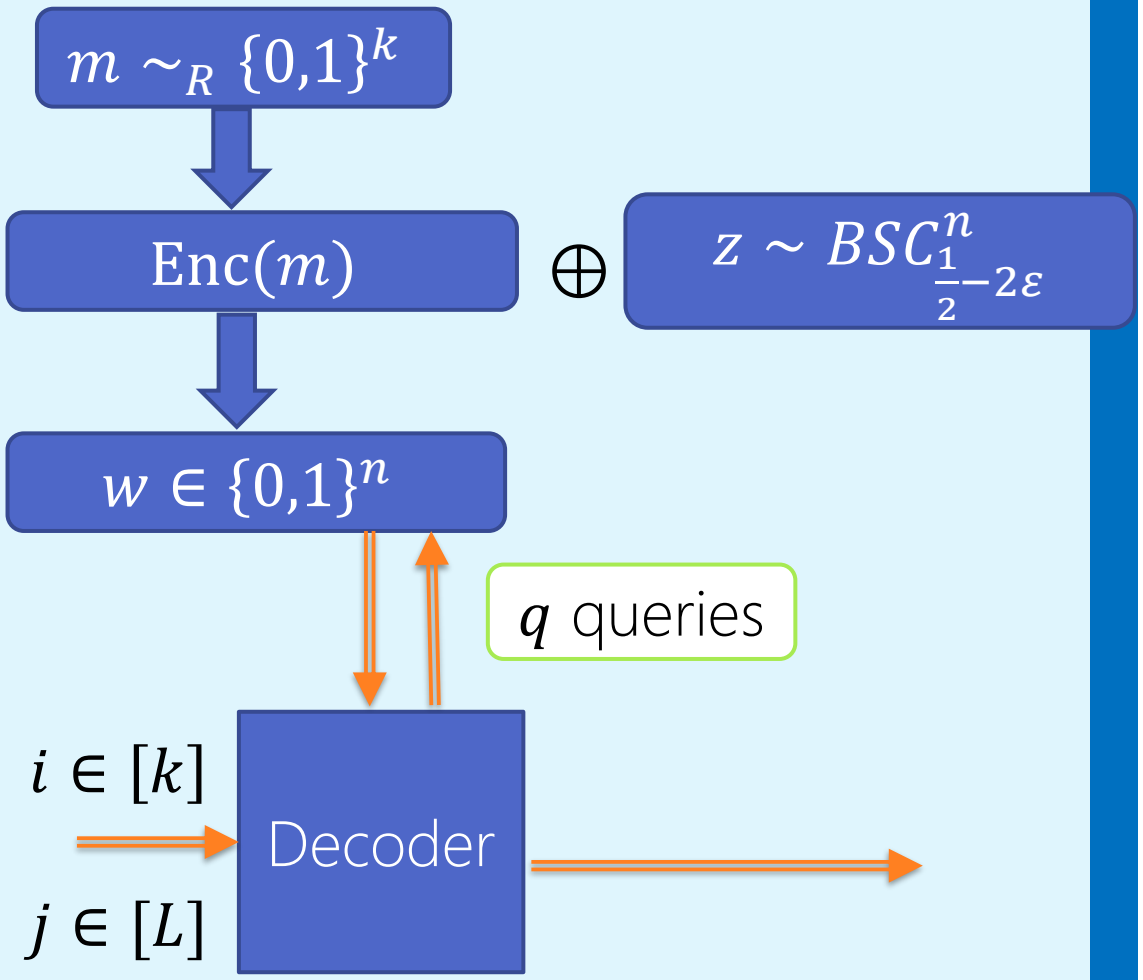
Reducing to a different problem

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



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

Local list decoding implies above decoding task (up to $O(\log k)$ factor in queries)

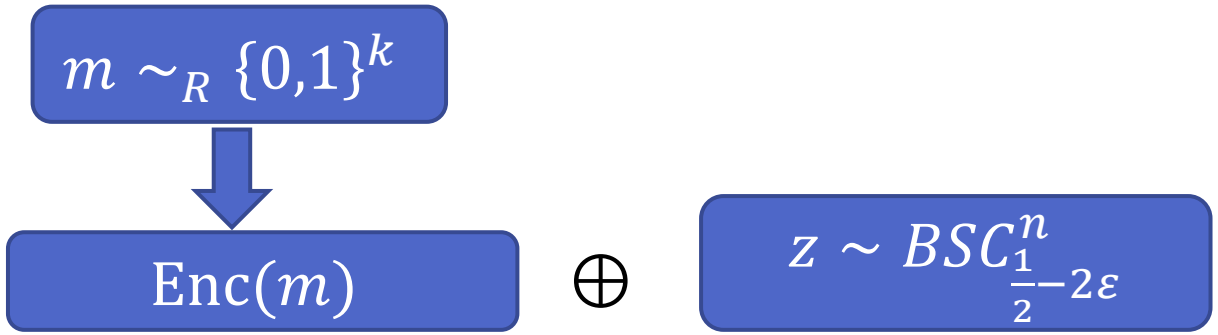


With probability at least $\frac{1}{3}$ over the choice of (m, z, w), $\exists\, j \in [L]$

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

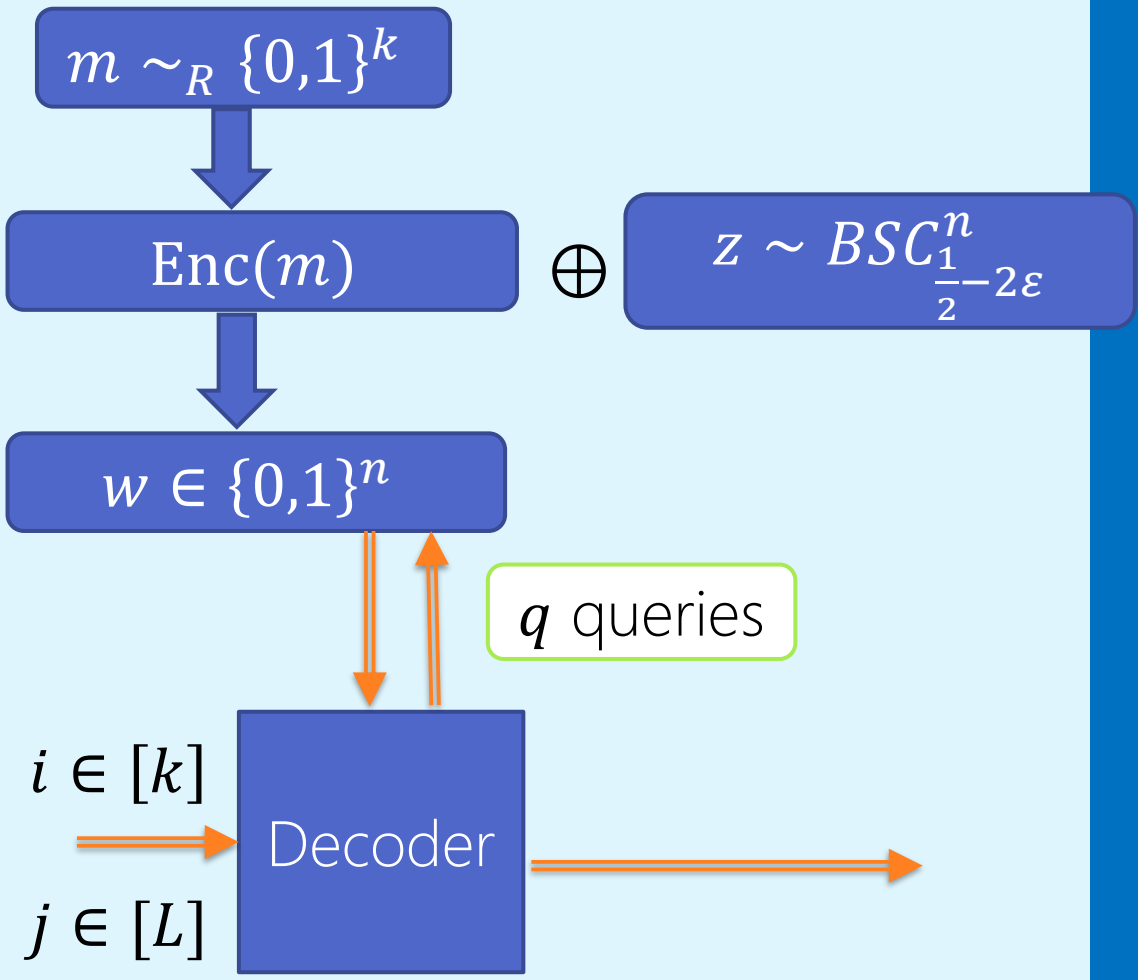
Reducing to a different problem

- 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)

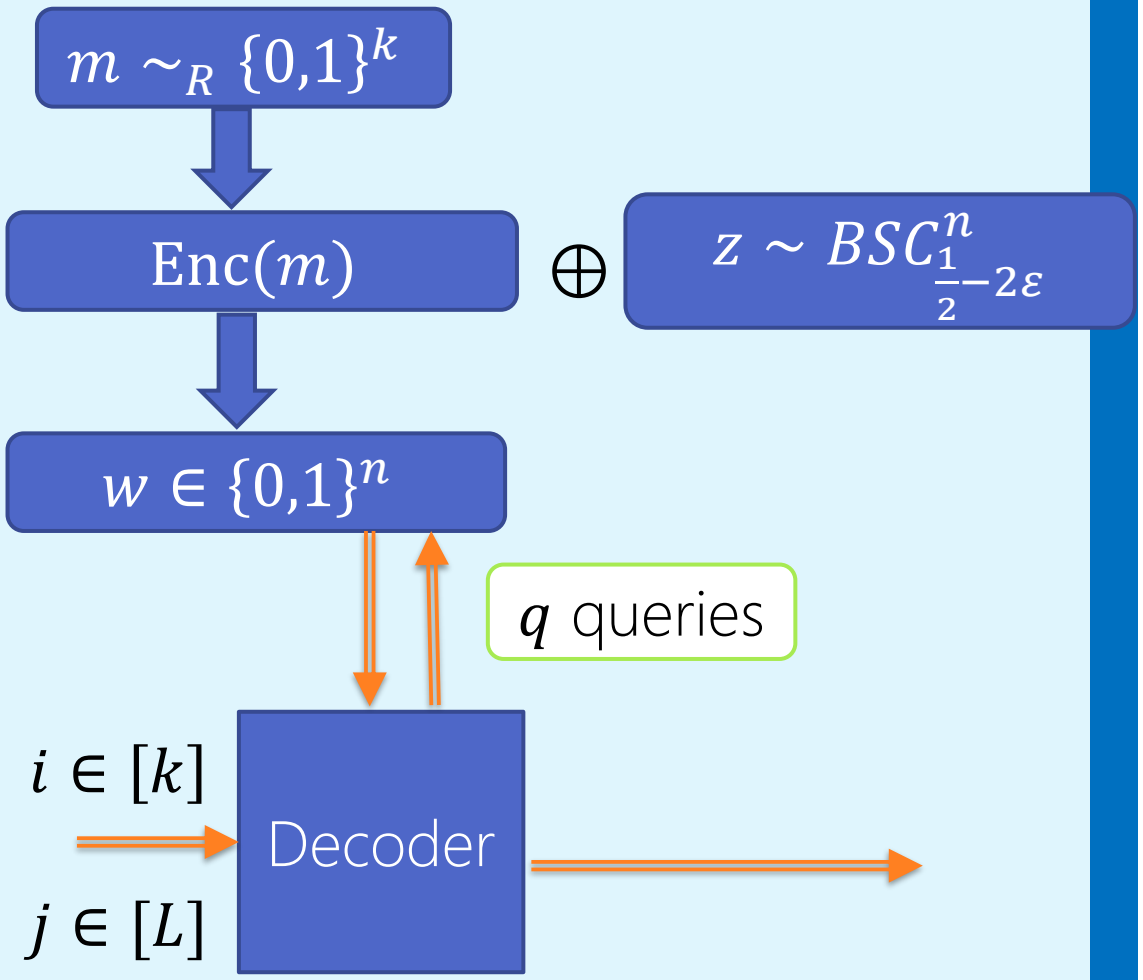


With probability at least $\frac{1}{3}$ over the choice of (m, z, w), $\exists\, j \in [L]$

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

Lower bounds on circuit sizes for coin problem

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

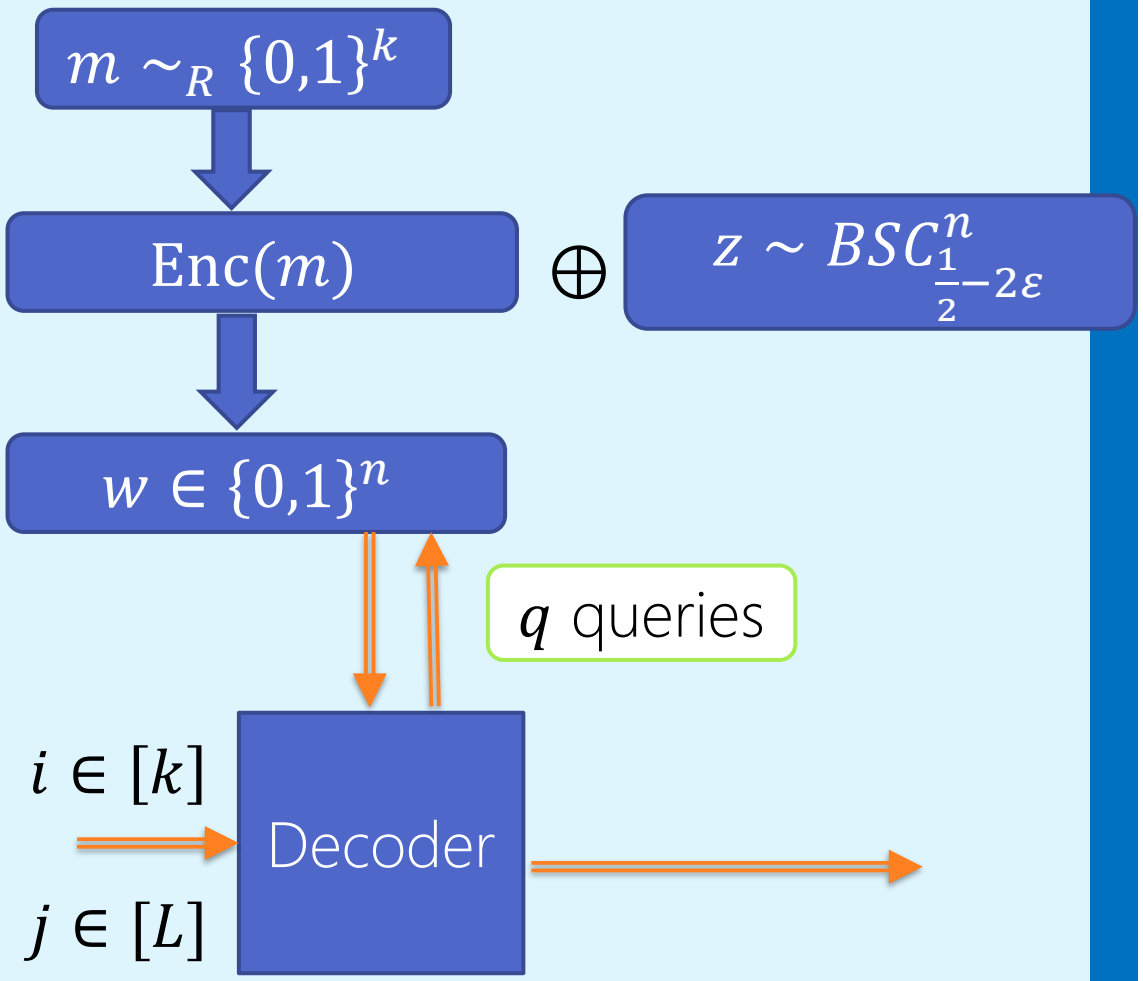


With probability at least $\frac{1}{3}$ over the choice of (m, z, w), $\exists\, j \in [L]$

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

Lower bounds on circuit sizes for coin problem

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



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

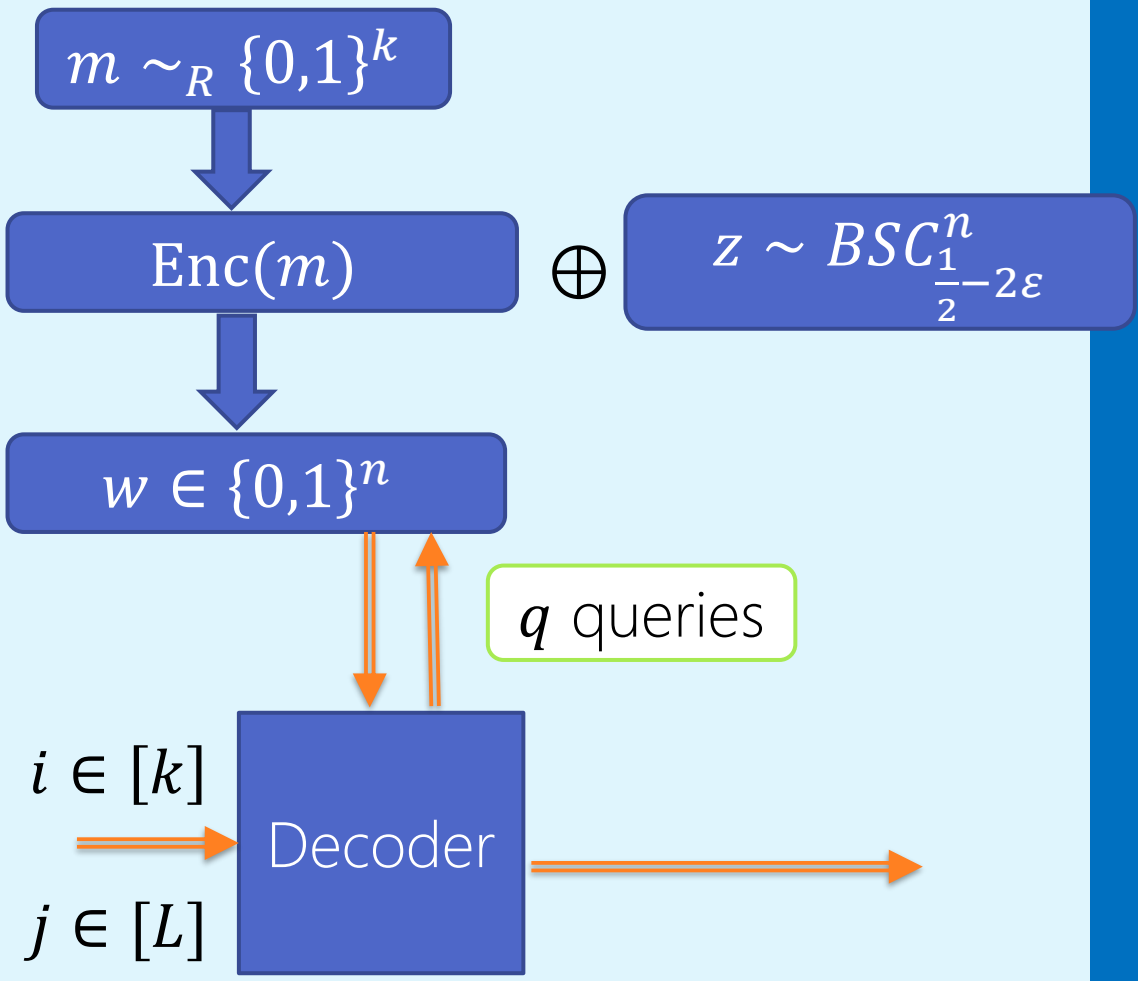
$$\Pr_{i\sim[k]}[\mathrm{Dec}^w(i,j) = m_i] \geq 1 - 1/2k$$

Lower bounds on circuit sizes for coin problem

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

  Then C has size at least

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



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

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

Lower bounds on circuit sizes for coin problem

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

  Then C has size at least

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

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. $\Pr_{z \sim BSC^n_{\frac{1}{2}-2\varepsilon}}[C(z) = 1] \geq 0.99$
  2. $\Pr_{z \sim BSC^n_{\frac{1}{2}}}[C(z) = 1] \leq 0.01$

  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 $w = Enc(m) \oplus z$

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. $\Pr_{z \sim BSC^n_{\frac{1}{2}-2\varepsilon}}[C(z) = 1] \geq 0.99$
  2. $\Pr_{z \sim BSC^n_{\frac{1}{2}}}[C(z) = 1] \leq 0.01$

  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 $Dec^w(i,j) = m_i$

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. $\Pr_{z \sim BSC^n_{\frac{1}{2}-2\varepsilon}}[C(z) = 1] \geq 0.99$
  2. $\Pr_{z \sim BSC^n_{\frac{1}{2}}}[C(z) = 1] \leq 0.01$

  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 $\wedge_{i \in [k]} b_{i,j}$

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. $\Pr_{z \sim BSC^n_{\frac{1}{2}-2\varepsilon}}[C(z) = 1] \geq 0.99$
  2. $\Pr_{z \sim BSC^n_{\frac{1}{2}}}[C(z) = 1] \leq 0.01$

  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 $\vee_{j\in[L]} \wedge_{i\in[k]} b_{i,j}$

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. $\Pr_{z\sim BSC^n_{\frac{1}{2}-2\varepsilon}}[C(z) = 1] \geq 0.99$
  2. $\Pr_{z\sim BSC^n_{\frac{1}{2}}}[C(z) = 1] \leq 0.01$

  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 $\vee_{j\in[L]} \wedge_{i\in[k]} b_{i,j}$
- Can do this with a circuit of depth 3 and size $O(k \cdot L \cdot q2^q)$

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. $\Pr_{z\sim BSC^n_{\frac{1}{2}-2\varepsilon}}[C(z) = 1] \geq 0.99$
  2. $\Pr_{z\sim BSC^n_{\frac{1}{2}}}[C(z) = 1] \leq 0.01$

  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 $\vee_{j\in[L]} \wedge_{i\in[k]} b_{i,j}$
- Can do this with a circuit of depth 3 and size $O(k \cdot L \cdot q2^q)$
- 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 $C: \{0,1\}^n \to \{0,1\}$ has depth d, and:
  1. $\Pr_{z\sim BSC^n_{\frac{1}{2}-2\varepsilon}}[C(z) = 1] \geq 0.99$
  2. $\Pr_{z\sim BSC^n_{\frac{1}{2}}}[C(z) = 1] \leq 0.01$

  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 $\vee_{j \in [L]} \wedge_{i \in [k]} b_{i,j}$
- Can do this with a circuit of depth 3 and size $O(k \cdot L \cdot q2^q)$

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:

$$\Pr_{m\sim\{0,1\}^k, z\sim BSC^n_{\frac{1}{2}-2\varepsilon}} [C_m(z) = 1] \geq \frac{1}{6}$$

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:

$$\Pr_{m\sim\{0,1\}^k, z\sim BSC^n_{\frac{1}{2}-2\varepsilon}}[C_m(z) = 1] \geq \frac{1}{6}$$

- Since $Enc(m) \oplus z$ is uniformly random for $z \sim BSC^n_{\frac{1}{2}}$:

$$\Pr_{m\sim\{0,1\}^k, z\sim BSC^n_{\frac{1}{2}}}[C_m(z) = 1] \leq \frac{L}{2^k}$$

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 $\vee_{j \in [L]} \wedge_{i \in [k]} b_{i,j}$
- Can do this with a circuit of depth 3 and size $O(k \cdot L \cdot q2^q)$

- From definition of decoder:

$$\Pr_{m \sim \{0,1\}^k, z \sim BSC^n_{\frac{1}{2}-2\varepsilon}} [C_m(z) = 1] \geq \frac{1}{6}$$

- Since $Enc(m) \oplus z$ is uniformly random for $z \sim BSC^n_{\frac{1}{2}}$:

$$\Pr_{m \sim \{0,1\}^k, z \sim BSC^n_{\frac{1}{2}}} [C_m(z) = 1] \leq \frac{L}{2^k}$$

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

$$\Pr_{z \sim BSC^n_{\frac{1}{2}-2\varepsilon}} [C_m(z) = 1] \geq 0.99 \text{ and}$$

$$\Pr_{z \sim BSC^n_{\frac{1}{2}}} [C_m(z) = 1] \leq 0.01$$

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 $\vee_{j\in[L]} \wedge_{i\in[k]} b_{i,j}$
- Can do this with a circuit of depth 3 and size $O(k \cdot L \cdot q2^q)$

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

$$\Rightarrow q \geq \frac{1}{\log k\sqrt{\varepsilon}} - \log L = \Omega\left(\frac{1}{\varepsilon^{0.5-o(1)}}\right)$$

- From definition of decoder:

$$\Pr_{m\sim\{0,1\}^k, z\sim BSC^n_{\frac{1}{2}-2\varepsilon}}[C_m(z) = 1] \geq \frac{1}{6}$$

- Since $Enc(m) \oplus z$ is uniformly random for $z \sim BSC^n_{\frac{1}{2}}$:

$$\Pr_{m\sim\{0,1\}^k, z\sim BSC^n_{\frac{1}{2}}}[C_m(z) = 1] \leq \frac{L}{2^k}$$

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

$$\Pr_{z\sim BSC^n_{\frac{1}{2}-2\varepsilon}}[C_m(z) = 1] \geq 0.99 \text{ and}$$

$$\Pr_{z\sim BSC^n_{\frac{1}{2}}}[C_m(z) = 1] \leq 0.01$$

What we saw

- Local list decoding of $Enc: \{0,1\}^k \to \{0,1\}^n$ 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 $\beta > 0$

Open problems

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

Open problems

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

Open problems

- Improving the lower bound for the small ε case from $\Omega\left(\frac{1}{\sqrt{\varepsilon}}\right)$
- Our lower bound for the case of large ε 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 ε case?
- Non-black-box techniques that help obtain better hardcore predicates from hard functions?

Thank You!