Relaxed Locally Correctable Codes in Computationally Bounded Channels

Elena Grigorescu (Purdue)

Joint with Jeremiah Blocki (Purdue), Venkata Gandikota (JHU), Samson Zhou (Purdue)
Classical Locally Decodable/Correctable Codes

Encoding: \( E: \{0,1\}^k \rightarrow \{0,1\}^n \)

Decoding: \( D: \{0,1\}^n \rightarrow \{0,1\}^k \) such that given \( w \) with \( \text{dist}(w,E(m)) < \delta n \) then \( D(w) = m \).

Goal: efficient encoding/decoding

Parameters: information rate: \( k/n \); minimum distance: \( \min \text{dist}(E(m_1), E(m_2)) \)

Locally decodable/correctable codes (LDCs/LCCs)

- **LDC**: Given oracle access to input \( w \) with \( \text{dist}(w,E(m)) < \delta n \), and \( i \), compute \( m_i \) with \( o(n) \) queries
- **LCC**: Given oracle access to input \( w \) with \( \text{dist}(w,E(m)) < \delta n \), and \( i \), compute \( (E(m))_i \) with \( o(n) \) queries

Status: \( q = 2^{O(\sqrt{\log n})} \), any constant rate \( 0 < R < 1 \) [KMRS17]

\( q > 2 \) (constant), \( n = 2^{2^{\sqrt{\log n}}} \) [Yek08, DGY11, Efr12]
Relaxed LDCs/LCCs (RLDCs/RLCCs)

RLDC/RLCCs: Given oracle access to input $w$ with $\text{dist}(w, E(m)) < \delta n$, $D$ makes $q = o(n)$ queries and:

1) $\forall i, D_i(w) = m_i$ if $w = E(m)$ (RLDC); $D_i(w) = E(m)_i$ (RLCC)

2) $\forall i, \Pr[b \notin \{m_i, \perp\}] < 1/3$ \hspace{1cm} (RLDC)
   $\Pr[b \notin \{E(m)_i, \perp\}] < 1/3$ \hspace{1cm} (RLCC)

3) Let $\text{Good} = \{j \mid \Pr[D_j(w) = m_j] > \frac{2}{3}\}$ \hspace{1cm} (RLDC)
   $\text{Good} = \{j \mid \Pr[D_j(w) = (E(m))_j] > \frac{2}{3}\}$ \hspace{1cm} (RLCC)

Then $|\text{Good}| > \rho n$, for some constant $\rho$.

Observation: 1) + 2) imply 3) for constant query codes and constant error rate

Status: RLDCs [BGHSV06]: $q = \Theta(1), n = k^{1+\epsilon}$

RLCCs [GRR18]: $q = \Theta(1), n = \Theta(\text{poly}(k))$, $q = (\log n)^{O(\log \log n)}, n = \Theta(k)$

Our results: $q = \text{poly} \log n$, $n = \Theta(k)$ for crypto version of definitions
Codes for Computationally Bounded Channels (CBC)

**Hamming channel**: the channel corrupts any pattern (possibly takes long time to corrupt adversarially)

**Shannon channel**: the channel introduces independent errors

**Lipton channel**: Computationally bounded - the channel is a PPT adversary

Previous work:

General Codes in CBCs achieve better communication capabilities than in the Hamming model

[Lip94, DGL04, Langberg04, MPSW05, Smith07, GS16, SS16]

Locally Decodable Codes in CBCs: Requires trusted setup/key exchange

- Private-key LDCs [OPS07] - Assumes existence of OWF, shared secret key
  - $\Theta(1)$ info rate and error rate over binary alphabet, $q = \omega(1)$

- Public-key LDCs [HO08, HOSW11] - Crypto assumptions: $\phi$-hiding schemes and IND-CPA secure cryptosystems
Computational Relaxed LCCs (CRLCC)

Security parameter $\lambda, s=$Gen$(1^\lambda)$, $s$ is public

---

**Sender**

$m$ → $A$

$E(s, m)$ → $A$

$E(s, m) + e$ → **Receiver**

$b = D(s, w, i)$

---

Defs: $p_{A,s} = \Pr[b \notin \{w_i, \bot\}]$ (Decoder’s error probability)

$Good_{A,s} = \{i \mid \Pr[D(s, w, i) = (E(m))_i] > \frac{2}{3}\}$

---

**Def:** (Gen, $E, D$) is a CRLCC with parameters $q$ queries, $\tau$ error rate, $0 < \rho \leq 1$, against PPT adversaries if $D$ makes $q$ queries to input $w$ and

1) For all $s$, if $w = E(s, m)$ then $D(s, m, i) = (E(s, m))_i$

2) For all $A$ in the class, $\Pr[Pr[b \notin \{w_i, \bot\}] > \text{negl.}] < \text{negl.}$

3) For all $A$ in the class, $\Pr[Good_{A,s} < \rho n] < \text{negl.}$
Computational Relaxed LCCs

\((Gen, E, D)\) is a CRLCC with parameters \(q\) queries, \(\tau\) error rate, \(\rho\), against a class of adversaries (here PPT) if \(D\) makes \(q\) queries to input \(w\) and

1. For all \(s\), if \(w = E(s, m)\) then \(D(s, m, i) = (E(s, m))_i\)

2. For all \(A\) in the class, \(\Pr[\Pr[b \notin \{w_i, \bot\}] > \gamma = \text{negl.}] < \mu = \text{negl.}\)

3. For all \(A\) in the class, \(\Pr[\text{Good}_{AS} < \rho] < \mu = \text{negl.}\)

\[p_{AS} = \Pr[b \notin \{w_i, \bot\}]; \text{Good}_{AS} = \{i | \Pr[D(s, w, i) = (E(m)_i] > \frac{2}{3}\}\]

Observation: Classical RLCC: for all \(A\) (not necessarily PPT) \(\forall i, |\text{Good}| > \rho, \gamma = 1/3, \mu = 0\)

Our results: Weak and Strong CRLCC for binary alphabet, constant information and error rate, \(\text{poly log}(n)\) queries, assuming the existence of collision-resistant hash functions.
Our results - Observations

Results: Weak and Strong CRLCC for binary alphabet, constant error and information rate, $\text{poly log}(n)$ queries, assuming the existence of collision-resistant hash function.

- Classical RLCCs [GRR18]: $q = (\log n)^{O(\log \log n)}$, constant information rate, subconstant error rate

- Previous constructions of RLCC in CBC need public/private-key crypto setup; our constructions don’t.

- Our setup assumption: public seed chosen once

- Key Idea: local expander graphs
Local Expander Graphs and Their Properties

[ErdoesGrahamSzemeredi75] \((A, B)\) contains a \(\delta\)-expander if for all subsets \(X \subseteq A, Y \subseteq B\) of fractional size \(\delta\), there is an edge between \(X\) and \(Y\).

\(\delta\)-local expander: 

\(G\) is a DAG such that for all vertices \(v\), and radii \(r\), \((A = [v - r + 1, v], B = [v + 1, v + r])\) contains a \(\delta\)-expander.
Local Expanders: Properties and Applications

Thm [EGS75, ABP18]: For any $\delta > 0$, there exist explicit $\delta$-local expanders $G$ on $n$ vertices with indegree($G$), outdegree($G$) = $O(log n)$

Def: For set $S$, vertex $v$ is $\alpha$-good if for any radius $r$, $|S \cap [v - r + 1, v]| \leq \alpha r$ and $|S \cap [v + r - 1, v]| \leq \alpha r$

Thm [EGS75, ABP18]: If we delete large set $S \subseteq V$, all $\alpha$-good vertices are on a path

Applications:
- proof of sequential work [MMV13, CP18]
- time-lock puzzles and fair coin flipping protocols [BN00, JM10]
- design of memory hard functions [ABH17, ABP17, BZ17, ABP18]
(Weak) CRLCCs using local expander graphs

**CRHF:** $H_s: \{0,1\}^* \rightarrow \{0,1\}^{L(\lambda)}$ is collision-resistant if for all PPT adversaries $A$, $Pr[A \text{ finds } H(x) = H(x')]$ is negl.

Labeling graph $G$ using $H$ and input $m = (m_1 \circ m_2 \circ m_3 \ldots \circ m_k) \in \Sigma^k$, where $\Sigma = \{0,1\}^{L(\lambda)}$.

Encoding of $m = (m_1 \circ m_2 \circ m_3 \ldots \circ m_k)$ is the concatenation of 3 parts

1. $(ECC(m_1) \circ ECC(m_2) \circ ECC(m_3) \ldots \circ ECC(m_k))$ ECC is good and efficiently decodable (eg., Justesen)
2. $(ECC(l(1)) \circ ECC(l(2)) \circ ECC(l(3)) \ldots \circ ECC(l(k)))$ underlying $G$ is $\delta$-local expander
3. $(ECC(l(k)) \circ ECC(l(k)) \circ ECC(l(k)) \ldots \circ ECC(l(k)))$ $k$ copies of last label
Ingredients of the Local Decoder

- Testing consistent labeling:

After decoding the ECCs, check if $v$’s label is consistent with parents’ labels $l'(v) = H(m' \circ l'(p_1) \circ ... \circ l'(p_t))$. Else $v$ is inconsistent.

- Testing $\alpha$-goodness:

Recall: Vertex $v$ is $\alpha$-good w.r.t set $S$ if for any radius $r$, $|S \cap [v - r + 1, v]| \leq \alpha r$ and $|S \cap [v + r - 1, v]| \leq \alpha r$

Test if vertex $v$ of $G$ is $\alpha/4$-good with respect to set $S$ of inconsistent nodes.

Test guarantees: accepts if $v$ is $\alpha/4$-good (hence also $\alpha$-good) (whp)
rejects if $v$ is not $\alpha$-good (whp)

$O(\log n)$ vertex queries
Local Decoding

\( w = (ECC(m'_1) \circ ECC(m'_2) \ldots \circ ECC(m'_k)) \circ ECC(l'(1)) \circ ECC(l'(2)) \circ \ldots \circ ECC(l'(k)) \circ ECC(l'(k)) \circ \ldots \circ ECC(l'(k)) \)

- **Encoding of labeling of \( \delta \)-expander \( G \)**
  - Ensures that the last block is decoded correctly
  - **\( D(i) \): Decode by majority vote**
  - Test consistency of vertex \( k \) in \( G \)
  - Test if vertex \( k \) is \( \alpha \)-good w.r.t set of inconsistent nodes
  - Output \( \perp \) if tests fail; o/w output decoded bit

- **\( D(i) \): Output same answer as for the corresponding vertex**

- **\( D(i) \): If \( i \) is in \( ECC(l'(j)) \), test if vertex \( j \) of \( G \) is \( \alpha \)-good with respect to set of inconsistent nodes**
  - If the answer is yes, output the decoding of \( ECC(l'(j)) \); o/w output \( \perp \)
Analysis: Key Ideas

If vertex is **consistent** and **correctly decoded** then

$$l(v) = l'(v) = H(m_v \circ l(p_1) \circ l(p_2) ... \circ l(p_t)) = H(m'_v \circ l'(p_1) \circ l'(p_2) ... \circ l'(p_t))$$

Implies $$m_v = m'_v$$ and $$l(p_1) = l'(p_1), l(p_2) = l'(p_2), ..., l(p_t) = l'(p_t)$$   [correct decoding of parent label!]

or colliding pair was found!

Hence, if a parent is consistent, then can iteratively backtrack along a path of consistent nodes and deduce correct decoding of a label!

Recall: Thm [EGS75, ABP18] If we delete large set $$S \subseteq V$$, all $$\alpha$$-good vertices remain on a path.

Conclusion: The test only returns the decoded bit when it thinks that block is correctly decoded (and $$\alpha$$-good.)
Extensions: Strong CRLCCs

**Def:** \((Gen, E, D)\) is a CRLCC with parameters \(q\) queries, \(\tau\) error rate, \(\rho\), against a class of PPT adversaries if \(D\) makes \(q\) queries to input \(w\) and

1) For all \(s\), if \(w = E(s, m)\) then \(D(s, m, i) = (E(s, m))_i\)
2) For all \(A\) in the class, \(\text{Pr}[[\text{Pr} [b \notin \{w_i, \bot\}] > \text{negl.}] < \text{negl.}]\)
3) For all \(A\) in the class, \(\text{Pr}[\text{Good}_{A,s} < \rho] < \text{negl.}\)

- Need to ensure that the adversary cannot corrupt the entire codeword and obtain a new encoding in which all tests check

- **Idea:** Reduce the degree of the graphs by a composition of \(\delta\)-expanders and path-like graphs and encode \`metanodes\` as blocks

- Use the extra fact that there are many \(\alpha\)-good nodes (long paths)
Conclusions and Further Directions

Our results: Weak and Strong CRLCC/CRLDC for binary alphabet, constant error and information rate, \( \text{poly} \log(n) \) queries, assuming the existence of collision-resistant hash function.

Open directions: Better tradeoffs: \( q = \Theta(1) \)?

Other local models in computationally bounded channels (non-relaxed LCCs, testing)?

THANK YOU!