Today

Locally Decodable Codes

- Definition / Motivation
- LDGs via multiv. polynomials
- LDGs via multiplicities
- LDG from matching vectors (matching vector construction)
**Definition**

\( l \)-LDC: maps \( \Sigma^k \rightarrow \Sigma^n \)

Corrects \( \epsilon \)-fraction error \( l \) locally

i.e., given oracle access to \( y \) s.t.

\( \exists m \text{ s.t. } \Delta(y, E(m)) \leq \epsilon \cdot n \)

\( \forall \text{ input } i \in [k] \)

\[ \Pr[D_y(i) = m_i] \geq \frac{2}{3} \]

---

**Motivation:**

**Current Encoding:**

- Either store all info in 1 big block
  - good error-correction, but slow
  \( (\approx \text{length of block}) \)
- Or break into small pieces
  - quick correction, but \( \Pr[\text{Error}] \rightarrow 1 \)

LDC's try to bridge gap.
Sublinear LDCs via Multivar. Polynomials

Idea: Need code to have local "redundancies" (small set of coordinates that have dependences)

- Reed-Solomon has no such redundancies

Idea: - use low-degree multivar. polynomials

- Locality? On every line, function values restricted.
General setting:

- \# variables = m
- degree = d
- Field size = \( q > \frac{d}{1-2\epsilon} \)
- Code = Evaluations of deg. d polys in m variables.

Resulting parameters

\[ n = q^m \]

\[ k = \binom{d+m}{m} \geq \left( \frac{d}{m} \right)^m \approx \frac{(1-2\epsilon)^m}{m^m} . n \]

\[ d = (-2\epsilon) \cdot n \]

locality \( l = q = n^m \)
Some interesting choices:

- \( m = \frac{1}{\varepsilon} : \frac{k}{n} \approx \varepsilon \)

\( l = n^\varepsilon \)

- \( q = O(1) : n = \exp(k^{1/2-1}) \)

\( l = q \)

- \( m = \frac{\log n}{\log \log n} : \quad n = \text{poly}(k) \)

\( l = \text{poly log } n \).

Initial beliefs:

Maybe roughly best possible behavior?

- locality \( n \Rightarrow \frac{k}{n} \Rightarrow o(n) \) ?

- locality \( O(1) \Rightarrow n = \exp(k^\varepsilon) ? \)
**Multiplicity Codes**: [Kopparty - Saraf - Yekhanin]

**Messages**: $d$, $m$-variate polynomials.

**Encoding**: Evaluation of message polynomial, and all its derivatives up to order $s$.

**Alphabet**: $\mathcal{E} = \mathbb{F}_q^{m+s \choose m}$ 

# such derivatives

**Key Lemma**: “Multiplicity Schwartz-Zippel”

\[ p \in \mathbb{F}_q[x_1, \ldots, x_m], \deg p \leq d, p \neq 0 \]

\[ \Rightarrow \exists \bar{a}, P_{\bar{a}} \left[ P \& \text{all its partial derivatives} \right] \leq \frac{d}{(s+1) \cdot q} \]
Parameters

\[ k = \binom{d+m}{m} \approx \left( \frac{d+m}{m+s} \right)^m \rightarrow \left( \frac{d}{s} \right)^m \]

\[ q = \frac{d}{s} (1-e) \]

\[ n = q^m = \frac{k}{(1-e)^m} \]

By letting \( m \) grow, \( e \) then \( s \) grow even faster, can have

\[ l = n^s, \quad \frac{k}{n} = (1-s)^m \text{ simultaneously!} \]
$O(1)$ - Locality Regime

[Yekhanin '07]
[Raghtavendra '08]
[Efremenko '09]

Main Result: \( \exists \) nodes with \( \ell = 3 \) and
\[
\eta = \exp(\exp(\sqrt{\log k}))
\]
(\text{compare with} \ \eta = \exp(k^{1/2}))

More generally, \( \ell = O(1) \)
\[
\eta = \exp(\exp((\log k)^{\varepsilon}))
\]

Construction without intuition in rest of notes.
Ingredients

- Parameter $m \in \mathbb{Z}^+$ (small...)
- field $\mathbb{F}_q$ with $m \mid q - 1$
  (so $\mathbb{F}_q$ has primitive $m^{th}$ root)
- $s \in \mathbb{Z}_m$, $0 < s$
- $s$-Nia matrix $M \in \mathbb{Z}_m^{k \times n}$

**Defn:** $M$ is $s$-nice if, for

\[
M = \begin{bmatrix}
M_1 & M_2 \\
M_2^T & M_1^T
\end{bmatrix}
\]

\(1\) $(M_1)_{ii} = 0$, \(2\) $(M_1)_{ij} \in \mathbb{F}$ if \(i \neq j\)

\(3\) $M$ is closed under column sums.
$\mathbb{Z}_m$-matrices $\Rightarrow \overline{\mathbb{F}}_q$-matrices

\[ M_{ij} \rightarrow g^{M_{ij}} = G_{ij} \]

[g primitive $m^{th}$ root in $\mathbb{F}_q$]

**Theorem:** $G$ is generator of $(\mathbb{Z}_l + 1)$-LDC

(Terminology: $G$ is "generator" of the encoding map $x \mapsto x \cdot g$)
Defn: $p \in \mathbb{F}_q[x]$ is $S$-zeroing poly if

1. $p(1) = 1$
2. $p(q^s) = 0 \forall s \in S$

Defn: $p \in \mathbb{F}_q[x]$ is $t$-sparse if $p$ has at most $t$ non-zero coefficients.

Lemma: If $S$ has a $t$-sparse $S$-zeroing poly, then $G = H(M)$ is $t$-LDC.

Proposition: Every $S \leq \mathbb{Z}_m^*$ has a $(|S|+1)$-zeroing polynomial.

(Lemma + Proposition $\Rightarrow$ Theorem)
Proof of Lemma

to be filled.

Construction of nine matrices
to be added.